May 12, 2025

Chair Anne Carney
Chair Amy Kuhn
Joint Standing Committee on the Judiciary
Maine Legislature
100 State House Station
Room 438
Augusta, ME 04333

Re: Maine L.D. 1822, Maine Data PrivacyProtection Act — *SUPPORT*

Dear Chair Carney and Chair Kuhn,

Consumer Reports[1] strongly supports L.D. 1822, which would provide Maine consumers with privacy protections matching those in some of the strongest state laws passed to-date. The bill would require businesses to abide by meaningful data minimization provisions, which would prevent them from collecting information that is not reasonably necessary to provide the specific product or service requested by consumers. It would also extend to Maine consumers important new protections relating to their personal information, including prohibitions against collecting, processing, or sharing sensitive data unless it is strictly necessary, a ban on the sale of sensitive data, restrictions against targeting advertisements to children, and more.

These provisions largely reflect the last several years of work on privacy legislation around the states, adopting targeted improvements made in other state privacy laws that incorporate feedback from regulators tasked with enforcing these laws,[2] as well as other key stakeholders.

---

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

[2] Connecticut Attorney General, Report to the General Assembly's Joint General Laws Committee, February 1, 2024, https://portal.ct.gov/-/media/ag/press_releases/2024/ctdpa-final-report.pdf?rev=8fbba0ba237a42748d3ad6544fd8228c&hash=41BCE2F7485413487EE5F534E6AC6C60; Connecticut Attorney General, Updated Enforcement Report Pursuant to Connecticut Data Privacy Act, April 17, 2025,

Under current law, consumers possess very limited power to protect their personal information in the digital economy, while online businesses operate with virtually no limitations as to how they collect and process that information (so long as they note their behavior somewhere in their privacy policy). As a result, companies have amassed massive amounts of data about consumers, which is often combined with their offline activities to provide detailed insights into their most personal characteristics, including health conditions, political affiliations, and sexual preferences. This information is often retained for indeterminate amounts of time, sold as a matter of course, and is used to deliver targeted advertising, facilitate individual pricing, and enable opaque algorithmic scoring—all of which, aside from reducing individual autonomy and dignity, can result in concrete harms for consumers, financial and otherwise.[3]

L.D. 1822 corrects that imbalance by establishing strong privacy protections over consumers' personal information. In particular, we appreciate that L.D. 1822 includes:

***Strong Data Minimization Provisions***

First and foremost, this bill's data minimization provision (Section 9608(2)), which is aligned with Maryland's recently passed privacy law and concurrent efforts in several other states,[4] would go a long way toward mitigating the rampant over-collection of consumer data that has led to a panoply of consumer harms.[5] A strong privacy law should limit the data companies can collect to match what consumers expect based on the context of their interaction with the business. For example, a mobile flashlight application should not be permitted to collect a consumer's precise geolocation information because such information is not necessary to provide the service requested and the collection of that data is unlikely to be in the consumer's interest.

In contrast, the core of the framework currently found in many state privacy laws — and the other privacy bills sitting before the committee (LD 1224 and LD 1088) — is "notice-and-choice," which focuses on disclosures in privacy policies. This framework allows

---

https://portal.ct.gov/-/media/ag/press_releases/2025/updated-enforcement-report-pursuant-to-connecticut-data-privacy-act-conn-gen-stat--42515-et-seq.pdf

[3] Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf

[4] E.g., Vermont H. 207, Connecticut S.B. 1356, (as passed by the Joint General Laws Committee), Massachusetts H. 78/S.45/S.29/H.104

[5] See, e.g., Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf; Consumer Financial Protection Bureau, Protecting Americans from Harmful Data Broker Practices (Regulation V), Proposed Rule; request for public comment, (December 3, 2024), https://files.consumerfinance.gov/f/documents/cfpb_nprm-protecting-ams-from-harmful-data-broker-practices_2024-12.pdf

businesses to continue collecting whatever personal data they want and using it for any reason they want as long as they disclose those practices in their privacy policies and allow consumers to opt out. However, very few consumers have the time to read privacy policies in practice, and would likely struggle to decipher their lengthy legalese even if they did. Moreover, the opt-out framework offloads all of the burden of consumer protection onto consumers themselves, while absolving companies of the responsibility to engage in responsible data collection. Rather than continue with this approach that harms consumers, LD 1822 appropriately sets out a rule that businesses can only collect and use data when it is "reasonably necessary" to provide the services the consumer asks for.

Ultimately, we prefer privacy legislation that also limits companies' *use* and *disclosure* of data to what is reasonably necessary to provide the service requested by the consumer. Unlike Representative O'Neill's LD 1977 from last year, LD 1822 only currently applies this standard to data collection, while allowing a much looser standard for processing activities. But simply reining in systemic overcollection of consumers' personal information alone would help eliminate common practices that have contributed to persistent surveillance that threatens individuals' physical safety and autonomy,[6] leads to a persistent drip of massive data breaches that facilitate identity theft and other scams,[7] and further embedds Big Tech's undemocratic control over society.[8]

***Sensitive Data Protections***

Companies should not be profiting from the sale of consumers' most personal data, such as children's data or data about a consumer's race, religion, sex life, finances, precise geolocation, or health. The bill appropriately bans this behavior, as opposed to the more permissive opt-in framework found in LDs 1224 and 1088.

While industry will argue that opt-ins are sufficient (some even arguing that they are *more* consumer friendly than a blanket ban), the reality is that opt-in frameworks aren't working to protect consumers' sensitive data in state privacy laws that include these provisions. Because

---

[6] See, e.g. Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, (October 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs; Office of Senator Ron Wyden, Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics, (February 13, 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

[7] Farhad Manjoo, the New York Times, Seriously, Equifax? This Is a Breach No One Should Get Away With, September 8, 2017, https://www.nytimes.com/2017/09/08/technology/seriously-equifax-why-the-credit-agencys-breach-means-regulation-is-needed.html

[8] Adrienne LaFrance, The Atlantic, The Rise of Technoauthoritarianism, January 30, 2024, https://www.theatlantic.com/magazine/archive/2024/03/facebook-meta-silicon-valley-politics/677168/

companies aren't typically required to separate their request for consent for necessary processing (e.g. data collection) from unnecessary processing (e.g. data sales), consumers are still often presented with take-it-or-leave it choices that don't leave them any better off than before. Furthermore, last year CR released a report on sensitive data opt-in provisions and found that some companies appeared to be ignoring their responsibility to obtain opt-in consent or continued to share our personal data even when we declined to opt-in.[9] To our knowledge, there hasn't been a single enforcement action related to this provision under existing state privacy laws. And ultimately, the solution to this issue isn't more consent boxes; consumers need stronger baseline protections.

Some examples of harmful uses of consumers' sensitive data include:

- *Scamming, stalking, and spying.* Fraudsters and other bad actors can use sensitive data to target vulnerable individuals for scams, or otherwise use personal information to cause harm. For example, scammers can use commercially available location data to increase the specificity of their phishing or social engineering scams, such as by including location-specific details, like mentioning a nearby business or the individual's recent activity.[10] Location data brokers are also commonly used by abusive individuals to locate people, hunt them down, and stalk, harass, intimidate, assault, or even murder them.[11]

- *Predatory use of consumer data.* The sale of consumer data can result in financially disastrous consequences for consumers. Some data brokers sell lists of consumers sorted by characteristics like "Rural and Barely Making It" and "Credit Crunched: City Families," which can be used to target individuals most likely to be susceptible to scams or other predatory products. And a recent case brought by the Texas Attorney General alleged that the insurance company Allstate secretly purchased information about consumers' driving behaviors (including their precise geolocation data), which it used in some cases to raise consumers' premiums or deny them coverage altogether.[12] They also sold the driving data to several other insurance companies without consumers' knowledge or consent.

---

[9] Maggie Oates et al., Consumer Reports, Companies Continue to Share Health Data Despite New Privacy Laws,
[10] Phishing Box, Tracking Data: Identifying the Anonymized, January 16, 2024, https://advocacy.consumerreports.org/wp-content/uploads/2024/01/Companies-Continue-to-Share-Health-Data-1-16-2024-Consumer-Reports.pdf
[11] Justin Sherman, Lawfare, People Search Data Brokers, Stalking, and 'Publicly Available Information' Carve-Outs, (October 30, 2023), https://www.lawfaremedia.org/article/people-search-data-brokers-stalking-and-publicly-available-information-carve-outs
[12] Office of the Texas Attorney General, Attorney General Ken Paxton Sues Allstate and Arity for Unlawfully Collecting, Using, and Selling Over 45 Million Americans' Driving Data to Insurance Companies, (January 13, 2025), https://www.texasattorneygeneral.gov/sites/default/files/images/press/Allstate%20and%20Arity%20Petition%20Filed.pdf

Moreover, online and in-person retailers can use information about individuals' location, demographics, finances, and more to make inferences about them that are then used to set individualized prices. Some grocery chains, such as Kroger, already collect this type of information on consumers and have sold it to third-parties as part of their "alternative profit" business lines.[13] Last year, the Federal Trade Commission released initial findings from its Surveillance Pricing study, confirming that sensitive data categories can be a key input of individualized prices shown to consumers.[14]

- *Tracking of sensitive locations.* Location information can be used to track individuals' visits to especially sensitive locations, such as reproductive or mental health facilities,[15] political rallies,[16] religious facilities,[17] and more. This information is often sold (or in some cases, inadvertently shared)[18] by app developers to data brokers, who then re-package the information and sell it to a variety of third-parties, including advertisers, political extremist groups, and law enforcement. The Federal Trade Commission has recently enforced against several location data brokers, including one that allegedly maintained and sold access to nearly 2,000 lists of individuals sorted by characteristics they had inferred from their collection of location data, including categories such as "parents of preschoolers," "Christian church goers," and "wealthy and not healthy."[19]

- *Data breaches.* Data brokers sit on trillions of data points, many of them sensitive and purchased from other businesses. Unsurprisingly, this makes them a top target for hackers and cyber criminals. For example, the data broker Gravy Analytics, which has claimed to "collect, process and curate" more than 17 billion signals from people's smartphones

---

[13] Jon Keegan, the Markup, Forget Milk and Eggs: Supermarkets Are Having a Fire Sale on Data About You, (February 16, 2023), https://themarkup.org/privacy/2023/02/16/forget-milk-and-eggs-supermarkets-are-having-a-fire-sale-on-data-about-you

[14] Federal Trade Commission, FTC Surveillance Pricing Study Indicates Wide Range of Personal Data Used to Set Individualized Consumer Prices, (January 17, 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

[15] Office of Senator Ron Wyden, Wyden Reveals Phone Data Used to Target Abortion Misinformation at Visitors to Hundreds of Reproductive Health Clinics, (February 13, 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

[16] Charlie Warzel and Stuart A. Thompson, New York Times, How Your Phone Betrays Democracy, (December 21, 2019), https://www.nytimes.com/interactive/2019/12/21/opinion/location-data-democracy-protests.html

[17] Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/news-events/news/press-releases/2024/12/ftc-takes-action-against-gravy-analytics-venntel-unlawfully-selling-location-data-tracking-consumers

[18] Joseph Cox, Wired, Candy Crush, Tinder, MyFitnessPal: See the Thousands of Apps Hijacked to Spy on Your Location, (January 9, 2025), https://www.wired.com/story/gravy-location-data-app-leak-rtb/

[19] *Id.*

every day,[20] reportedly suffered a massive data breach that may have leaked the location data of millions of individuals.[21] This type of data makes it trivially easy to reconstruct the everyday comings and goings of individuals, politicians, and even servicemembers.[22]

***Appropriately Scoped Non-discrimination Provisions***

Not only does the non-discrimination language in Section 9608 clarify that consumers cannot be charged for exercising their rights under the law, but it makes it clear that legitimate loyalty programs, that reward consumers for repeated patronage, are supported by the bill.

At the same time, there are a few provisions that we recommend the drafters tweak in order to provide the level of protection that Maine consumers deserve:

***Include Strong Enforcement Provisions***

While we understand the importance of balancing the equities at stake in privacy legislation, consumers should be able to hold companies accountable in some way for violating their rights. As the representative from the Maine Attorney General's Office outlined in his testimony,[23] AG-only enforcement is likely to be insufficient. Unfortunately, most state Attorney General offices are underresourced and do not have the capacity to bring enough actions to meaningfully deter illegal behavior, meaning consumers may have no recourse in the event of a violation that harms them. Despite ample evidence suggesting widespread non-compliance with existing privacy laws,[24] there have not been commensurate enforcement efforts to-date. Consumer Reports has put out a number of reports demonstrating noncompliance with state privacy laws, including a report from earlier this month showing that many companies were showing targeted

---

[20] Federal Trade Commission, FTC Takes Action Against Gravy Analytics, Venntel for Unlawfully Selling Location Data Tracking Consumers to Sensitive Sites, (December 3, 2024), https://www.ftc.gov/system/files/ftc_gov/pdf/2123035gravyanalyticscomplaint.pdf

[21] Joseph Cox, 404Media, Hackers Claim Massive Breach of Location Data Giant, Threaten to Leak Data, (January 7, 2025), https://www.404media.co/hackers-claim-massive-breach-of-location-data-giant-threaten-to-leak-data/

[22] Justin Sherman et al., Duke Sanford School of Public Policy, Data Brokers and the Sale of Data on U.S.Military Personnel, (November 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/11/Sherman-et-al-2023-Data-Brokers-and-the-Sale-of-Data-on-US-Military-Personnel.pdf

[23] Aaron Frey, Maine Attorney General's Office, Testimony in Support of LD 1822, (May 5, 2025) https://legislature.maine.gov/testimony/resources/JUD20250505Frey133909563028562659.pdf

[24] See, e.g. two separate studies indicating that less than 30 percent of top websites comply with universal opt-out requests: Privado, State of Website Privacy Report 2024, (December 2024), https://www.privado.ai/state-of-website-privacy-report-2024; Data Grail, Data Privacy Trends Report, https://www.datagrail.io/resources/interactive/data-privacy-trends/, (December 2024)

ads despite receiving legally binding universal opt-out signals.[25] Yet, to our knowledge, there are more states with active comprehensive privacy laws (13) than there have been public enforcement actions. It is therefore unsurprising that market behavior has yet to improve.

While we think an allowance for both public and private enforcement mechanisms would make sense — dozens of other consumer protection laws do the same — and are generally skeptical of claims that such an approach would open the floodgates to frivolous litigation, we are open to discussing guardrails to prevent that outcome if raised in good-faith. We would also support limited exclusions from the private right of action for small businesses, as is being considered in Vermont's H. 208.[26]

***Mandate the Universal Opt-Out***

Section 9608(6) currently provides that "a controller may satisfy the controller's obligation under this subsection to establish a secure and reliable mechanism for a consumer to exercise the right to opt out under subsection 5" by **either** providing an accessible link **or** allowing a consumer to opt–out via an opt-out preference signal (OOPS). None of the 13 currently effective state privacy laws that allow consumers to opt-out via an OOPS provide this sort of optionality. OOPSs allow consumers to broadcast to businesses they interact with online their preference to opt out from their personal information being sold or shared with third parties through a simple toggle. Otherwise, consumers must hunt down and navigate divergent opt-out processes for potentially thousands of different companies, which is simply not tenable. Changing the "or" in Section 9608(6)(C)(1) to an "and," would resolve this issue, which does not appear to be intentional on the part of the drafters.

***Remove Entity Level Exemptions***

The bill currently exempts from coverage any financial institution or an affiliate of a financial institution, as well as covered entities and business associates under the Health Insurance Portability and Accountability Act. These carveouts arguably make it so that large tech companies (Apple, Amazon, Google, Facebook, and Microsoft) would be exempted from the entire bill if one arm of their business receives enough financial information from banks or crosses the threshold into providing traditional healthcare services, a line many of them are already currently skirting.[27] At most, the bill should exempt *information* that is collected

---

[25] Matt Schwartz *et al.*, *Mixed Signals: Many Companies May Be Ignoring Opt-Out Requests Under State Privacy Laws*, Consumer Reports, (Apr. 1, 2025), https://innovation.consumerreports.org/Mixed-Signals-Many-Companies-May-Be-Ignoring-Opt-Out-Requests-Under-State-Privacy-Laws.pdf

[26] Vermont H. 208, Section 2424(d)(2)(A), https://legislature.vermont.gov/Documents/2026/Docs/BILLS/H-0208/H-0208%20As%20Introduced.pdf

[27] See e.g., The Economist, "Big Tech Pushes Further into Finance," (Dec. 15, 2022), https://www.economist.com/business/2022/12/15/big-tech-pushes-further-into-finance; Richard Waters,

pursuant to those laws, applying its protections to all other personal data collected by such entities that is not currently protected.

******

We look forward to working with you to ensure that Maine consumers have the strongest possible privacy protections.

Sincerely,

Matt Schwartz
Policy Analyst

---

"Big Tech searches for a way back into healthcare," Financial Times, (May 17, 2020), https://www.ft.com/content/74be707e-6848-11ea-a6ac-9122541af204