CENTER FOR DEMOCRACY & TECHNOLOGY

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

in Opposition to
LD 1224, An Act to Comprehensively Protect Consumer Privacy,
LD 1088, An Act to Enact the Maine Consumer Data Privacy Act, and
LD 1284, An Act to Repeal Provisions of Law Governing the Privacy of Broadband Internet Customer Personal Information.

Eric Null, Co-Director, Privacy & Data Program
Center for Democracy & Technology
Washington, DC

Before the Maine State Legislature
Hearing of the Judiciary Committee
Monday, May 5, 2025

Members of the committee, thank you for allowing me to provide feedback in support of LD 1822, An Act to Enact the Maine Online Data Privacy Act, and in opposition to three other privacy bills: LD 1224, LD 1088, and LD 1284.

My name is Eric Null, I am the co-director of the privacy & data program at the Center for Democracy & Technology, a thirty-year-old nonpartisan, nonprofit organization focusing on protecting individual rights, civil rights, and civil liberties in the digital age.

In this testimony, I will first focus on why CDT supports LD 1822, specifically because it moves us beyond the notice-and-consent regime to a true data minimization regime. Then, I will discuss a few ways it could still be improved. Last, I will discuss why Maine should not pass the three other privacy bills you are considering today, including repeal of its broadband privacy law.

One of the primary goals of privacy legislation should be to move beyond the failed notice-and-consent regime, which has been dominant since the 1990s, has allowed a free-for-all on data collection and processing, and ultimately places the burden of reviewing privacy policies and protecting privacy on already-overburdened individuals. We know people do not view privacy policies as effective or useful.[1] We know people do not read privacy policies.[2] And we know that reading privacy policies, even if people wanted to, would require hundreds of hours per year.[3] As a result, people have a sense of futility in privacy and feel a lack of control over privacy risks, and they often underestimate the risks of disclosing data.[4]

Data minimization, on the other hand, shifts the primary privacy burden to the companies who benefit most from the collection and exploitation of data by requiring their to justify their data practices as necessary to provide their products or services, or

[1] Sixty-one percent of adults consider privacy policies to be an ineffective way for companies to explain data practices, and almost seventy percent consider privacy policies to be just something to "get past." Colleen McClain *et al*, *How Americans View Data Privacy*, Pew Research Center (2023), https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy.

[2] Fifty-six percent of American adults say they agree to privacy policies without reading them, compared to only eighteen percent who say they rarely or never agree without reading. *Id.*

[3] A 2008 study estimated that people would spend 244 hours per year, or forty minutes a day, reading privacy policies if they read all policies that apply to them. Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, I/S: A Journal of Law and Policy for the Information Society 540, 560 (2008), https://www.technologylawdispatch.com/wp-content/uploads/sites/26/2013/02/Cranor_Formatted_Final1.pdf. Privacy policies have only gotten longer since. Ryan Amos *et al*, *Privacy Policies Over Time: Curation and Analysis of a Million-Document Dataset*, In Proceedings of the Web Conference (2021), https://arxiv.org/pdf/2008.09159.

[4] Wenjun Wang *et al.*, *An Exploration of the Influencing Factors of Privacy Fatigue Among Mobile Social Media Users From the Configuration Perspective*, Scientific Reports (2025), https://www.nature.com/articles/s41598-024-84646-z.

as fitting into another permissible purpose.[5] It also helps prevent privacy harms at the outset because data a company does not have cannot lead to downstream harm through misuse, unauthorized access, disclosure to third parties including law enforcement, or some other harmful action. Data minimization has bipartisan support: a recent Consumer Reports survey found that seventy-two percent of Republicans and seventy-nine percent of Democrats "support a law that limits companies to using only the data they need to provide their service."[6]

LD 1822 includes strong data minimization provisions by limiting collection of non-sensitive data to that which is reasonably necessary to provide a product or service,[7] and by limiting collection, processing, and sharing of sensitive data to that which is strictly necessary to provide a product or service.[8] These requirements help prevent boundless data collection practices, and they help avoid further saddling consumers with the burden of consenting to every data practice engaged in by every company they interact with. Similar requirements have already passed in Maryland, where they will come into effect in October 2025.

Two other Maine bills, LD 1224 and LD 1088, would change very little about privacy practices. The requirement in those bills for "data minimization," if you can call it that, is weak. For non-sensitive data, companies can collect data reasonably necessary to any disclosed purpose–in other words, anything in the lengthy privacy policies that people don't read. That is already a restatement of deceptive trade practices law,[9] and is actually weaker, because the latter's limits apply to all data practices (use, disclosure) as well as collection. For sensitive data, the only limits are on processing: companies can process sensitive data only with opt-in consent. While opt-in consent for processing sensitive data may be better than nothing, it is not better than the minimization provisions in LD 1822. Overall, these requirements are not privacy *protections* as much as privacy *burdens*, shouldered again by the consumer.

There is, of course, room for improvement in LD 1822. First, the minimization protections for non-sensitive data apply only to collection, but they should also apply to processing and sharing. If the limits do not apply to those practices, a company may be

---

[5] Eric Null, *States Are Letting Us Down on Privacy*, Center for Democracy & Tech. (Jan. 28, 2024), https://cdt.org/insights/states-are-letting-us-down-on-privacy.
[6] Scott Medintz, *Americans Want Much More Online Privacy Protection Than They're Getting*, Consumer Reports (Nov. 20, 2024), https://www.consumerreports.org/electronics/privacy/americans-want-much-more-online-privacy-protection-a9058928306.
[7] §9608(2)(A).
[8] §9608(1)(A).
[9] *See generally*, FTC Statement on Deception, FTC (Oct. 14, 1983), https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf.

limited in its initial collection of data, but it would generally be free to process or share non-sensitive data for any purpose unrelated to the product or service.

Second, the knowledge standard is not properly calibrated. CDT has historically been concerned with language surrounding "knowing" the age of internet users because of the potential for that language to incentivize or even force companies to institute privacy-invasive age-assurance and age-verification techniques.[10] LD 1822 applies additional protections to users a company knows or "reasonably should know" a user is a minor. That standard is likely to *reduce* privacy and anonymity online, because companies may feel compelled to comply with those provisions by requiring all users to upload identifying documentation showing their age when normally that information would be kept private. We urge that the bill be amended to rely on a "knowledge fairly implied under objective circumstances" standard, as that standard is less likely to incentivize companies to adopt across-the-board age verification techniques.

Third, privacy laws are only as strong as their enforcement, and they should be enforced through multiple channels. LD 1822 includes Attorney General enforcement, but explicitly disallows the private right of action that already exists in Maine's Unfair Trade Practices law, which is itself limited to actual damages and equitable relief. Without that private right of action, the bill would lead to perverse results: a Maine resident who finds themselves subject to identity theft, physical danger, harassment, or some other harm because of the data practices of a company may not be able to hold that company accountable under the privacy law. Attorney General enforcement is not sufficient to make that Maine resident whole.

If Maine insists on placing the entire enforcement burden on the Attorney General's office, it should at least ensure the office is appropriated enough funds to build a dedicated team, like in Texas.[11]

Finally, CDT opposes LD 1284, the bill to repeal Maine's broadband privacy law, particularly given LD 1822 includes a carve-out for broadband providers. Back in 2016, the Federal Communications Commission passed a nationwide rule protecting the

[10] See Letter from CDT et al. to Majority Leader Schumer et al., Opposition to S. 3663's Threats to Minors' Privacy and Safety Online, Nov. 28, 2022, at 2 https://cdt.org/wp-content/uploads/2022/11/Coalition-letter-opposing-Kids-Online-Safety-Act-28-Nov-PM.pdf ("Service providers will thus face strong incentives to employ age verification techniques to distinguish adult from minor users, in order to apply these strict limits only to young people's accounts. Age verification may require users to provide platforms with personally identifiable information such as date of birth and government-issued identification documents, which can threaten users' privacy, including through the risk of data breaches, and chill their willingness to access sensitive information online because they cannot do so anonymously.").

[11] Texas built a $5 million privacy-specific enforcement team and they have been out ahead on enforcement efforts. Cobun Zweifel-Keegan, *A View from DC: the Price of Privacy Enforcement*, IAPP (Feb. 28, 2025), https://iapp.org/news/a/a-view-from-dc-the-price-of-privacy-enforcement.

privacy of broadband subscribers, a significant win for consumers. The rule was simple: broadband providers could use and disclose data for service-related purposes (or pursuant to other narrow exceptions), but other, non-service-related uses required consent from the subscriber.[12] That rule, despite its sensible and beneficial privacy protections, was unfortunately overturned in 2017 by Congress under the Congressional Review Act, which also prevents the agency from adopting "substantially similar" rules without Congressional approval.[13] In the aftermath, Maine was the only state courageous enough to adopt a similar law (with a unanimous vote in the Senate and bipartisan support overall[14]) to protect Maine residents against the exploitation of data collected by broadband providers and used for marketing and other unrelated purposes. Those protections are purpose-built for broadband providers and make sense in that context. Maine should not repeal those protections.

[12] In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services, Dkt. No. 16-106, Report and Order, Oct. 27, 2016, https://docs.fcc.gov/public/attachments/FCC-16-148A1.pdf (App'x A).
[13] *Congress Has Repealed the FCC's Privacy Rules – Now What?*, Cooley (Mar. 29, 2017), https://www.cooley.com/news/insight/2017/2017-03-29-congress-repeals-fccs-privacy-rules.
[14] *Governor Mills Signs Internet Privacy Legislation*, State of Maine (June 6, 2019), https://www.maine.gov/governor/mills/news/governor-mills-signs-internet-privacy-legislation-2019-06-06