INTERNET SAFETY LABS

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

April 9, 2025

Joint Committee on Advanced Information Technology and Cybersecurity
Sen. Michael Moore and Rep. Tricia Farley-Bouvier, Chairs

Re: Testimony in Support of the Massachusetts Consumer Data Privacy Act and the Massachusetts Data Privacy Act

Dear Chair Moore, Chair Farley-Bouvier and Members of the Committee:

I am writing on behalf of Internet Safety Labs in support of H.78, the Massachusetts Consumer Data Privacy Act (MCDPA), and S.45/S.29/H.104, the Massachusetts Data Privacy Act (MDPA). We appreciate the leadership that this Committee, and particularly Chairs Moore and Farley-Bouvier have shown towards enacting meaningful privacy protections for Massachusetts residents by sponsoring these bills.

Internet Safety Labs (ISL) is a 501(c)3 non-profit product safety testing organization. We have been assessing and reporting on safety risks (including privacy risks) since 2019. We create Safety Labels for mobile apps which can be viewed on our App Microscope (https://appmicroscope.org). Our safety labels report on observed data sharing between the app and the developer, and all third parties as evidenced by the network traffic between the app and these entities. In other words, we assess privacy based on the observed behavior of apps and websites, and not on what the developers say in privacy policies.

In 2022 we conducted the first of its kind US K-12 Edtech safety benchmark, auditing more than 1700 apps that were recommended or required by a representative sample of K-12 schools across the US. We are intimately familiar with the kinds of risks children (and adults) are exposed to by using technology the way it's intended (see in depth reports here: https://internetsafetylabs.org/resources/reports/2022-us-k12-edtech-benchmark/[1].

[1] The thirteen schools from Massachusetts in the 2022 benchmark can be seen by selecting MA on the map here: https://public.tableau.com/app/profile/internetsafetylabs/viz/K-12EdTechBenchmark2022/StateSummary

INTERNET SAFETY LABS

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

Here are some highlights from the benchmark that underscore the privacy risks students face:

- **68%** of the apps sent data to Google.[2]
  - **75%** of the schools that provide personal computing devices to students were providing Chrome OS based devices (i.e. Google).[2]
  - **100%** of Android apps requested Location permissions.
- **78%** of the apps scored the highest risk due to evidence of sharing data with very high risk third parties, usually advertising and marketing platforms.[2]
- **79%** of the apps requested location permission; **52%** of the apps accessed calendar and contacts.[2]
- Nearly **50%** of the apps recommended or required in schools were not education specific apps.[2]
- While COPPA Safety Harbor certified apps consistently had no behavioral ads, they had a **higher percentage of ads** (21.6%) than the overall sample (15.2%)[3] of which 28% of the apps were not strictly for children[2]. COPPA certified apps also were much more likely to be found sending data to risky third parties than apps with no certification or privacy promise (73.8% of COPPA certified apps vs. 54.6% of apps with no certification or privacy promise).[3]

Figure 1 shows an example safety label of the worst/leakiest app from our 2022 benchmark[4]. Note that there were 149 unique companies observed in the network traffic flow, thirty of which were registered data brokers. [5]

[2] "2022 K-12 EdTech Safety Benchmark: National Findings – Part 1", December 13, 2022, Internet Safety Labs. https://internetsafetylabs.org/wp-content/uploads/2022/12/2022-k12-edtech-safety-benchmark-national-findings-part-1.pdf

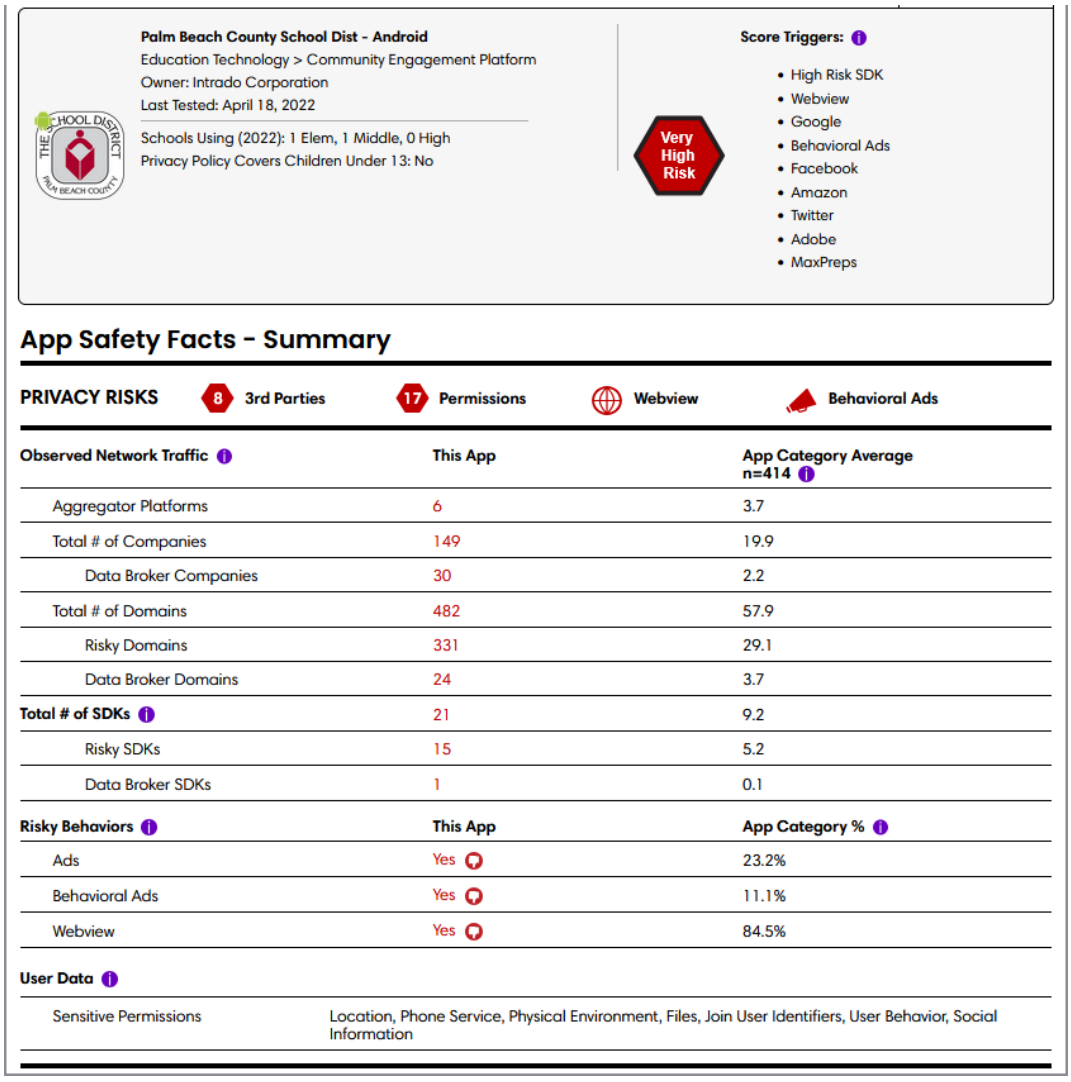
[3] "2022 K-12 EdTech Benchmark Findings Report 2: School Technology Practices & 3rd Party Certifications Analysis", June 27, 2023, Internet Safety Labs, https://internetsafetylabs.org/wp-content/uploads/2023/06/2022-K12-Edtech-Safety-Benchmark-Findings-Report-2.pdf

[4] Happily, this app is no longer available on the app stores.

[5] ISL believes the number of data brokers in the network traffic is significantly higher than this number due to the ineffective penalties in data broker laws, and due to deficiencies in current data broker laws.

INTERNET SAFETY //LABS

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



Palm Beach County School Dist - Android
Education Technology > Community Engagement Platform
Owner: Intrado Corporation
Last Tested: April 18, 2022

Schools Using (2022): 1 Elem, 1 Middle, 0 High
Privacy Policy Covers Children Under 13: No

Score Triggers:

Very High Risk

- High Risk SDK
- Webview
- Google
- Behavioral Ads
- Facebook
- Amazon
- Twitter
- Adobe
- MaxPreps

App Safety Facts - Summary

PRIVACY RISKS 8 3rd Parties | 17 Permissions | Webview | Behavioral Ads

Observed Network Traffic	This App	App Category Average n=414
Aggregator Platforms	6	3.7
Total # of Companies	149	19.9
Data Broker Companies	30	2.2
Total # of Domains	482	57.9
Risky Domains	331	29.1
Data Broker Domains	24	3.7
Total # of SDKs	21	9.2
Risky SDKs	15	5.2
Data Broker SDKs	1	0.1

Risky Behaviors	This App	App Category %
Ads	Yes	23.2%
Behavioral Ads	Yes	11.1%
Webview	Yes	84.5%

User Data	
Sensitive Permissions	Location, Phone Service, Physical Environment, Files, Join User Identifiers, User Behavior, Social Information

Figure 1: ISL Safety Label for Palm Beach County School District Android App, tested on 04/18/2022 https://appmicroscope.org/app/1579/

From our research, we can state definitively that the magnitude of commercial surveillance is staggering. Last year, we identified and researched the beating heart infrastructures that enable commercial surveillance at scale[6]. 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

[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

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 assert "cookieless tracking", and "personalized experiences for *visitors"*. Note, 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, 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 of IDRPs.[6]

Finally, the data collected by these surveillance infrastructures span digital sources and physical world sources and include highly sensitive data and inferences. Experian boasts of 1,900+ attributes per consumer[6].

Consent alone won't fix this problem. In fact, in the past week alone, ISL observed inaccurate information in two prominent edtech providers' privacy policies incorrectly stating that COPPA allows the schools to provide consent on behalf of the students. Consent is a deeply flawed approach to privacy protection. Indeed, in our 2022 benchmark, only 14% of schools evidenced any ability for parents or students to consent to technology use.[3]

Unfortunately, most state privacy laws do not do enough to protect people's privacy.[8] These laws, including the Virginia and Connecticut laws most often cited by

---

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

[8] *See* EPIC and U.S. PIRG Education Fund, *The State of Privacy 2025: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better* (Jan. 2025), https://epic.org/wp-content/uploads/2025/01/EPIC-PIRG-State-of-Privacy-2025.pdf.

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

industry as the "model" states should follow, simply cement the status quo into law – endless privacy policies filled with legalese that consumers don't read and don't have any choice but to agree to or not use the service. Massachusetts can do better.

Both the MCDPA and MDPA contain the most critical elements needed in any strong privacy bill: strong data minimization rules, restrictions on the sale of sensitive data, and strong enforcement mechanisms.

Data Minimization

The key with a data minimization provision is to ensure it is tied to the specific product or service requested by the individual, not simply to whatever purpose the collecting entity decides it wants to collect data for or discloses in their privacy policy. Most state privacy laws simply limit the collection and use of personal data to whatever purposes are "disclosed to the consumer." This maintains the status quo of long privacy policies that no one reads. A data minimization rule should instead require companies to better align their data practices with what the consumer expects. A flashlight app doesn't need your location data. Social media companies shouldn't know every click I make online, even outside their services.

In 2022, ISL published ten principles for safe software and Principle #4 is Data Collection Minimization where data collection must be proportional to the deal being established between the product and the consumer. This kind of contextual proportionality is vital for meaningful data minimization, and we are happy to see alignment in both MCDPA and MDPA.

The MCDPA and MDPA require that entities only collect, use, and transfer data that is "*reasonably necessary and proportionate*" to provide or maintain a product or service requested by the consumer. This rule will encourage companies to innovate to find more privacy-protective ways of doing business and cut down on data abuse. One of the easiest and best ways to keep people safe when using digital products is to collect/observe/and derive less personal information

Restrictions on the sale of sensitive data

The MCDPA and MDPA both set heightened protections for sensitive data (i.e., biometrics, location, health data) such that it cannot be used for advertising purposes. Selling of sensitive personal data has been shown repeatedly to present physical, emotional, and reputational risks to individuals and groups. ISL believes personal data markets are profoundly risky to individuals and societies—and especially to children. The proposed H.78 definition of sensitive data and prohibition of the sale of it is an excellent

INTERNET SAFETY LABS

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

start to keep everyone safer, a protection included in the recently enacted Maryland Online Data Privacy Act that we urge Massachusetts to adopt.

Strong enforcement

Enforcement by both Attorneys General and a private right of action allowing consumers to enforce their rights is critical to ensuring that privacy laws are complied with. Just last week, Consumer Reports released a report showing that a key provision of many state privacy laws – the right to opt-out of targeted advertising and the sale of your data – is simply being ignored in many cases.[9] They reported:

> Of the 40 retailers we tested, 12 (30 percent) appeared to serve us targeted ads on other websites despite our sending of [a signal called "Global Privacy Control" indicating they wanted to opt-out] with every web request. In practical terms, this means that consumers' personal data may be sold or shared with third parties even when they've taken the appropriate steps to protect themselves.

Without a private right of action, consumers are powerless to do anything to push back against this non-compliance with the law unless the Attorney General takes up the case. Data abusers know that Attorney General resources are limited and therefore the chance of enforcement is low. Massachusetts consumers have had the right to bring a lawsuit for violations of their consumer rights under Chapter 93A for decades – there is no reason that the rules should be different for the consumer rights provided in a privacy bill.

We ask that the Committee give a favorable report to a strong comprehensive privacy bill like the MCDPA or MDPA that contains at minimum these three critical protections. Given the particular harms that stem from the sale of location data, we also ask that the Committee give a favorable report to H.86/S.197, the Location Shield Act in the event that the Legislature is not willing to move forward on an omnibus privacy bill.

Thank you for the opportunity to testify. We are at your service for any further clarifications or data. We appreciate the Committee's leadership on this critical issue.

---

[9] Consumer Reports, *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws* (Apr. 2025), https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf.

INTERNET
SAFETY
LABS

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

Sincerely,

Lisa LeVasseur
Executive Director & Research Director
Internet Safety Labs