

May 3, 2025

Judiciary Committee

Re: Testimony in Support of LD 1822, An Act to Enact the Maine Online Data Privacy Act

Dear Members of the Committee:

I am writing on behalf of Internet Safety Labs in support LD 1822, An Act to Enact the Maine Online Data Privacy Act.

Internet Safety Labs (ISL) is a non-profit digital product safety testing organization and has been assessing and reporting on safety risks (including privacy risks) since 2019. We conduct independent safety research and 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 or other notices.

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 privacy 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/>).

Figure 1 shows an example of the worst/leakiest app from our 2022 benchmark¹. Note that there were 149 unique companies observed in the app's network traffic flow, thirty of which were registered data brokers.²

¹ Happily, this app is no longer available on the app stores.

² 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.

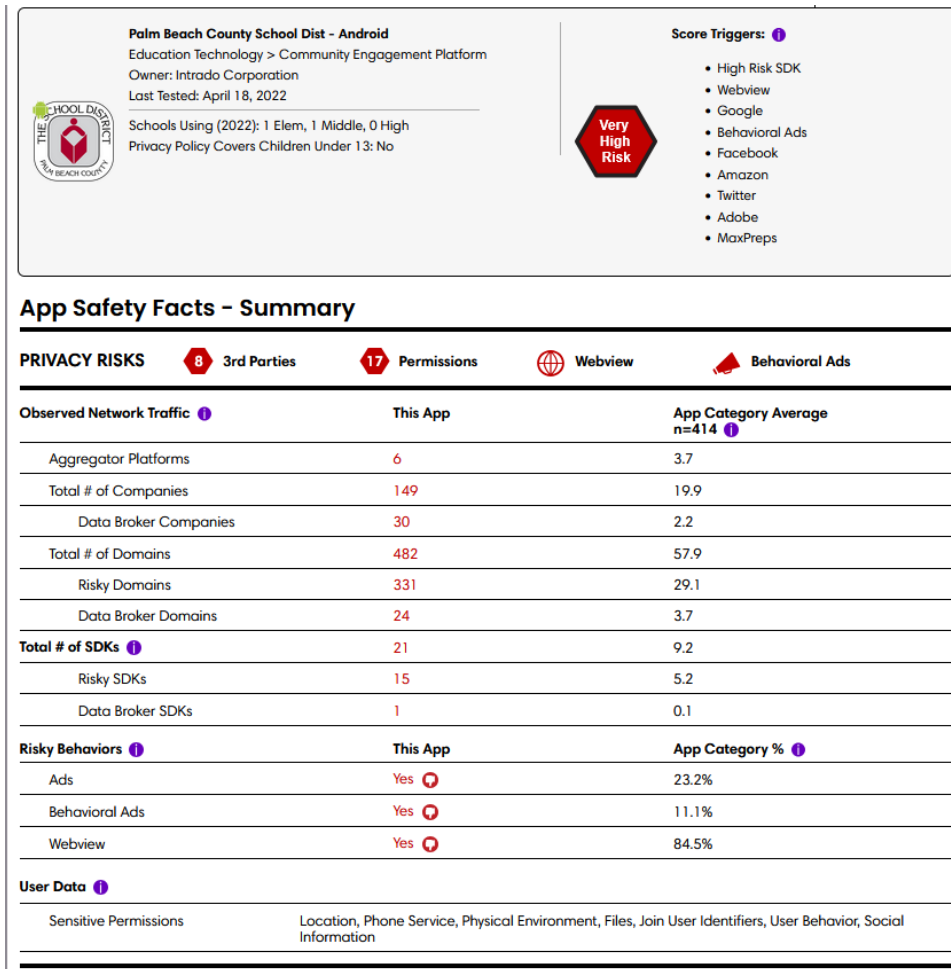


Figure 1: ISL Safety Label for Palm Beach County School District Android App, tested on 04/18/2022.

From our research, we can state definitively that commercial surveillance is ubiquitous and the scale staggering. Last year, we identified and researched the foundational infrastructure that enables commercial surveillance at scale³. 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. ISL tracked 93 identity resolution platforms and 246 customer data platforms, and 20 companies that provide both types of platforms worldwide⁴. Only 16.4% of these platforms were registered data brokers, whereas it’s highly likely that many more of them should be. Note also that these platforms

³ “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>

⁴ <https://internetsafetylabs.org/resources/references/identity-resolution-and-customer-data-platform-companies/>

indiscriminately Hoover up and monetize personal data without regard to age. 539 (35%) of the K-12 apps in our 2022 research sent data to these commercial surveillance platforms.

As of today, the CDP Institute shows hundreds of CDPs with education data, non-profit data, and disturbingly, healthcare data. In preparing these comments, we found 350 CDPs with healthcare data, 37 of which also perform unique person identification (identification resolution).⁵

ISL constantly assesses these platforms and their sites proudly assert “cookieless tracking”, and “personalized experiences for *visitors*”. Note, this is a deliberate word choice; not customers but visitors⁶. There is nearly no place online where we aren’t being tracked.

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, including Google and Meta. 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 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 IDRs^{3,7}.

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 consumer³.

Consent alone won’t fix this problem. In fact, in recent research, 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 fails as privacy protection.

LD 1822: Prohibiting Risky Data Practices

We are pleased to see that LD 1822 provides two crucial measures to make digital products safer. First, a limitation on the collection of sensitive personal information. In 2022, ISL published ten principles⁸ 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. One of the easiest and best ways to keep people safe when using digital products is to collect/observe/and derive less personal information.

Secondly, prohibition on the sale of sensitive personal data is a much needed and profoundly important measure and we’re happy to see it in LD 1822. Selling of sensitive personal data has been shown repeatedly to present physical, emotional, and reputational risks to individuals and groups. ISL believes

⁵ <https://www.cdpinstitute.org/vendors/>

⁶ Here’s one example IDRP: <https://getuntitled.ai/blog/website-visitor-tracking-software/>

⁷ <https://internetsafetylabs.org/resources/references/identity-resolution-and-customer-data-platforms-found-in-2022-edtech-benchmark-network-traffic/>

⁸ <https://internetsafetylabs.org/resources/specifications/principles-of-safe-software/>

personal data markets are profoundly risky to individuals and societies—and especially to children. The proposed LD 1822 robust definition of sensitive data in conjunction with the prohibition of the sale of it is an excellent start to keep everyone safer.

ISL also supports the list of “processing activities that present a heightened risk of harm to a consumer” in section 9611, Data protection assessment.

Finally, ISL appreciates the specifications to ensure that downstream processors uphold both the user’s and the controller’s data processing requirements.

LD 1822: Concerns

- **FERPA data exception:** While we’re glad to see the wholesale prohibition of the sale of personal information of minors, we are concerned about excluding data covered under FERPA. Edtech and other technology used by K-12 students is under-scrutinized when it comes to *actual* data sharing behaviors. Schools often don’t have the technical resources to assess claims from edtech vendors and instead take them at their word⁹. In 2024, ISL compared 84 edtech and educational apps against the data processing agreements made between tech vendors and local education agencies (LEAs; schools, districts, and state level entities). Only 12% of the studied apps with data processing agreements (DPAs) accurately listed all the data elements collected by the app in practice¹⁰. 44% of the DPAs failed to correctly identify the 3rd parties receiving the data. Finally, 55% of the apps with DPAs were found to be sending data to adtech entities. (Note that this doesn’t always mean that ads or behavioral ads were observed in the apps.) In short, FERPA doesn’t effectively serve to minimize risky student data sharing.
- **Excluded businesses:** ISL believes that *all* institutions should be held to strict personal data privacy protections. **Non-profit organizations:** Non-profit entities like the AARP, political action committees, and churches hold volumes of sensitive information that can—and is—weaponized. Non-profits should not be excluded from privacy protections, particularly prohibiting the sale of sensitive personal data. **Medical apps:** LD 1822 seems to defer to privacy protections provided by HIPAA. We are in the early stages of conducting research on medical apps and from our preliminary results, we have reason to believe that “HIPAA compliant” apps are sharing personal data sharing with marketing and advertising entities. As noted earlier, there is a sizeable market for healthcare data

⁹ Only 29% of the 663 schools studied had evidence of broad scale vetting of technologies being recommended to students. “2022 K-12 EdTech Benchmark Findings Report 2: School Technology Practices & 3rd Party Certifications Analysis”, pg. 29, Internet Safety Labs, June 27, 2023.

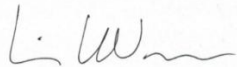
¹⁰ As detected by our testing and review of actual network traffic from the app.

and despite regulations, this highly sensitive information is being trafficked.

Higher Education: While our sample set of studied universities and colleges is small yet (only 17 schools), we found evidence of data monetization in at least one¹¹ which also claims that contact information is non-sensitive. However, email addresses—even when hashed-- can uniquely identify people.¹²

- **Opting out of data selling:** We understand the tradition of this legal precedent and also appreciate the existence of the Global Privacy Control¹³ (GPC) mechanism for opting users out, but the safest option is for consumers to opt *into* data selling. Data monetization creates unacceptable privacy risks to consumers and violates ISL Safe Software Principle #5: Private by Default¹⁴. Moreover, research confirms that users rarely modify default settings in apps and websites¹⁵.

Thank you for the opportunity to testify. ISL, our empirical research, and reference tools are at your service. We appreciate the Committee's leadership on this critical issue.



Lisa LeVasseur
Executive Director & Research Director
Internet Safety Labs

¹¹ <https://www.devry.edu/compliance/notice-of-right-to-opt-out.html>

¹² Even when hashed, emails can be, through probabilistic identification methods, used as a unique personal identifier. <https://www.adexchanger.com/ad-exchange-news/burning-a-hole-in-the-invincibility-of-email-hashing/>

¹³ <https://globalprivacycontrol.org/>

¹⁴ <https://internetsafetylabs.org/resources/specifications/principles-of-safe-software/>

¹⁵ <https://www.cnet.com/tech/tech-industry/default-settings-for-privacy-we-need-to-talk/>