AARON M. FREY
ATTORNEY GENERAL

TEL: (207) 626-8800
TTY USERS CALL MAINE RELAY 711

STATE OF MAINE
OFFICE OF THE ATTORNEY GENERAL
6 STATE HOUSE STATION
AUGUSTA, MAINE 04333-0006

REGIONAL OFFICES
84 HARLOW ST. 2ND FLOOR
BANGOR, MAINE 04401
TEL: (207) 941-3070
FAX: (207) 941-3075

125 PRESUMPSCOT ST., SUITE 26
PORTLAND, MAINE 04103
TEL: (207) 822-0260
FAX: (207) 822-0259

14 ACCESS HIGHWAY, STE. 1
CARIBOU, MAINE 04736
TEL: (207) 496-3792
FAX: (207) 496-3291

Testimony in Support of LDs 1822, in Opposition to to LD 1088 and 1224

Senator Carney, Representative Kuhn, and honorable members of the Joint Standing Committee on Judiciary, my name is Brendan O'Neil, I am an Assistant Attorney General and appear on behalf of Attorney General Aaron Frey to testify in support of L.D. 1822 and in opposition to L.D.s 1088 and 1224, all proposing different approaches to comprehensive consumer privacy. We thank the Committee for investing its time into these proposals at this critical moment as advances in technology, the digital information economy, the rise of artificial intelligence, and digital surveillance raise many concerns. As we learn more about these issues, it is critical that Maine's consumers gain greater control and rights over their and their families' information.

The Attorney General's Office supports L.D. 1822 because, if enacted, Maine would be among the states leading the nation on privacy, with among the strongest and most protective provisions. Of the three bills, we believe L.D. 1822 will do more to restore an appropriate balance between consumers and industry regarding control over individuals' information and data. In supporting L.D. 1822, we want to highlight certain critical components of a strong comprehensive data privacy bill, along with suggestions for improvements:

Meaningful data minimization: A core protection for Mainers is limiting the information that companies may collect about us and our activities online to the minimum necessary to provide the product or service the consumer is requesting, coupled with keeping that information only for the minimum period necessary to do so. This keeps data collection focused on the consumer's needs. It also minimizes the work consumers must do to opt out of data collection on each website or application they engage with and, because of this, we think this form of data minimization is more efficient and more effective at protecting Mainers' data than the notice-and-opt-out model of privacy legislation found in L.D.s 1224 and 1088[1] L.D. 1822 includes, in §9608, this kind of meaningful data minimization and we strongly support passing a privacy bill including these provisions. Further, L.D. 1822 provides stronger protections for Maine's

[1] Because businesses and other entities collecting individual data will almost always know more about what they do with that data than consumers, "that may mean that placing the burden on [industry] to identify and mitigate risks to consumers would be a more efficient approach than obligating consumers to continually take action to guard the consumer's data." Consumer Financial Protection Bureau, *State Consumer Privacy Laws and the Monetization of Consumer Financial Data*, Section 2.3, n. 21, November 2024 (https://www.consumerfinance.gov/data-research/research-reports/state-consumer-privacy-laws-and-the-monetization-of-consumer-financial-data/).

children by limiting the collection and use of data about youths up through age 17, rather than only up through age 12 as in L.D.s 1224 and 1088.

This form of data minimization is in Maryland's privacy statute enacted last year, and is being considered by state legislatures including in Connecticut and Massachusetts. And limiting data retention is now in the federal rule implementing the Children's Online Privacy Protection Rule (COPPA) as updated in January by the Federal Trade Commission's recent rulemaking.[2]

This version of data minimization is much more robust and protective of consumers than versions that describe limiting data collection to the practices a company discloses in its privacy policy. That version is found in L.D.s 1224 and 1088. Under that model, companies may continue to collect any information about us they wish so long as they merely disclose it in a privacy policy, which they may change at any time. We believe that is no limit. The Attorney General's office does not support legislation with that version because we believe it does not sufficiently protect consumers and instead keeps data collection focused on the collectors' economic needs. As the Federal Trade Commission recently found, "Many companies' insistence that their data collection practices are justified simply because they are 'disclosed' to consumers only amplifies [concern about companies' data handling and oversight]." These so-called disclosures are very hard to read (often made across various policies, located in different places across websites, apps, etc.), nearly impossible to understand, too vague to effectively communicate a platform's actual practices, and subject to change (and it is up to the consumer to determine what has changed and when)."[3]

Limiting the data collected from and about us to the absolute minimum necessary, and the time it's kept to only as long as necessary, is strong privacy protection. In 2024, the Attorney General's office received over 1,000 data breach notices alerting nearly 1 million Mainers that their data was put at risk. Data breach investigations by state Attorneys General or the FTC often involve significant amounts of consumer information, including sensitive data, and data that has been kept far longer than it is needed, resulting in increased scam and fraud risk to consumers and significant liability for businesses. Consumers, and companies, are at less risk of a data breach when less information is collected and when it is deleted as soon as no longer needed according to a public schedule.

Robust data minimization is critical at this time - more and more of our data and information is being collected, bought, sold, and processed against consumers' expectations, without our knowledge, and sometimes to our detriment. Financial institutions and, increasingly, other companies and firms offering consumer financial products, are collecting large quantities of consumer data, building new business models around monetizing that data as a source of revenue, including by selling that data to 3rd parties.[4] Consumers highly value their financial data, perhaps even more than their medical records, and are especially concerned about

---

[2] 16 C.F.R. 312.10, see also Statement of FTC Chair Lina Khan, January 16, 2025, page 2 (https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/statement-chair-lina-m-khan-regarding-final-rule-amending-childrens-online-privacy-protection-rule)

[3] Federal Trade Commission, *A Look Behind the Screens: Examining the Data Practices of Social Media and Video Streaming Services*, Section IV(D), September, 2024 (https://www.ftc.gov/reports/look-behind-screens-examining-data-practices-social-media-video-streaming-services)

[4] *Supra* note 1, Section 3.

maintaining the privacy of that data.[5] While consumers are increasingly using digital tools for banking and payment services, financial institutions are also increasingly sharing consumer information with advertisers, perhaps without the awareness of consumers, and some have launched their own advertising platform affiliates.[6]

Social media companies and video streaming services collect significant amounts of data about consumers, both directly and indirectly by purchasing data, and those companies share this data with affiliates and 3rd parties.[7] These companies sometimes cannot identify what data they collect about consumers.[8] L.D. 1822 attempts to address such vast overcollection and hidden uses through its strong data minimization and data deletion requirements, which we commend.

We believe that data minimization as found in L.D. 1822 is much more protective of Mainers than the notice and opt-out model found in L.D.s 1088 and 1224 by collecting less data and by better balancing the work of data protection and the risks that follow data collection and retention.

Exemptions for data, not entities: The Attorney General's office supports legislation that avoids exempting entire sectors of the economy on the basis that some of the work an entity does may be regulated by a federal statute which provides some privacy regulation. Instead, we support legislation that exempts data, not entities, and only to the extent the specific activity – the collection and use of the data – is regulated by a federal statute. Anything more than that we believe is overbroad and leaves consumers unprotected and without rights over significant data collection practices. Some federal statutes, such as the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA), while establishing a regulatory floor with some privacy-related provisions, expressly permit states to enact greater privacy protections.[9] We strongly support limiting any exceptions to the use of data, not the entire entity beyond the use of the data, thereby increasing the privacy protections for Mainers. Further, at a time when significant questions exist about whether the federal regulators on the privacy beat, including the CFPB and the FTC, will continue to exist, will face significant cuts in staffing, and will divert any remaining enforcement efforts elsewhere, Mainers may not be able to rely on federal privacy enforcement and states have additional incentive to raise the floor and provide stronger privacy protections for their citizens.[10]

---

[5] *Id.*

[6] *Id*

[7] *Supra* note 3.

[8] *Id*

[9] "Given financial institutions' rapid investment in expanding their own data monetization and absent stronger federal protections, States should consider whether they wish to continue to exempt these activities from the consumer rights and protections their comprehensive state privacy laws provide." *Supra*, note 1, Section 5, noting that "Under the GLBA, the term "financial institution" broadly encompasses a wide variety of businesses engaged in financial activities, including lending, transferring money or securities, financial advisory services, asset management, consumer reporting, debt collection, loan servicing, various transactional services, and in many circumstances acting as a service provider for companies engaged in these activities.", citing 12 U.S C. § 1843(k)(4); 12 C.F.R. §§ 225.28, 225 86.

[10] Commissioner Slaughter Opening Statement, U.S. House of Representatives, Committee on Energy and Commerce, Subcommittee on Commerce, Manufacturing, and Trade. Hearing on *The World Wild Web Examining Harms Online,* Wednesday, March 26, 2025 (https://democrats-energycommerce house.gov/sites/evo-subsites/democrats-energycommerce house.gov/files/evo-media-document/testimony_rebecca-kelly-slaughter pdf).

States enforcing their existing privacy statutes report that overbroad entity-level exemptions are challenging for consumers and for privacy enforcement – Connecticut is considering legislation to scale back its exemptions. We strongly support the position taken in L.D. 1822 to include only data-level exemptions for activity regulated by the Gramm-Leach-Bliley Act (GLBA) and the Fair Credit Reporting Act (FCRA). However, exempting entire health care entities, nonprofits, and institutions of higher education removes major sectors of Maine's digital economy from these privacy rights for Mainers and significantly limits this legislation. We recommend the Committee consider strengthening L.D. 1822 by eliminating the following entity-level exemptions in §9604(1):

- (F) - Health care affiliates, practitioners, or affiliates thereof – This exemption allows such entities to use hidden pixels, data brokers, or other means to collect, process, and sell any information – including non-HIPAA-related data - about consumers, for any purpose, including marketing or additional profit. HIPAA-related data is already exempt under §9604(2)(B), rendering an entity-level exemption unnecessary and redundant, and leaving Mainers at risk. Perhaps unique among other entities covered by this legislation, consumers will always need to interact with these entities and should be able to keep their information safe when they need healthcare.
- (C) – Institutions of higher education – This provision risks exempting any post-high school educational or training entity, including for-profit Internet-based colleges, private colleges, and possibly any entity offering courses or certificates or degrees of any kind, or any entity setting itself up as a "college". As with health care entities, the data of students is already exempted under §9604(2)(M), rendering an entity-level exemption redundant and creating risks for Mainers. Institutions of higher education of any kind serving Mainers would be able to collect, buy, and sell significant amounts of non-FERPA-related data. It is reasonable to expect that such institutions will and should be as able to comply with this legislation as other covered entities.
- (B) – Nonprofit entities – Nonprofit entities collect a significant amount and breadth of consumer data, and other states have not exempted them. Nonprofits may be large entities, may have a regional or national presence, and are often sophisticated organizations. Smaller nonprofits may utilize sophisticated vendors to assist them with meeting 'back-office' regulatory and administration obligations. Nonprofits should be expected to protect Mainers' information by complying with L.D. 1822.

Enforcement: The enforcement mechanism, in each of the bills should be improved. As with other consumer protection laws, the Attorney General's Office believes it is necessary that Mainers be empowered to enforce their own rights under any comprehensive privacy legislation. There is nothing sufficiently different about consumer privacy that warrants treating it differently from other consumer protection statutes. We believe the Legislature, in granting rights to individual consumers, should not require them to rely on a state agency to enforce those rights. We note that privacy legislation in Massachusetts includes a private right of action. Other state Attorneys General are enforcing their states' privacy statutes and we expect to do so as well. However, even with additional resources being provided to our office, we likely will not be able to pursue every violation. Maine consumers should be empowered to protect themselves. We are prepared to work with the Committee to address concerns and balance Mainers' ability to pursue their claims with businesses' ability to operate with certainty. In particular, we believe the

Legislature can address concerns about excessive litigation by clearly and particularly identifying the parts of the legislation for which individuals may bring claims. Following are a few proposals we suggest the Committee consider:

- Coupling a right to cure with a private right of action – this would help those entities which are attempting to comply in good faith by giving them an opportunity to address inadvertent noncompliance or minor/technical noncompliance. We recommend any such right to cure be subject to a sunset;
- Exempting small businesses from a private right of action for some period of time; and
- Delay implementation of a private right of action for some period of time to give businesses and consumers time to adjust to the new privacy protections.

Information for consumers: We appreciate L.D. 1822 enhancing the rights of Maine consumers by enabling them to request a list of the 3rd parties to which a controller has sold the consumer's data. This critical information enables consumers to follow their data downstream so that they may learn more about who is using their data and request its deletion. This is another area in which L.D. 1822 provides stronger protections for Mainers than L.D.s 1088 and 1224. We suggest improving upon this by enabling consumers to request the information a company has about a consumer which it claims is publicly available information (PAI). Because PAI is carved out of the definition of personal data, companies have no obligation to reveal information it has designated as PAI to consumers, nor do consumers have an opportunity to challenge this designation. And, because of the challenges presented by PAI as reported by states enforcing their statutes, we also recommend the Committee consider the change to its definition being considered by the Connecticut Legislature.[11]

Opt-out preference signals: Particularly in the absence of a private right of action, consumers should have the ability to – as simply and easily as possible, with minimal friction – exercise their opt out rights through technology that can efficiently and conveniently signal their preference to opt out of the sale of personal data, use for targeted ads, or processing for certain purposes. We recommend the Committee consider eliminating §9608(6)(C)(2) (e) and (f) in L.D. 1822.

Affiliates: The Federal Trade Commission and the Consumer Financial Protection Bureau both raised concerns last year about consumer data being shared with affiliates, some of which are part of extensive corporate conglomerates, including affiliates in foreign countries.[12] Such affiliates may be providing services very different from the collector of the data, and consumer data may be used for unknown purposes beyond its original collection, such as AI training.[13] However, the definition for Sale of Personal Data exempts sharing with Affiliates, which may be a significant loophole that undermines Mainers' expectations about who has access to their data and for what purposes. We suggest narrowing the Affiliate exemption to restrict such transfers to providing or maintaining a specific product or service requested by the consumer.

---

[11] See S.B. 1356, 2025, Section 1(34) (https://www.cga.ct.gov/asp/cgabillstatus/cgabillstatus.asp?selBillType=Bill&which_year=2025&bill_num=1356).

[12] *Supra* notes 1 and 3.

[13] *Supra* note 3, at section IV(D); note 1, at sections 2 3, 3.

Internet Service Providers (ISPs): The Attorney General has consistently opposed any attempt to repeal Maine's landmark consumer protection law providing some of the strongest privacy protections for broadband internet customers nationwide.[14] Consistent with our office's testimony opposing L.D. 1284 which would repeal the ISP privacy law, we oppose L.D. 1088 which also includes a repeal provision. Again, this first in the nation law restricts the extent to which ISPs may use, disclose, or sell their customers' personal information, such as Mainers' browsing history, their location, the content of their communications, and their financial and health information. As the Federal Trade Commission has noted, because ISPs are essentially the gateways or onramps to the internet, they can collect vast amounts of information regarding their customers' online activity. Recognizing that position, the Maine Legislature wisely enacted the ISP law with very strong protections for consumers online information, and it should not now retreat from its zealous protection of our residents' privacy.

Thank you for your consideration of these comments, and I am happy to answer any questions.

[14] 35-A M.R S A. c. 94.