epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@epic.org
https://epic.org

May 5, 2025

The Honorable Anne Carney, Senate Chair
The Honorable Amy Kuhn, House Chair
Maine State Legislature Judiciary Committee

Dear Chair Carney, Chair Kuhn, and Members of the Committee:

EPIC writes in support of LD 1822, An Act to Enact the Maine Online Data Privacy Act, because it would provide critical protections Mainers need to stay safe online. We also write in opposition to LD 1224, LD 1088, and LD 1284 because they fail to accomplish that goal. The Electronic Privacy Information Center (EPIC) is a nonprofit research organization established in 1994 to secure the fundamental right to privacy in the digital age for all people. EPIC has long advocated for strong privacy laws at the state and federal levels and was heavily involved in last session's deliberations on a data privacy bill in Maine.[1]

LD 1822 builds on existing state privacy laws already enacted in nineteen states and incorporates essential provisions to provide Mainers with the protections they need to stay safe online. Key provisions of LD 1822 include:

- **Data minimization:** LD 1822 limits the unfettered collection of personal data by setting a baseline requirement that entities only collect personal data that is reasonably necessary to provide or maintain a product or service requested by the consumer.
- **Strong protections for sensitive data:** LD 1822 sets heightened protections for sensitive data like biometrics, location, and health data such that its collection and use must be strictly necessary for the product or service the consumer requests, and it may not be sold.
- **Preventing discrimination:** LD 1822 extends civil rights to online spaces by prohibiting entities from processing data in a way that discriminates or otherwise makes unavailable the equal enjoyment of goods and services on the basis of race, color, religion, national origin, sex, sexual orientation, gender, or disability.
- **Protections for children and teens:** LD 1822 prohibits targeted advertising to minors and bans the sale of minors' data.

In my testimony, I will discuss why it is so critical that Maine enact a strong privacy law, the current state of state privacy laws, and go into detail on a few key protections that are crucial to keep Mainers safe online. I also include an attachment with a few suggested amendments to the bill.

[1] *See* e.g. EPIC, *The State Data Privacy Act: A Proposed Model State Privacy Bill,* https://epic.org/the-state-data-privacy-act-a-proposed-model-state-privacy-bill/.

Data Abuse Harms Mainers

Advertisers and data brokers track our every move online and our data is constantly used against us, harming our wallets, opportunities, and rights. Examples of these harms include:

1. **Increased insurance premiums.** Texas Attorney General Ken Paxton recently sued insurance giant Allstate for unlawfully collecting, using, and selling Texans' location data through secretly embedded software in mobile apps such as Life360 and GasBuddy. Paxton alleged that Allstate and other insurers then used the covertly obtained data to justify raising Texans' insurance rates.[2]
2. **Increased pricing on consumer goods**. The Federal Trade Commission recently found that retailers frequently use people's personal information to set targeted, tailored prices for goods and services—from a person's location and demographics, down to their mouse movements on a webpage.[3]

Small businesses are harmed by these systems as well. As Check My Ads, an advocacy group formed by former advertising industry employees recently wrote to Congress:

> Privacy legislation that emphasizes data minimization and transparency leads to higher-quality, more relevant data. Right now, the advertising supply chain is bloated with third-party data—often inaccurate, outdated, or collected without meaningful consent. Acxiom, one of the world's largest data brokers, even admitted their consumer data is made up of "informed guesses," with the hope it doesn't lead to credit denial or other harm. This kind of data is not only unreliable—it wastes ad spend. Privacy-focused frameworks should encourage a shift to first-party data—information voluntarily shared by users—delivering more accurate, context-rich insights. Advertising that uses high-quality data performs better. With privacy legislation in place to curb harmful data practices and enforce consent, advertisers gain access to permissioned, engaged audiences—the kind that convert and stay loyal.[4]

These economic harms are on top of the harms to our rights. Last year, Senator Ron Wyden found that Near, a location data broker, sold location data to an anti-abortion organization who used it to target misinformation and ads to people who visited reproductive health clinics, including in Maine.[5]

---

[2] Press Release, Att'y Gen. of Texas, *Att'y Gen. Ken Paxton Sues All-state and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Cos.* (Jan 13, 2025), https://www.texasattorneygeneral.gov/news/releases/attorney-general-ken-paxton-sues-allstate-and-arity-unlawfully-collecting-using-and-selling-over-45.

[3] FTC, *FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices* (Jan. 2025), https://www.ftc.gov/news-events/news/press-releases/2025/01/ftc-surveillance-pricing-study-indicates-wide-range-personal-data-used-set-individualized-consumer.

[4] Letter from Check My Ads to House Energy & Commerce Comm. Privacy Working Group 8 (Apr. 2025), https://checkmyads.org/wp-content/uploads/2025/04/Privacy-Working-Group-RFI-Check-My-Ads-Submission.pdf.

[5] Press Release, Sen. Ron Wyden, *Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics* (Feb. 2024), https://www.wyden.senate.gov/news/press-releases/wyden-reveals-phone-data-used-to-target-abortion-misinformation-at-visitors-to-hundreds-of-reproductive-health-clinics.

The State of State Privacy Law: Existing Laws Don't Do Enough

Because there is no federal comprehensive privacy law, states have been enacting laws to fill this void. Since 2018, 19 states have passed comprehensive privacy laws. EPIC and U.S. PIRG recently released a report grading these laws.[6] Nearly half failed, and none received an A. These laws do little to limit mass data collection and abuse.

Many of these state laws closely follow a model initially drafted by tech giants.[7] This draft legislation was based on a privacy bill from Washington state that was modified at the behest of Amazon, Comcast, and Microsoft.[8] An Amazon lobbyist encouraged a Virginia lawmaker to introduce a similar bill, which became law in 2021. Unfortunately, this Virginia law became the model that industry lobbyists pushed other states to adopt. In 2022, Connecticut passed a version of the Virginia law with some additional protections, which has now become the version often pushed by lobbying groups doing the bidding of Big Tech companies in select states. **Privacy laws should not be written by the very companies they are meant to regulate.**

Laws based on industry's model bill, which includes LD 1224 and LD 1088, do not meaningfully limit what data companies can collect or what they can do with that data — they merely require that companies disclose these details in their privacy policies, which consumers rarely read. Companies should not be allowed to determine for themselves what are the permissible purposes of collecting and using consumers' personal information. Unfortunately, the limitations on data collection in LD 1224 and LD 1088 allow companies to do just that. They read:

> *A controller shall limit the collection of personal data to what is adequate, relevant and reasonably necessary in relation to the purposes for which the data is processed, as disclosed to the consumer.*

This reinforces the failed status quo of "notice and choice" — businesses can list any purpose they choose in their privacy policies, knowing that very few consumers will read them. In fact, it incentivizes companies to list as many purposes as possible, and as broadly as possible, to cover every conceivable reason they would ever want to collect your data. And the only "choice" the consumer has is to not use the service at all. The clearer limits on data collection in LD 1822 are critical because they require companies to better align their data practices with what consumers expect, allowing Mainers to use online services without being forced to sacrifice their privacy.

---

[6] EPIC and U.S. PIRG Edu. Fund, *The State of Privacy: How State "Privacy" Laws Fail to Protect Privacy and What They Can Do Better,* EPIC and U.S. PIRG (Jan. 2025), https://epic.org/state-of-privacy-2025/.
[7] Jeffrey Dastin, Chris Kirkham & Aditya Kalra, *Amazon Wages Secret War on Americans' Privacy, Documents Show*, Reuters (Nov. 19, 2021), https://www.reuters.com/investigates/special-report/amazon-privacy-lobbying/.
[8] Emily Birnbaum, *From Washington to Florida, Here Are Big Tech's Biggest Threats from States*, Protocol (Feb. 19, 2021), https://www.protocol.com/policy/virginia-maryland-washington-big-tech; Mark Scott, *How Lobbyists Rewrote Washington State's Privacy Law* (Apr. 2019), https://www.politico.eu/article/how-lobbyists-rewrote-washington-state-privacy-law-microsoft-amazon-regulation/.

Data Minimization, Sensitive Data Protections, and Strong Enforcement: The Keys to a Strong Privacy Law

Data Minimization

LD 1822 relies on a concept that has long been a pillar of privacy protection: data minimization. When consumers interact with a business online, they reasonably expect that their data will be collected and used for the limited purpose necessary to provide the goods or services that they requested. For example, a consumer looking up symptoms on WebMD does not expect that what they're reading is sent in the background to Meta, Google, and over a dozen advertisers, but that's exactly what's happening right now.

To incentivize better data practices, LD 1822 set a baseline requirement that entities only collect data that is "*reasonably necessary and proportionate*" to provide or maintain a product or service requested by the consumer. This standard is referred to as "data minimization" and it better aligns business practices with what consumers expect.

The rule in LD 1822 is modeled on the rule in the Maryland Online Data Privacy Act, which was enacted last year. It is not as strict as the rule advanced by this Committee last session. It doesn't go far as privacy advocates would like – we prefer that data minimization rules cover both how much data a company can collect *and* how they can use that data. LD 1822 takes a compromise position and applies to collection only, which mirrors the rule in Maryland's law. Data minimization offers a practical solution to a broken internet ecosystem by providing clear limits on how companies can collect and use data.

A Ban on the Sale of Sensitive Data Prevents Some of the Worst Data Harms

LD 1822 sets heightened protections for sensitive data such that its collection and use must be *strictly necessary* to provide the product or service the consumer is asking for. This is a critical provision that protects the data we all consider to be the most sensitive, such as our location, health, and financial data. It also bans the sale of sensitive data entirely. Both of these rules are included in the recently enacted Maryland Online Data Privacy Act.

Many an app has likely prompted you to request access to your location. Sometimes, the app has a legitimate reason to access the information, like displaying your local weather. Sometimes, it doesn't. In either case, the app may be selling your location data to a third party. A top Catholic Church official was forced to resign a few years ago after a Catholic media site used cellphone data to show that the priest was a regular user of the queer dating app Grindr and visited gay bars.[9]

[9] Michelle Boorstein et al., *Top U.S. Catholic Church Official Resigns After Cellphone Data Used to Track Him on Grindr and to Gay Bars*, Wash. Post (July 21, 2021), https://www.washingtonpost.com/religion/2021/07/20/bishop-misconduct-resign-burrill/.

The recent bankruptcy of genetic testing company 23andMe further highlights the need for heightened protections for sensitive data. 23andMe has genetic data on 15 million customers, so a massive amount of highly sensitive information—now 23andMe's most valuable asset—will be sold off to the highest bidder. After a federal judge gave permission for the company to sell its sensitive customer data, millions of customers have no control over who their information is sold to. While research shows that most Americans believe—incorrectly— that the personal health information they give to health apps and websites is protected by the Health Information Portability and Accountability Act (HIPAA), the law does not apply to 23andMe's handling of consumer genetic information. I suggest an amendment in the enclosure to ensure sensitive data is protected in the case of a merger or bankruptcy.

Enforcement is Critical

Robust enforcement is critical to effective privacy protection. Strong enforcement by state government via Attorney General authority is an essential component of a strong privacy law. Funds should be appropriated to ensure the Attorney General can meaningfully enforce the law, particularly in the absence of a private right of action to supplement state enforcement.

* * *

EPIC also asks you to oppose LD 1284, which would repeal Maine's ISP privacy law. We feel that the law's protections are still critical even if a comprehensive privacy law is enacted in Maine because of the unique relationship between a consumer and their broadband service provider.

* * *

LD 1822 is not a privacy advocate's ideal bill. EPIC would prefer that the data minimization rule cover data use in addition to collection. We'd like to see a private right of action included so that individuals can enforce their rights under the law. We'd prefer that the bill cover non-profits. But LD 1822 reflects a compromise that would provide Mainers with important privacy protections that they lack today and is the most consumer-friendly privacy bill before this Committee. EPIC asks that you to support LD 1822 and oppose LDs 1224, 1088, and 1284. I am happy to be a resource to the Committee as it navigates this issue.

Sincerely,

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
Deputy Director, EPIC

Encl.

EPIC's Suggested Amendments

1. **Delete §9808(1)(G), which conflicts with the data minimization rule**
   §9808(1)(G) refers to obtaining consent for purposes that are not disclosed in the privacy policy, which conflicts with the data minimization provision in §9808(1)(A) limiting data collection to what is reasonably necessary and proportionate to provide or maintain the specific product or service requested by the consumer. It is unclear how these two provisions would work together, but at worst it provides a loophole for companies to simply ask for consent for any data use they desire. Consent has been proven to be an ineffective way to protect privacy.

2. **Confirm that controllers must offer universal opt-out mechanism**
   §9808(6)(C) appears to give controllers the option of providing an opt-out link or allowing consumers to opt-out via a universal opt-out preference signal. This conflicts with §9607(2), which gives consumers the right to exercise their opt-out rights via a global device setting. And nearly every other state that has a universal opt-out mechanism (including CT and NH) require both an opt-out link ***and*** the option of a universal opt-out preference signal.

   EPIC asks that you change the "or" to an "and" in line 28 on page 14, which would mirror CT, NH, and most other state laws.

3. **Ensure sensitive data such as genetic data is protected in mergers and bankruptcy sales**
   The recent bankruptcy of genetic testing company 23andMe revealed loopholes in many state privacy laws that fail to protect consumers from the sale of their sensitive data in the event of a merger, acquisition, or bankruptcy.[10] An exemption in the definition of "sale" that excludes the transfer of data during a bankruptcy proceeding renders consumers' right to opt out of data sales useless in terms of 23andMe's sale resulting from bankruptcy. California amended its privacy law last year to remove this exemption and clarify that consumers can opt out of the sale of their data even in the context of a bankruptcy proceeding.[11]

   To provide protections for Mainers in these situations, we recommend (1) striking subsection (B)(6) from the definition of "sale" and (2) adding the following to the exemptions in §9613(1):

   > L. Transfer assets to a third party in the context of a merger, acquisition, bankruptcy or similar transaction when the third party assumes control, in whole or in part, of the controller's assets, only if the controller, in a reasonable time prior to the transfer, provides an affected consumer with:
   >
   > (A) A notice describing the transfer, including the name of the entity receiving the consumer's personal data and the applicable privacy policies of such entity and
   >
   > (B) a reasonable opportunity to:
   >
   > (i) withdraw previously provided consent related to the consumer's personal data, and
   >
   > (ii) request the deletion of the consumer's personal data;

[10] Kara Williams, *Concern over Potential 23andMe Data Sale Highlights Weaknesses of State Privacy Laws* (May 2, 2025), https://epic.org/concern-over-potential-23andme-data-sale-highlights-weaknesses-of-state-privacy-laws/.
[11] Cal. Assembly Bill No. 1824 (2024), https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=202320240AB1824.

4. **Remove addition to "publicly available information" definition that opens loophole**
"Publicly available information" is exempted from coverage of the bill, so it is critical that it is defined as narrowly as possible. LD 1822 proposes adding a provision that includes in the definition any information about a consumer that a person "obtains from a person to whom the consumer disclosed the information unless the consumer has restricted the information to a specific audience."

   This addition is a dangerous extension of the definition and a big loophole in our view -- it would make a wide swath of information publicly available in a way that many consumers wouldn't expect to be. And in many instances, consumers might not even have the ability to restrict the audience. For example, this would mean any time a consumer provides data to a company (e.g. signing up for an account or filling out an application) and doesn't limit the audience, it is public information and exempt from coverage under the law.

   It seems more like this should instead be an exemption to the definition, i.e. "Publicly available information" does not include information that the consumer has restricted to a specific audience." That would be our preference but at minimum, EPIC would ask that it be amended to match the language in last session's Committee bill, which reads:

   > A website or online service made available to all members of the public, either for free or for a fee, including a website or online service in which all members of the public can log on to the website or online service either for free or for a fee, unless the individual who made the information available via the website or online service has restricted the information to a specific audience.

5. **Add definition of "minor"**
There is no definition of "minor" in the bill. The summary indicates that it is meant to be under 18 years of age, but there's no definition of it in the bill.