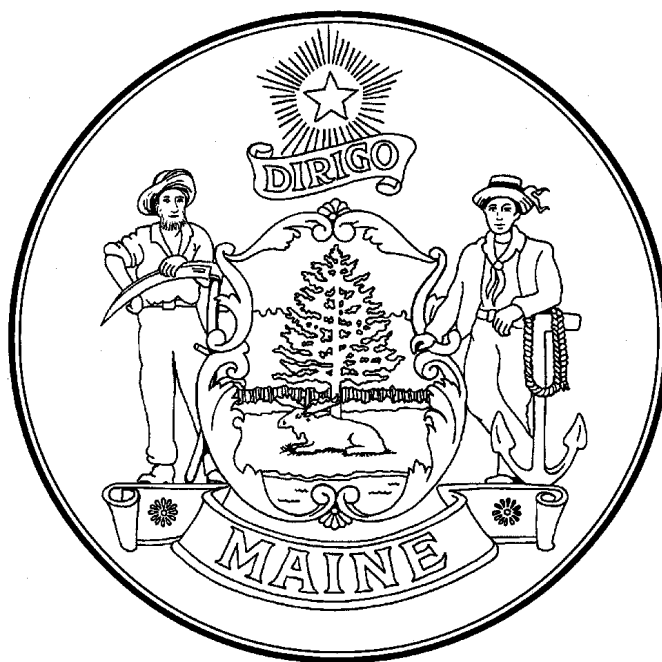


MAINE STATE LEGISLATURE

The following document is provided by the
LAW AND LEGISLATIVE DIGITAL LIBRARY
at the Maine State Law and Legislative Reference Library
<http://legislature.maine.gov/lawlib>



Reproduced from scanned originals with text recognition applied
(searchable text may contain some errors and/or omissions)

May 5, 2025

Hon. Anne Carney, Senate Chair
Hon. Amy Kuhn, House Chair
Joint Standing Committee on Judiciary
100 State House Station
Augusta, Maine 04333-0100

RE: LD 1822, An Act to Enact the Maine Online Data Privacy Act (Rep. Kuhn)

Dear Senator Carney, Representative Kuhn, and members of the Judiciary Committee:

L.L.Bean appreciates the opportunity to provide testimony regarding L.D. 1822. The company has been working internally on data privacy for several years, and since 2020 have voluntarily extended privacy protections to all our customers, regardless of their home state. Maine citizens deserve to have the same data privacy protections enjoyed by residents of other states, regardless of which businesses they choose to engage with.

We appreciate the time and effort Representative Kuhn and the cosponsors have dedicated to this privacy bill. We support most of the bill as it aligns with current privacy laws or aligns with L.L.Bean's current practices. Our concerns are few, but significant. We would like to provide some feedback regarding our primary concern - the data minimization section.

Like most consumer businesses in 2025, L.L.Bean collects Personal Data from and about consumers even when they have not directly requested a product or service. For example, a cookie (or other identifier) may be placed that tracks a consumer's browsing history, allowing us to later serve advertisements tailored to their interests. If "service" is meant to be defined broadly to include offering a website, and personal data may be collected based on a visit to the website, we believe the language should be modified to make such intent clear.

The Maine Legislature can now benefit from the experiences of other states that enacted privacy legislation in recent years. We now know that the existing models work. Privacy laws in states like Connecticut, Colorado, and Virginia are effectively protecting consumers. For example, the Texas Attorney General sued Allstate under the Texas Privacy and Security Act for practices that legislators are aiming to protect consumers against. In contrast, the "Maryland model" on which L.D. 1822's data minimization standard is based is an outlier, and importantly, remains untested since Maryland's law is not yet effective. L.L.Bean is concerned that this heightened data minimization standard puts Maine businesses in jeopardy and goes beyond what is necessary to protect Mainers.

Customer data enables businesses to create relevant ads and deliver them to individuals who are most likely to find them helpful. In 2025, personalization is an expected and appreciated service for many consumers. For those who are not interested in this service, they have choices under other states' privacy laws. They can opt-out of targeted advertising, use Global Privacy Control, or block cookies to manage their preferences.

Made for
the shared
joy of the
outdoors

L.L.Bean

L.D. 1822's data minimization standard effectively bans the vast majority of personalized, targeted advertising. For L.L.Bean, this more restrictive language puts us at a competitive disadvantage to our out-of-state competitors. Not surprisingly, our company relies on sales to Maine resident-customers far more than our competitors do. For that reason, hamstringing our ability to market to these valuable customers will have an outsized impact on L.L.Bean versus our competitors, for whom marketing to Mainers is an afterthought. Moreover, these restrictions are being proposed at a historically challenging time for Maine retailers. The ongoing retreat of Canadian customers from U.S. businesses, coupled with the increased costs associated with new universal (and threatened reciprocal) tariffs, is squeezing marketing budgets. That means that the marketing investments we do make have to be efficient. Personalized, targeted ads are among our most efficient marketing investments.

L.L.Bean appreciates the opportunity to provide this information to the Committee and is happy to serve as a resource for any future questions or discussions regarding privacy. Our goal is to support Maine's legislators in passing a successful privacy bill in our home state.

Sincerely,

Christiana van Voorhees

Christy van Voorhees
Legal Counsel
Co-Chair, L.L.Bean's Data Privacy Program

Made for
the shared
joy of the
outdoors

L.L.Bean



May 5, 2025

Senator Anne Carney, Chair
Representative Amy Kuhn, Chair
Joint Standing Committee on Judiciary
State House, Room 438
Augusta, Maine 04333

Re: Testimony in Support of LD 1822, An Act to Enact the Maine Online Data Privacy Act and Against LDs 1088, 1224, and 1284

Dear Senator Carney, Representative Kuhn, and Members of the Joint Standing Committee on Judiciary:

My name is Lauren Wille and I am the Legal Director at Disability Rights Maine. DRM is Maine's designated Protection and Advocacy agency, and our mission is to advance justice and equality by enforcing rights and expanding opportunities for people with disabilities in Maine. Thank you for the opportunity to provide testimony in support of LD 1822, and against LDs 1088, 1224, and 1284.

LD 1822 is an important policy that will allow Maine to protect its citizens in the face of rapidly evolving technology. This bill prohibits entities, including for-profit companies, from collecting digital consumer data except where necessary to provide the product or service requested by the consumer. And, crucially, it prohibits such entities from processing consumer data in a way that discriminates or makes unavailable the enjoyment of goods and services on the basis of enumerated statuses, including disability. In contrast to LD 1822, LDs 1088 and 1224 would allow companies to collect personal information as long as the consumer clicks "I agree," or the collection is disclosed in a privacy policy. Very few people read privacy policies, and those of us who do, will be forced to choose between our privacy and accessing a service.

Assistive technology has been tremendously beneficial in helping people with disabilities become more independent, but, as technology expands, so do the privacy concerns. There are apps that help people track chronic pain, transcribe speech for people who are Deaf or hard of hearing, provide wheelchair accessibility information, read aloud written

160 Capitol Street, Suite 4, Augusta, ME 04330
207.626.2774 • 1.800.452.1948 • Fax: 207.621.1419 • drme.org

MAINE'S PROTECTION AND ADVOCACY AGENCY FOR PEOPLE WITH DISABILITIES

information on devices, and provide daily task reminders, to name just a few. These apps are not “health care providers” that are subject to confidentiality under HIPAA. Instead, users might agree to give up privacy protections in order to access the technology. Users may not be aware of the implications of this data being collected, processed, and sold to third-parties. But they may notice that suddenly they are receiving very targeted ads for equipment, certain medications, and other products. The ordinary consumer may not be aware of the exchange of personal data that has occurred to enable this.¹

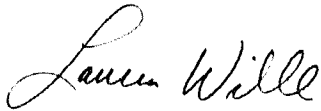
The recipients of our sensitive data include entities are not subject to confidentiality laws under HIPAA, which only governs health records connected to health care providers. With the proliferation of apps, a great many consumers do not understand that, and how, their personal data is being collected, processed, and sold to other entities. LD 1822 provides protection for all consumers, including consumers with disabilities. In our work at DRM, we see daily how the lack of privacy, through the lens of ableism, leads to rampant discrimination and exploitation of individuals with disabilities. This bill is one step toward safeguarding that usage and allowing people to have control over their personal data and how it is used.

In addition, LD 1822 enables consumers to, among other things, confirm whether their data is being collected, access that data, correct inaccuracies, and opt out of processing and sale of personal data for targeting marketing.

LD 1822 provides comprehensive protections for Mainers, including Mainers with disabilities, and DRM urges this esteemed Committee to vote Ought to Pass. We also urge you to oppose LDs 1088 and 1224, which do not go far enough, and LD 1284, which would repeal our internet privacy law.

Thank you for your time and consideration.

Sincerely,



Lauren Wille, Esq.
Legal Director
Disability Rights Maine

¹ For a comprehensive analysis of the benefits and risks of data collection as it relates to health equity, see Silvia Yee & Mary Lou Breslin, *This Data, Not That Data: Big Data, Privacy, and the Impact on People with Disabilities*, Disability Rights Education and Defense Fund, https://healthlaw.org/wp-content/uploads/2023/03/This-Data-Not-That-Data_Disability-Rights-Education-and-Defense-Fund_FINAL.pdf (last accessed May 5, 2025).

**Testimony of Patrick Woodcock
Before the Committee On Judiciary
L.D. 1088, LD 1224, LD 1284, and LD 1822
May 5, 2025**

Senator Carney, Representative Kuhn, and members of the Committee on Judiciary, my name is Patrick Woodcock. I am here on behalf of the Maine State Chamber of Commerce, representing a network of 5,000+ small to large businesses. Thank you for the opportunity to provide testimony on the four bills related to data privacy.

The utilization of digital advertising is not just an important component of marketing, but for many Maine businesses it represents the entirety of many businesses method of connecting with potential customers. The Maine State Chamber of Commerce will review any legislation governing restrictions on online data on whether the legislation will put our businesses at a competitive disadvantage in utilizing these tools. This is especially important at a time when there is significant uncertainty in our state's economic outlook and concerns about the future of Maine's largest industry, tourism. Quite simply, now is not the time for Maine to limit commercial digital tools to attract customers to spend their money in our state.

Online data and business advertising has become so closely intersected and ultimately core to economic activity that Congress should be establishing clear and consistent standards throughout the United States. In fact, last year the Maine State Chamber of Commerce, alarmed at some state proposals, wrote the attached letter to the Maine congressional delegation urging action at the federal level. We reiterated these concerns last week in meetings with the four delegation members. Businesses are marketing across state lines. Individuals are traveling across state lines. The idea of distinct rules in 50 different states should unite business and privacy groups alike in advocating for federal legislation.

Short of a federal law the states should create as much consistency and alignment in state legislation. The Chamber believes both LD 1088 and LD 1224 follow the model of protecting sensitive data, allowing opt-out standards that more than a dozen states have adopted. The Maine State Chamber of Commerce supports these bills and would urge the Committee to utilize these bills as the basis for future work sessions. We appreciate both Representatives Roberts and Henderson for their sponsorship.

We are concerned about LD 1822 and believe it would place Maine businesses at a competitive disadvantage. While attorney Stacey Stitham of Brann & Isaacson will subsequently outline the specific legal concerns about the legislation, I would reinforce that the structure does not follow the standard of over a dozen other states, limits digital tools such as geolocation methods of reaching customers, and introduces a data minimization standard that introduces ambiguity at the heart of individual interaction with the internet. We would recommend the Committee not go down this unique pathway in protecting digital privacy that is untested, but rather adopt standards that are now being applied in over a dozen states.

As we move into work sessions there are some additional points the Chamber would recommend the Committee consider:

- 1) **ISP Legislation.** We thank Senator Stewart for introducing LD 1284. We agree that if the Committee moves forward with comprehensive data privacy legislation that there should be one law and the ISP law would create inconsistencies in implementation and customer experience.
- 2) **Vehicle Telematics.** Vehicle telematics data privacy is a critical aspect of consumer data privacy. Consumer data privacy legislation should address the relationship between vehicle telematics and consumer data.
- 3) **Healthcare.** We should consider a broader level of exemption for healthcare entities where protecting healthcare data is core to their mission and subject to existing federal and state laws and standards.

Thank you for consideration of this testimony and I would welcome any questions from the Committee.

MAINE
S T A T E
CHAMBER
of
COMMERCE

The voice of Maine business

June 10, 2024

The Honorable Susan Collins
413 Dirksen Senate Office Building
Washington, D.C. 20510

The Honorable Angus King
133 Hart Senate Office Building
Washington, D.C. 20510

The Honorable Chellie Pingree
2354 Rayburn House Office Building
Washington, D.C. 20515

The Honorable Jared Golden
1710 Longworth House Office Building
Washington, D.C. 20515

Dear Senator Collins, Senator King, Representative Pingree, and Representative Golden:

Thank you for the opportunity to meet during the Maine State Chamber of Commerce's annual trip to Washington, D.C. I am writing as a follow-up to provide you with additional information on data privacy, which has had some legislative activity since we last met.

As we mentioned, the Maine Chamber strongly encourages support for federal legislation that would create a uniform standard to protect consumer privacy. As you know businesses of all sizes rely heavily on data to attract new customers and remain competitive, particularly in e-commerce and these techniques have become increasingly sophisticated. Meanwhile, consumers are wanting a greater role in determining how their data is processed and transferred and that sensitive data be protected. As a result, fifteen states have enacted comprehensive data privacy laws that attempt to both protect consumers and maintain business methods to attract customers online. While many states share commonalities in the individual state laws, the Maine State Chamber of Commerce is concerned that a patchwork of state laws will be challenging for businesses to navigate, leading to compliance complexities and increased costs.

Specifically, proposed legislation in Maine this past legislative session would have departed from other states and limited Maine businesses from utilizing digital platforms to target potential customers. L.D. 1977, *An Act to Create the Data Privacy and Protection Act*, would have undermined business's ability to compete through e-commerce, making Maine an outlier. On the retail side, businesses would be limited in how they online market to Maine consumers and therefore, would need to spend more dollars to market their products online to ensure it gets in front of the correct audience. Maine's hospitality and tourism industries would also have a more difficult time competing online with large, well-established restaurants and lodging facilities as they would not be able to promote their business through first party advertising, which has become an integral party of online marketing. The bill passed 75 – 70 in the Maine House and failed 18 – 15 in the Senate.

The Chamber believes now is the time to create consistency across state borders and reflect the current market for e-commerce. Federal legislation is imperative to avoid a patchwork of state

privacy laws that would create confusion for both consumers and businesses and fail to protect sensitive data. As a result, we welcome the introduction of the *American Privacy Rights Act* by Senator Cantwell and Representative McMorris Rodgers. The implementation of a comprehensive federal data privacy law will provide much-needed clarity and consistency for businesses and consumers alike. The legislation has advanced in the House of Representatives Energy and Commerce's Subcommittee on Innovation.

While the Chamber requests your support of this legislation, we encourage your careful consideration of specific provisions included in the APRA draft and believe there are a couple areas where it could be improved. Specifically, the Chamber believes a national data privacy law should fully preempt current and future state privacy laws. Failing to include clear preemption language may enable more confusion and compliance challenges as states seek to pass individual privacy laws with restrictions beyond a national standard. While the legislation includes preemption language, it could be strengthened to ensure state consistency. We also recommend that comprehensive data privacy legislation include clear enforcement overseen by the Federal Trade Commission and state attorney generals. The APRA draft also includes a Private Right of Action (PRA), which the Chamber believes could lead to frivolous and costly litigation, as has been displayed in Illinois where their Biometric Information Privacy Act includes a PRA.

Again, the Maine State Chamber of Commerce appreciates your consideration and urges Congress to pass a national data privacy law this session to ensure businesses can remain innovative and competitive, and consumers have understandable and uniform privacy protections across state lines.

Sincerely,

Patrick Woodcock
President and CEO
Maine State Chamber of Commerce



May 13, 2025

The Honorable Anne Carney, Chair
The Honorable Amy Kuhn, Chair
Maine Committee on Judiciary
c/o Legislative Information Office
100 State House Station
Augusta, ME 04333

RE: Oppose Unless Amended - LD 1822, an Act to Enact the Maine Online Data Privacy Act

Dear Chair Carney, Chair Kuhn and Members of the Maine Committee on Judiciary.

On behalf of the Securities Industry and Financial Markets Association,¹ we thank you for the opportunity to provide comments on LD 1822, which would enact the Maine Online Data Privacy Act. SIFMA brings together the shared interests of hundreds of securities firms, banks and asset managers located throughout Maine and across the country. There are more than 23,500 people employed by the financial services industry in Maine, including more than 1,700 of employees in the securities industry.² SIFMA's mission is to support a strong financial services industry, investor opportunity, capital formation, job creation, and economic growth.

SIFMA commends the Committee for its dedication to protecting the privacy of Maine residents. Financial services firms remain committed to protecting the privacy of our consumers and ensuring compliance with the robust laws governing privacy in the industry. However, as drafted, this bill would create unnecessary, overlapping, and problematic requirements that could negatively impact both Maine's securities firms and investors. SIFMA respectfully requests the amendments below:

1. The Gramm-Leach Bliley Act ("GLBA") exemption should be revised by striking lines 7 through 10 on page 8 and replacing them with the following: "E. Any financial institutions and affiliates subject to Title V of the Gramm-Leach-Bliley Act, 15 USC 6801 et seq.;"
2. On page 20, include language to allow broker dealers to comply with regulations and investigations conducted by our primary regulator – the Financial Industry Regulatory Authority ("FINRA") – a non-governmental regulator designated by Congress to oversee the securities industry: "A. Comply with federal laws or regulations, or regulations of a self-regulatory organization as defined by United States code title 15, section 78(a)(26) and the laws and rules of the State or local laws and ordinances."

¹ SIFMA is the leading trade association for broker-dealers, investment banks and asset managers operating in the U.S. and global capital markets. On behalf of our industry's one million employees, we advocate on legislation, regulation and business policy affecting retail and institutional investors, equity and fixed income markets and related products and services. We serve as an industry coordinating body to promote fair and orderly markets, informed regulatory compliance, and efficient market operations and resiliency. We also provide a forum for industry policy and professional development. For more information, visit <http://www.sifma.org>.

² US Department of Labor - Bureau of Economic Analysis (2023)

The Importance of a GLBA Entity-Level Exemption

Currently, LD 1822 includes a limited exemption for data collected, processed, sold, or disclosed pursuant to GLBA. The law, originally enacted in 1999, provides a comprehensive federal regime that governs financial institutions' privacy and data protection controls, including the disclosure of privacy practices to customers, cybersecurity controls, and restrictions on the unauthorized sharing of nonpublic personal information. This law comes with significant oversight and enforcement by financial regulators. Additionally, the Securities and Exchange Commission adopted Regulation S-P – which sets securities industry-specific privacy requirements based on GLBA – just one year later.

Financial services firms covered by GLBA and Regulation S-P already have comprehensive, mature, and effective privacy programs in place. LD 1822 could disrupt those programs and negatively impact both Maine residents and businesses. In fact, the potential confusion that LD 1822 could create may potentially put residents at increased risk from bad actors.

Such confusion would largely stem from the fact that the GLBA explicitly applies to covered entities. As such, covered financial services firms generally treat all customer data the same way, regardless of how or why it was collected. This means that, functionally, all data collected or processed by GLBA-covered financial services firms receive GLBA protection. However, while most data processed by GLBA-covered entities would likely be considered “collected, processed, sold, or disclosed” pursuant to the GLBA, that is not necessarily clear for all data. LD 1822 would require differentiation of this data, which could lead to harmful unintended outcomes. For instance, the GLBA contains important provisions related to the prevention of fraud – provisions that align with Maine's senior investor protection program – which LD 1822 could disrupt.

Moreover, requiring the information to be dissected into categories – each governed by different laws – would impose a significant compliance burden on financial services firms and increase customer confusion. Even consumers that request the deletion of or changes to data determined to be outside the GLBA may still have their request denied because that data is subject to other federal laws or regulations (e.g., retention periods established by securities regulators), while also possibly losing GLBA protections. Consumers are unlikely to know or care which data is collected, processed, sold, or disclosed pursuant to the GLBA, yet they know when they are dealing with their bank, brokerage firm, or investment adviser and providing a uniform standard of care across all of a firm's data is critical to positive outcomes.

For the reasons above we urge you to consider adding an exemption for GLBA-covered entities and their affiliates.

Safeguard Investor Protections Provided by the FINRA and other Self-Regulatory Organizations

A further potential consequence of requiring firms to differentiate between GLBA-covered data or systems and Maine Online Data Privacy and Act-covered data or systems is that LD 1822 could be used by bad actors to frustrate the investor protections put in place by the industry's non-governmental regulators.

FINRA is a non-governmental regulator that operates pursuant to authority granted to it by the Securities Exchange Act. Generally, federal law requires all broker-dealers to register with FINRA –

and to obtain and maintain that registration, a broker-dealer must comply with FINRA's SEC-approved investor protection rules.

This includes protections regarding internal inspections, monitoring employee interactions with customers, reporting suspicious activity to the relevant authorities, and documenting suspicious activity – among many other items. As drafted, this bill could empower bad actors to erase or change their data in firm systems, require firms to share investigatory information with bad actors, restrict firms from making reports to outside authorities, or require firms to delete information necessary to fulfill their regulatory obligations. It is imperative that this bill is updated to recognize the critical role FINRA plays in investor protection and allow firms to continue to comply with their unique regulatory obligations.

Thank you in advance for your time and consideration. Effective data privacy protections are more important than ever before, and we would like to work with your committee to better align the proposal with longstanding federal law and consumer protections. We appreciate your willingness to consider our concerns. If you have any questions, please contact me at (212) 313-1211 or sklarer@sifma.org.

Sincerely,

/s/

Stephanie I. Klarer

Assistant Vice President

SIFMA



May 29, 2025

The Honorable Anne Carney
The Honorable Amy Kuhn
100 State House Station
Augusta, Maine 04333

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

The Business Software Alliance¹ supports strong privacy protections for consumers and appreciates your work on LD 1822. Although we share the goal of protecting privacy, we are concerned about how LD 1822 will work in practice — including its potential to prevent companies from developing new technologies and improving existing ones, even when doing so aligns with consumer expectations.

BSA is the leading advocate for the global software industry. Our members are enterprise software and technology companies that create the business-to-business products and services used across every sector of the economy. For example, BSA members provide cloud storage services, customer relationship management software, human resource management programs, identity management services, and collaboration software. In our advocacy, BSA works to advance legislation that ensures consumers' rights — and obligations imposed on companies — function in a world where different types of companies play different roles in handling consumers' personal information.

We are concerned that LD 1822 risks freezing technology as it exists today. We strongly recommend revising the bill to ensure that companies can responsibly develop new products and services, in line with consumer expectations. We realize that LD 1822 incorporates the data minimization standard from Maryland's recently-adopted privacy law — and is intended to limit the amount of personal data that companies collect. However, this language does not clearly recognize that companies may need to process personal data to improve existing products they provide to consumers or develop new ones that consumers are likely to want. As consumers, all of us want our technology to work better in 10 years than it does today — but the bill's language risks freezing technology in place, by failing to provide a clear path for product improvement and development.

We recommend revising the bill to clearly recognize that companies can process personal data to improve and develop products responsibly, in ways that align with consumer expectations.

¹ BSA's members include: Adobe, Alteryx, Asana, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cohere, Dassault Systemes, Databricks, Docusign, Dropbox, Elastic, EY, Graphisoft, HubSpot, IBM, Informatica, Kyndryl, MathWorks, Microsoft, Notion, Okta, OpenAI, Oracle, PagerDuty, Palo Alto Networks, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Trend Micro, TriNet, Workday, Zendesk, and Zoom Communications Inc.

One option is to revise the bill's exemptions, in Section 9613. That provision currently permits companies to process personal data for a narrow set of internal uses — and can be revised to expressly allow responsible product development and improvement. Specifically, we recommend revising Section 9613.2 to state:

2. Internal use. The obligations imposed on a controller or processor under this chapter do not restrict a controller's or processor's ability to collect, use or retain personal data for internal use to:

A. Effectuate a product recall;

B. Identify and repair technical errors that impair existing or intended functionality; or

C. Perform internal operations that:

(1) Are reasonably aligned with the expectations of the consumer or can be reasonably anticipated based on the consumer's existing relationship with the controller; or

(2) Are otherwise compatible with processing data to provide a product or service specifically requested by a consumer or performing under a contract to which the consumer is a party, including improving existing products or developing reasonably-related new products.

This approach would also ensure that when companies process data to improve or develop products, they comply with a separate data minimization provision that limits the processing of data under the bill's list of exceptions. That provision, in Section 9613.7, requires that any personal data processed pursuant to an exception in the bill is only processed to the extent that the processing is:

A. Subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and reduce reasonably foreseeable risks of harm to consumers relating to the collection, use or retention of personal data;

B. Reasonably necessary and proportionate to the purposes listed in this section; and

C. Adequate, relevant and limited to what is necessary in relation to the specific purposes listed in this section.

Our recommended change would therefore incorporate this further safeguard. We would welcome a chance to discuss this recommendation with you, and to talk more broadly about the practical impact of the bill's data minimization language.

In addition to our concerns about LD 1822's approach to data minimization, we also have several practical concerns about how the bill would function in practice. These include:

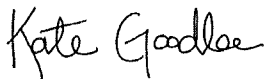
- Ensuring processors can protect consumers' personal data without unnecessary delays. Section 9609.1(6) requires processors to give controllers the opportunity to object to subprocessors. While we agree that a consumer's data should be protected when it is handled by subprocessors,

we strongly recommend a different approach: requiring processors notify a controller about the use of a subprocessor and pass on the processor's obligations to that subprocessor. This is important because subprocessors are frequently used to provide services consumers rely on. A processor will often rely on dozens (or more) subprocessors to provide a single service. In some cases, a processor may need to quickly replace a subprocessor — like when a subprocessor has a security breach. In other cases, a processor may offer a service that depends on bringing together a specific group of subprocessors — so objecting to one subprocessor prevents use of the service altogether. We urge you to avoid these concerns and revise Section 9609.1(6) to state:

- ~~After providing the controller an opportunity to object, e~~ Engage any subcontractor to assist with processing personal data on the controller's behalf only in accordance with a written contract that requires the subcontractor to meet the processor's obligations regarding the personal data under the processor's contract with the controller.
- Clarify that the use of an algorithm alone does not trigger a data protection assessment. Section 9611.1 requires companies to conduct data protection assessments for activities that present a heightened risk of harm to consumers. It lists specific scenarios that cause such risk. However, Section 9611.2 states that a controller is to conduct a data protection assessment for "each of the controller's processing activities that present a heightened risk of harm to a consumer, *including an assessment for each algorithm that is used.*" This language is ambiguous — and we strongly recommend clarifying that the use of an algorithm alone does not require a data protection assessment. Instead, the bill should clarify that assessments for activities that present a heightened risk of harm to consumers (as identified in Section 9611.1) should include an assessment of any relevant algorithms. We recommend revising Section 9611.2 to state:
 - A controller shall conduct and document a data protection assessment for each of the controller's processing activities that present a heightened risk of harm to a consumer, and such assessments shall consider any ~~including an assessment for each~~ algorithms that are is used.

Thank you for considering our views. We welcome an opportunity to further engage with you or a member of your staff on these important issues.

Sincerely,



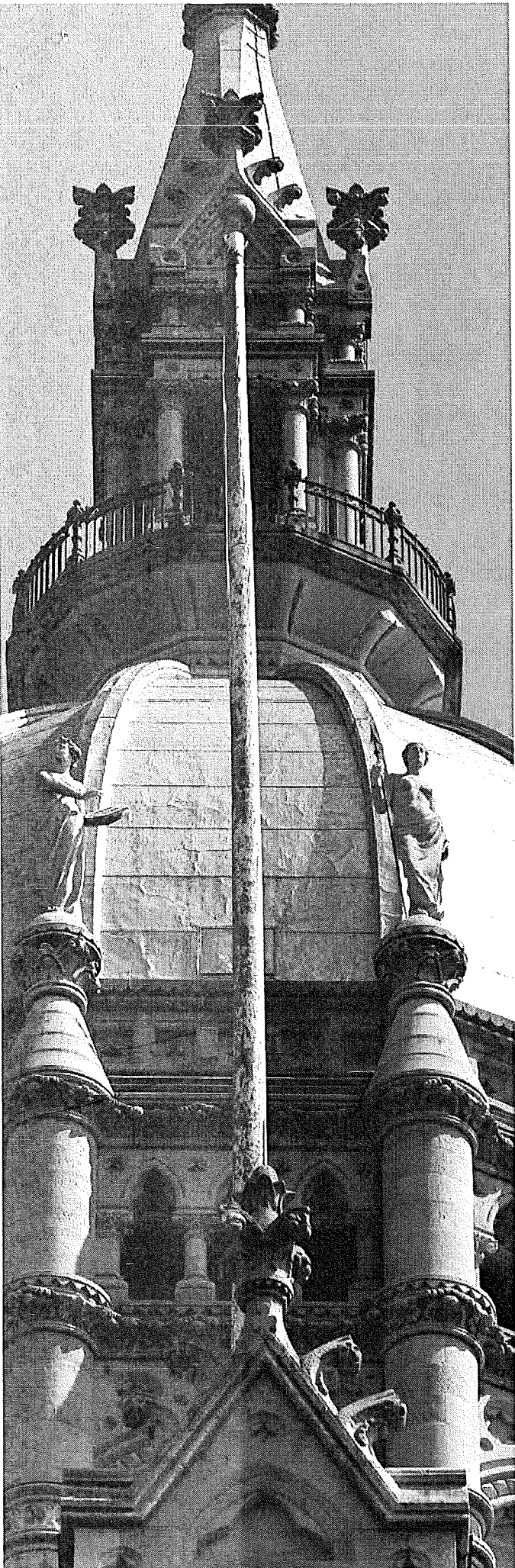
Kate Goodloe
Managing Director, Policy
Business Software Alliance

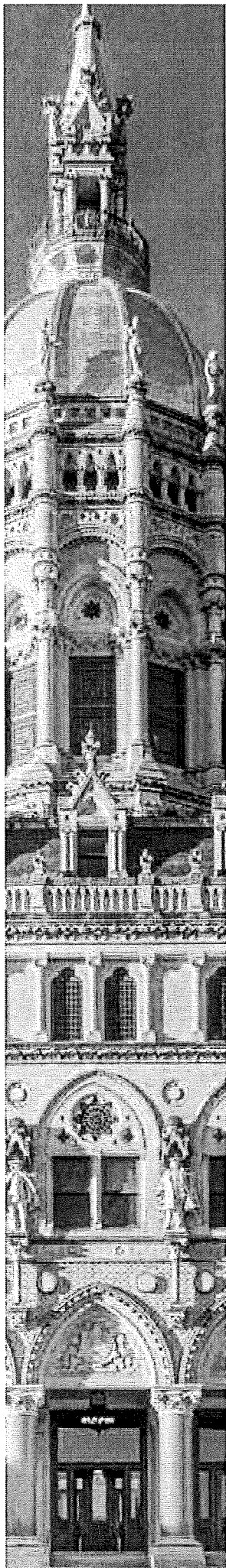
UD 822



UPDATED ENFORCEMENT
REPORT PURSUANT TO
CONNECTICUT DATA PRIVACY
ACT, CONN. GEN. STAT. § 42-515,
ET SEQ.

April 17, 2025





The Office of the Attorney General (“OAG” or “Office”) is issuing this updated enforcement report (“Updated Report”) under the Connecticut Data Privacy Act (“CTDPA” or “Act”), Conn. Gen. Stat. § 42-515, et seq., to highlight common deficiencies and problematic privacy practices that we are investigating and/or addressing under the Act. The OAG issued our initial CTDPA Enforcement Report (“Initial Report”) on February 1, 2024,¹ which covered the first six months of enforcement. Now that the CTDPA has been in effect for over a year, we issue this Updated Report covering calendar year 2024 as part of our ongoing efforts to be transparent about our compliance expectations and enforcement priorities.

Since our Initial Report, the OAG has continued to take significant steps to prompt compliance with the CTDPA. We have now issued dozens of notices of violation (“cure notices”), as well as a number of broader information requests, under the Act. We remain focused on key aspects of the CTDPA related to transparency in public-facing privacy notices and sensitive data processing, among other areas, but have also broadened our efforts to address problematic cookie use banners and dark patterns that trick consumers. Our priorities have also expanded as new legislation related to minors’ privacy and consumer health data took effect, and as our universal opt-out provisions came online.

In this Updated Report, we provide an update on (1) the OAG’s broader privacy and data security efforts; (2) consumer complaints received under the CTDPA to date; (3) several enforcement efforts highlighted in our Initial Report; and (4) our expanded enforcement priorities. As in our Initial Report, this Updated Report concludes with recommendations for strengthening the CTDPA’s protections.

Broader Privacy Efforts

Even before passage of the CTDPA, Connecticut has long been recognized as a leader in the privacy space—the OAG was the first office in the country to create a standalone Privacy Section. In addition to enforcing the CTDPA, the Privacy Section also advises the Attorney General regarding the enforcement of various other state and federal privacy laws, including Connecticut’s data breach notification statute (Conn. Gen. Stat. § 36a-701b), Safeguards Law (Conn. Gen. Stat. § 42-471), and the Connecticut Unfair Trade Practices Act (“CUTPA”), as well as the federal Health Insurance Portability and Accountability Act (“HIPAA”) and Children’s Online Privacy Protection Act (“COPPA”). The Privacy Section undertakes a wide range of activities that protect the privacy of Connecticut consumers.

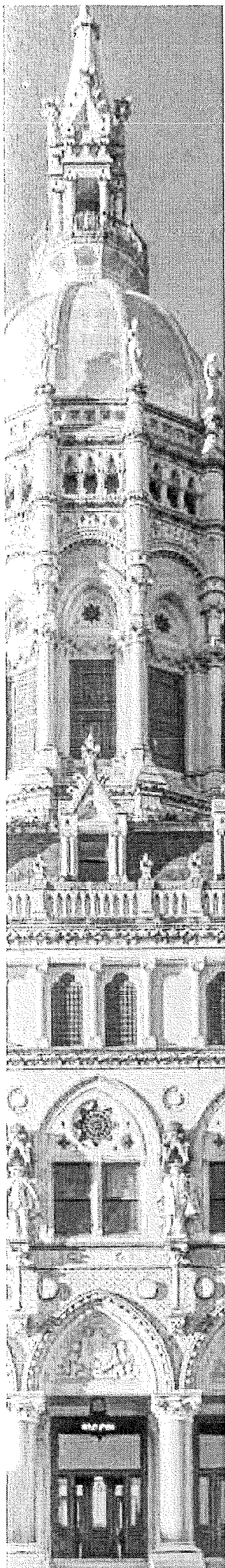
Breach Notice Review

As noted in our Initial Report, the Privacy team reviews all data breaches reported to the Office under Connecticut’s breach notice statute. The number of breach notices received by the OAG has increased dramatically over the years—in 2024, the OAG received 1,900 breach notifications.² We review each notification for compliance with our breach notice and data security laws, and frequently follow up with companies for further details concerning notice timelines, the privacy protections offered to affected residents, the safeguards in place at the time of the breach, and post-breach remedial measures.

In our Initial Report, we highlighted that we had begun issuing “warning letters” to companies concerning lengthy breach notice timelines. Connecticut law requires that notice be provided both to the OAG and Connecticut residents without unreasonable delay, but not later than sixty (60) days after breach discovery. See Conn. Gen. Stat. § 36a-701b(b)(1). Our warning letters are aimed at addressing a troubling trend of breach notice timelines stretching out many months from breach discovery in violation of Connecticut law.

[1] Under the CTDPA, the OAG was mandated to make a report (“Initial Report”), no later than February 1, 2024, to include: (1) the number of notices of violation the Attorney General has issued; (2) the nature of each violation; (3) the number of violations cured; and (4) any other matter the Attorney General deemed relevant.

[2] The Office received over 800 data breach notifications in 2019, 1,200 in 2020, over 1,500 both in 2021 and 2022, and approximately 1,800 in 2023.



delays. In these letters, we continue to stress that we view the statutory notice period to run from the date that a company becomes aware of suspicious activity, not the date it determines the full impact to personal information.³ Further, we underscore that Connecticut residents must receive notice of a data breach as soon as possible so that they may take appropriate steps to protect themselves from identity theft.

More recently, we have taken these efforts a step further, pursuing several breaches involving egregious notice timelines and requiring Assurances of Voluntary Compliance (“AVCs”) from the reporting companies. These AVCs, among other things, require the companies to implement clear incident response and notification plans, and provide timely notice of data breaches going forward. The AVCs also require payments to the State reflective of the impact to Connecticut residents, and as a penalty for failure to comply with Connecticut law. Our Office will continue to take this approach, as well as consider more formal action, to address notice delays going forward. Companies that have received a prior warning letter and subsequently report any new breaches outside the statutory timeframe may be subjected to even higher penalties as willful violations of the law.

Data Breach Investigations & Recent Settlements

In addition to breach notice efforts, the Privacy Section is currently leading or assisting with numerous state-specific or multistate investigations of large-scale data breaches and other high-profile matters implicating consumer privacy.⁴ For example, our team responded quickly to the massive data breach at Change Healthcare (“Change”), that impacted more than one-third of the U.S. population. This incident is the largest-ever healthcare-related security breach. It crippled the healthcare industry, jeopardized countless healthcare providers’ solvency and ability to treat patients, and created serious risks of individual harm through scams and identity theft.

Further, within the past year, the Section has negotiated and entered into a number of important settlements setting robust data security and privacy expectations, including in cases like Enzo Biochem, Guardian Analytics, and Marriott. Marriott in particular has been lauded as a benchmark-setting resolution— in that case, a coalition of 50 attorneys general co-led by Connecticut, reached a settlement with Marriott after an investigation into a large multi-year data breach of one of its guest reservation databases. Under the settlement, Marriott agreed to strengthen its data security practices using a dynamic risk-based approach, provide important consumer protections, and make a \$52 million payment to the states.

Legislative Work & Outreach

Along with our enforcement work, the Privacy Section continues to monitor federal and state privacy and data security initiatives and provides the Attorney General with counsel on proposed legislation. The Section participates in various National Association of Attorneys General (“NAAG”) working groups involving data security and privacy issues, including co-leading a subgroup of states focused on consumer data privacy legislation. Further, the Section continues to engage in extensive outreach to constituents, community groups, and businesses about data security and privacy in Connecticut, including specific education efforts focused on the CTDPA.

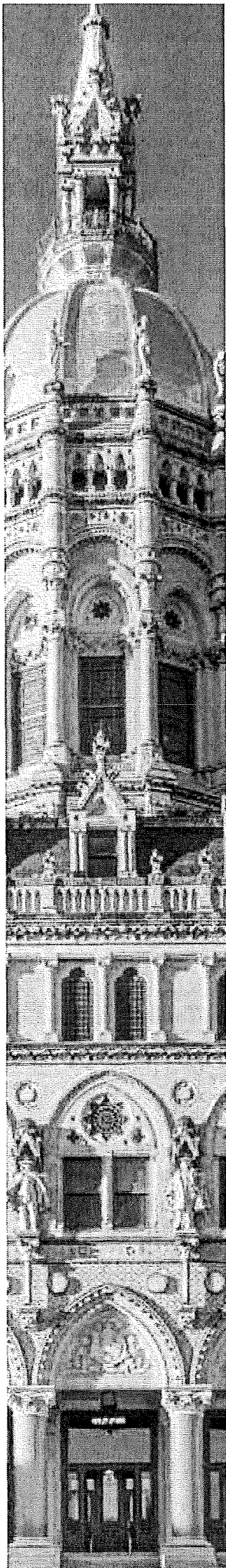
Most recently, we have updated our CTDPA FAQ page to highlight the Act’s consumer health data, minors’ privacy, and the universal opt-out provisions. We have also developed additional resources for consumers to learn how to send their opt-out preference signal (“OOPS”), and for businesses seeking to configure their online services to honor the Global Privacy Control (“GPC”) signal.⁵ On December 30, 2024 Attorney General Tong issued a press release regarding the universal opt-out provisions, emphasizing that this is a key step forward for consumer privacy rights and urging consumers to take advantage of this right to control their data.⁶

[3] See also 2022 Office of Civil Rights Cybersecurity Newsletter (“the time period [for reporting] begins when the incident is first known, not when the investigation of the incident is complete, even if it is initially unclear whether the incident constitutes a breach as defined in the rule.”) (quoting Modifications to HIPAA Rules, 1/25/13).

[4] In the past several years, working with multistate partners, the Section has entered into a number of key settlements setting robust data security and privacy expectations, including in cases like Equifax, Uber, Anthem, Target and Home Depot, Experian/ TMobile, Google Location Tracking, Easy Healthcare/ Premium, Immediate, Blackbaud, and Morgan Stanley.

[5] See The Connecticut Data Privacy Act FAQ page, CTDPA Universal Opt Out Resources (updated Jan. 29, 2025), <https://portal.ct.gov/ag/sections/privacy/the-connecticut-data-privacy-act>.

[6] Press Release, Connecticut Office of the Attorney General, Attorney General Tong advises Connecticut consumers and businesses of opt out rights and requirements (Dec. 30, 2024), <https://portal.ct.gov/ag/press-releases/2024-press-releases/tong-advises-connecticut-consumers-and-businesses-of-opt-out-rights->



The Privacy Section continues to field privacy-related consumer complaints. Since our Initial Report, the OAG has received a steady volume of complaints under the CTDPA. Though it's been over a year since the CTDPA's passage, many complaints involve consumers' unsuccessful attempts to exercise data rights. It should not require our Office's intervention for Connecticut residents' data requests to be processed and honored. Further, we continue to receive complaints regarding websites that combine public records and post individual "profiles" online, which profiles are often extensive, unwanted and inaccurate. The profiles cross the line from public to private and underscore the need for legislative fixes to address the too-broad exemption related to "publicly available information."

In addition to complaints related to the CTDPA, our Office has received over one hundred complaints related to data breaches this year alone. Frequently, companies send data breach notices that are vague and do not sufficiently explain to Connecticut residents why they are receiving the notice— data breach letters sent to Connecticut residents must make clear who the company is, why they have the impacted individual's data, and what specific personal information was compromised.

Early Enforcement Efforts— Updates & Takeaways

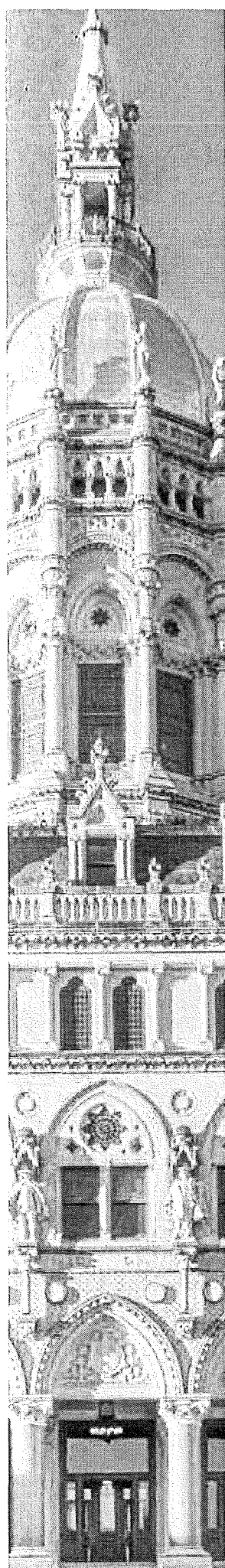
While many of the matters highlighted in our Initial Report remain ongoing, including investigations related to genetic information, geolocation data, and minors' data, we wanted to take this opportunity to highlight several key takeaways from our early enforcement efforts that we hope will provide insight regarding our Office's compliance expectations going forward.

Privacy Notices

As noted in our Initial Report, the CTDPA's transparency requirements are a crucial component of the law— these provisions ensure that Connecticut residents have insight into the collection, use and sharing of their personal data, understand their new data rights, and are able to exercise those rights. The OAG has continued to review companies' privacy notices and the functionality of consumer rights mechanisms under the CTDPA.

We have now issued three separate "privacy notice sweeps" consisting of over two dozen cure notices in total, all aimed at addressing privacy notice deficiencies. As noted in our Initial Report, we have seen many prompt and positive responses to these cure notices— with nearly all companies having taken steps to come into compliance. In particular, companies addressed flagged deficiencies by:

- incorporating the CTDPA and specific mention of all of its consumer data rights;
- incorporating, bolstering, or fixing consumer rights request mechanisms, including adding clear and conspicuous links to opt out of targeted advertising and the sale of personal data;
- incorporating and enhancing disclosures regarding the requisite consumer appeal process;
- strengthening disclosures concerning the processing and sharing of personal data, including sensitive data;
- reformatting privacy notices into a dedicated webpage with clear spacing, typeface, and type size;
- removing language limiting consumers' rights to access or to request a copy of their personal data only to data collected within the last twelve months, where no such limit exists in the CTDPA (or several other state data privacy acts for that matter);
- removing language implying a limit to the number of times a consumer may exercise certain data rights;
- removing language implying that the company will charge consumers for the exercise of data rights by default, as opposed to only for manifestly unfounded, excessive or repetitive requests; and
- removing conflicting language in privacy notices (i.e., where a company stated they did not process data for sale whereas other disclosures indicated that such sales were occurring).



Despite these efforts, we continue to find company privacy notices with glaring racial deficiencies. Indeed, although we are now well after the CTDPA's effective date, we continue to come across privacy notices that have not been updated for years. As more and more states' consumer data privacy laws come online, companies that have not engaged in any effort to update their privacy notices will not be in compliance with these laws. Companies should consider all privacy notices and public-facing representations to be under review.

We are also troubled by privacy notices that create a misimpression that consumer rights are exclusive to residents in only one state, or only in certain states, and that are not sufficiently inclusive of states that have enacted consumer data privacy laws. While companies do not necessarily need to include separate sections in privacy notices for every state that has passed or will pass a comprehensive consumer data privacy law, companies must avoid language that creates ambiguities over whether Connecticut residents have data rights, or conversely, that create the false impression that Connecticut residents lack those rights. There is no excuse for privacy notices that confuse or mislead Connecticut residents about their data rights or that ultimately deter them from exercising those rights.

Further, we underscore the need for companies to be proactive and responsive to our cure notices, notices of violation, and requests for additional information. By and large, companies have shown good faith efforts to bring their notices into compliance and have worked diligently to respond to the deficiencies we have flagged. However, where companies have not done so, we have taken and will continue to take more formal steps to ensure that those concerns are addressed and prioritized going forward.

Just as companies must promptly respond to our Office, they should prioritize consumer rights requests. By honoring valid requests, companies will avoid consumers submitting complaints to our Office. Companies must ensure that they have properly functioning data rights mechanisms and sufficient internal processes in place to timely review all consumer inquiries and requests.

Facial Recognition Technology

In our Initial Report, we noted that the OAG sent a cure notice after becoming aware of media reports and receiving consumer complaints regarding a Connecticut supermarket's use of biometric software for purposes of preventing and/or detecting shoplifting. This led the OAG to carefully consider more broadly Connecticut retailers' use of facial recognition technology ("FRT") as a loss-prevention tool under the CTDPA. While our Office is unable to provide legal advice, we are now providing informal guidance to ensure that Connecticut residents' privacy rights are respected and upheld by businesses choosing to deploy FRT despite its inherent and significant risks to consumers.⁷

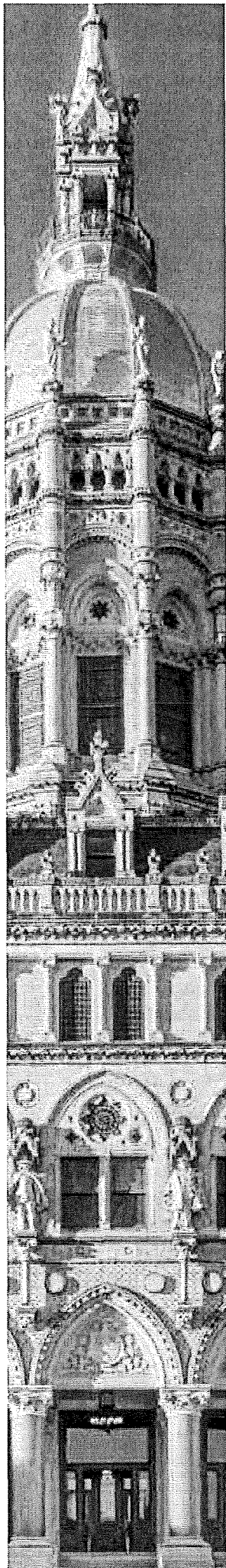
By its nature, FRT involves the collection, use, and sometimes sharing of consumers' biometric information. The CTDPA defines sensitive data to expressly include biometric data⁸ and appropriately sets forth heightened protections for such data. While the CTDPA contains a so-called crime/fraud exception, this is *not* a blanket exception.⁹ Further, key requirements related to data minimization, purpose limitation, and data security apply even where an exception allegedly exists.¹⁰ In other words, businesses that deploy FRT must comply with the CTDPA—there is no "out" on compliance.

[7] This informal guidance does not confer any rights on any person and does not operate to bind the OAG or the public. This guidance further does not preempt federal, state, or local laws, or impact the OAG's enforcement authority under the CTDPA or other applicable statutes.

[8] "Sensitive data" means personal data that includes ... (B) the processing of genetic or biometric data for the purpose of uniquely identifying an individual, ... (Conn. Gen. Stat. § 42-515(27)).

[9] See Conn. Gen. Stat. § 42-524(a)(9) ("Nothing... shall be construed to restrict a controller's, processor's or consumer health data controller's ability to prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or any illegal activity...").

[10] Conn. Gen. Stat. § 42-524(f).



accessible, clear, and meaningful notice about the use of FRT.¹¹ Such disclosures should clearly point consumers to their rights related to such data. Transparency is critical, especially given that the CTDPA requires that businesses obtain consumers' affirmative consent for the processing of sensitive data¹² and that such consent must be, among other things, *informed* and *freely given*.¹³ Additionally, businesses must provide an effective mechanism for consumers to revoke consent and honor consumers' requests to do so.¹⁴

Under the CTDPA, businesses that use FRT must conduct Data Protection Assessments ("DPAs") as processing sensitive data poses a heightened risk of harm to consumers.¹⁵ While the CTDPA does not dictate a format for DPAs, the scope and detail in DPAs involving FRT should reflect its significant, and well documented, potential impact to consumers' civil liberties. DPAs must carefully assess and document whether and how any benefits from FRT outweigh the serious risks posed to individuals' privacy rights.¹⁶

Businesses that choose to deploy FRT should actively monitor its use through DPAs. For example, businesses should track the number of true and false positive identifications and understand whether these correlate with demographic differences that may result in discrimination. This is particularly important given that the CTDPA prohibits businesses from processing personal data in a manner that unlawfully discriminates against consumers.¹⁷

Prior to deploying FRT, businesses should adopt strong policies and procedures related to conducting and documenting DPAs, including an appropriate risk rating methodology, as well as implementing FRT-specific bias and discrimination training for all relevant stakeholders. When using FRT, businesses should capture outcomes of alerts and notifications for feedback and training purposes. Businesses should also continue to monitor the impacts of technological changes to FRT and repeat DPAs upon substantial changes to the system or trends in the observed data.

Businesses deploying FRT should pay special attention to the CTDPA's requirements around data minimization, purpose limitation, and data security— these provisions are at the heart of the CTDPA and become even more significant in the context of FRT. Businesses must limit the amount of personal data processed through FRT, as well as establish and uphold clear data retention and deletion policies and procedures for biometric data. Further, businesses must only process biometric data according to the specific purpose for which such data was collected. Finally, businesses must implement and maintain a comprehensive information security program to protect personal data processed through FRT, including but not limited to strict access controls, multi-factor authentication, and appropriate segmentation.

We have included this informal guidance to provide baseline expectations for businesses that choose to deploy FRT, but it is not exhaustive. Because of FRT's inherent risks and the heightened potential for harm, businesses must seriously consider all consumer rights and privacy obligations under the CTDPA prior to deployment.¹⁸ This guidance is not a blessing or an endorsement of the use of FRT. Given that FRT and related legislation are quickly evolving, this guidance is subject to change.

Marketing and Advertising Practices

In our Initial Report, we noted that the OAG sent an inquiry letter to a national cremation services company based on a complaint from a Connecticut resident who received an advertisement in the mail from them after recently completing chemotherapy. Based on our review, we later issued a cure notice to the cremation services company, as well as inquiry letters to the data analytics firm that identified the individual for the marketing list and the data broker that supplied the data at issue.

[11] See Conn. Gen. Stat. §§ 42-520(c), et seq.

[12] Conn. Gen. Stat. §§ 42-515(7) and 42-520(a)(4).

[13] Conn. Gen. Stat. § 42-515(7).

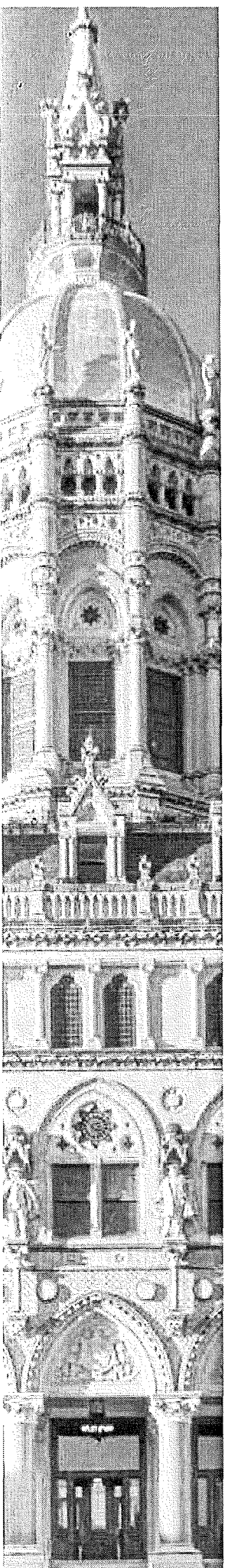
[14] Conn. Gen. Stat. § 42-520(6).

[15] Conn. Gen. Stat. § 42-522(b).

[16] Conn. Gen. Stat. § 42-522(b).

[17] Conn. Gen. Stat. § 42-520(a)(5).

[18] While this informal guidance focuses on the application of the CTDPA to FRT, businesses deploying this technology must ensure that they also comply with other applicable privacy and consumer protection laws, including CUIPA.



identify recipients for the mailer at issue, we determined that the attributes used were name, age, and zip code only. Nonetheless, as a result of our cure notice, the cremation services company updated its privacy notice to disclose the processing of personal data obtained from third-party data analytics and marketing firms, as well as to identify the specific categories of personal data obtained from those firms. Ultimately, this matter illustrates how even the processing of non-sensitive data for advertising can lead to unwanted effects akin to the misuse of sensitive data. This is especially true in industries that involve sensitive topics such as cremation services and companies should exercise heightened caution and oversight when engaging in advertising in these types of industries.

In our broader investigation, we also pushed the data analytics firm to closely consider the CTDPA's requirements and, as a result, the firm has committed to suppress all sensitive data attributes for Connecticut residents in all future marketing campaigns. Finally, we are continuing to review the sensitive data practices of data brokers at issue, as well as data brokers more broadly, including as informed by insights drawn from this matter. Our Office will continue to focus on the entire data flow and we have encouraged legislative changes that will make it easier for Connecticut residents to understand all of the entities that may have their data so that they can best exercise their data rights.

Palm Recognition

We highlighted in our Initial Report that the OAG sent an inquiry letter to a major web service provider and retailer after the company announced its plans to widely deploy its palm recognition service across the U.S., including in Connecticut stores. We sought to understand what steps the retailer had taken to ensure that its roll-out was done in compliance with the CTDPA. We paid close attention to the company's disclosures and consent process, with a particular focus on the CTDPA's requirement that such consent be informed. The company worked with us to provide answers to our inquiries and we were able to address our concerns upfront. This matter is an example of how a cooperative and forthcoming approach to OAG inquiries can yield a productive and positive result.

Connected Vehicles

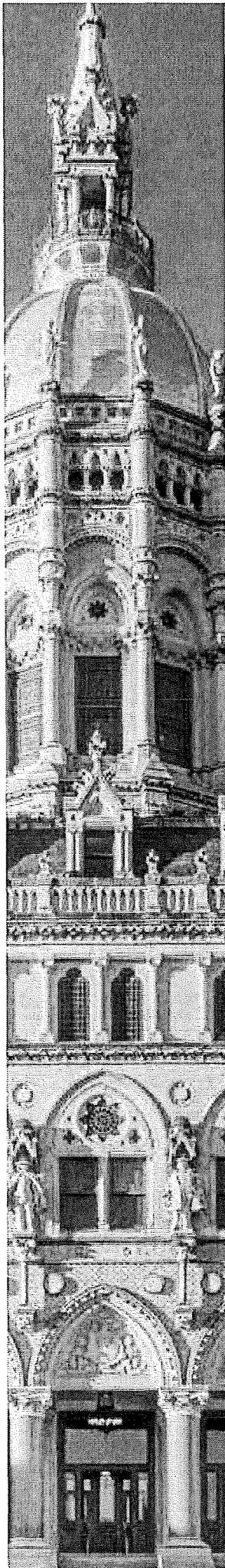
As noted in our Initial Report, the OAG sent a cure notice, as well as broader inquiries, to a large car manufacturer after public reports raised concerns that connected vehicles were collecting and sharing a range of highly personal data about consumers. As a result of our cure notice, the company quickly updated its privacy notice to clarify what personal data is collected from consumers as opposed to employees. We have since expanded our review to include other car manufacturers, which matters remain ongoing.

Genetic Data

In our Initial Report, we noted that the OAG had issued an inquiry letter to a genetic testing and ancestry company, seeking details related to a data security incident that exposed sensitive records for over seven million users. Our investigation is ongoing— in addition to reviewing the data security incident itself, we are focused on the company's compliance with applicable privacy laws, including the CTDPA. Our Office would like to remind Connecticut residents to use extreme caution when a business asks them to turn over highly sensitive personal data like genetic data. Connecticut residents should also keep in mind their important data rights under the CTDPA, including the right to delete their personal data, opt out of the sale of their data, and revoke consent for the processing of such data.

Teens' Data

In our Initial Report, we highlighted that the OAG sent a cure notice to a company in connection with its anonymous peer messaging app directed at teens after a children's advocacy group raised concerns that the app is inherently harmful to minors. This prompted us to review the company's practices under the CTDPA, among other laws. This matter underscores why the CTDPA's thresholds should not apply to the processing of minors' data— the law should not require that a company collect data from tens of thousands of minors for the Act to apply.



Problematic Opt-out Mechanisms/ Dark Patterns

As part of the next wave of our enforcement efforts, we have expanded our focus to include not just privacy notices but also cookie banners. Through our review, we identified a number of cookie banners that undermine or even override consumers' ability to make important privacy choices, including the right to opt out of targeted advertising or the sale of their personal data through the use of tracking technologies. In the Fall of 2024, we issued a cure notice sweep aimed at addressing these problematic practices, and have identified additional companies for a second sweep.

Under the CTDPA, if a controller sells personal data to third parties or engages in targeted advertising, the controller "shall clearly and conspicuously disclose such processing, as well as the manner in which a consumer may exercise the right to opt out of such processing." Further, the CTDPA prohibits controllers from obtaining consumers' consent through the use of dark patterns. A "dark pattern" is defined as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice..."¹⁹

The cookie banners that we flagged violate these provisions of the CTDPA, and likely CUTPA, by failing to provide consumers with a symmetrical choice- meaning that the path for a consumer to "opt out" of targeted advertising or sale (the more privacy-protective option) is more difficult or time-consuming than the path to "opt in" (the less privacy-protective option).

For example, one of our target companies utilizes a cookie banner that allows the consumer to "opt in" to the use of cookies by clicking on an "AGREE" button, which is prominently highlighted in color. By contrast, to "opt out," the consumer must click on "SHOW PURPOSES," and then navigate to an entirely separate window to make that choice. Further, once there, the consumer's preferences are automatically defaulted to "opt in" to "Performance, Functionality, Targeting, and Social Media Technologies" – the less-privacy protection option.

Similarly, another target company utilizes a cookie banner that states: "By continuing to browse our site you accept our cookie policy" and then provides the consumer with only one option – to "opt in" to the use of cookies by clicking on a button that reads, "ACCEPT ALL COOKIES." Although the company includes a link to "click here for more information," that link simply brings the consumer to the general privacy policy and offers no opportunity to "opt out" of cookies.

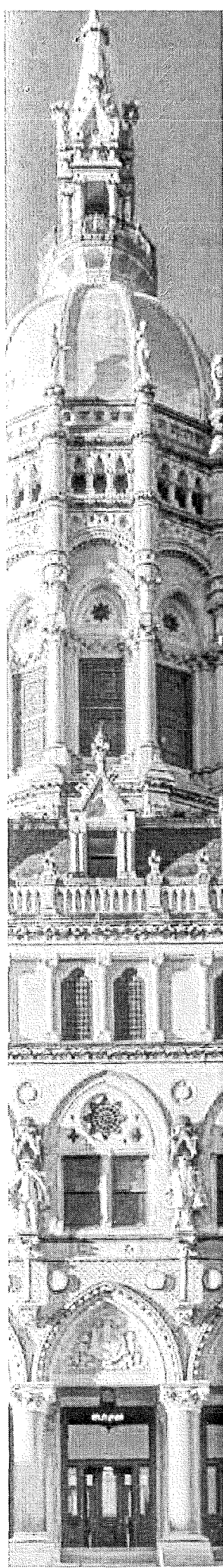
To comply with the CTDPA, companies that utilize cookie banners that provide consumers with the option to accept all cookies, should also offer a symmetrical option to reject all cookies. Both options should be displayed on the screen at the same time, and in the same color, font, and size. Whenever possible, the banner should either display each time the consumer accesses the site and/or the mechanism to update/change cookie preferences should be prominently displayed on the site such that the consumer has the means to update/change those preferences at any time.²⁰

SB3 (2023) Enforcement Efforts

The CTDPA was amended before it even took effect through 2023's Senate Bill 3 ("SB3") which contains provisions focused on minors' data and consumer health data. These new provisions have been a focus of some of our recent enforcement efforts and are discussed below.

[19] See also Conn. Gen Stat. § 42-520(a)(6) ("A controller shall provide an effective mechanism for a consumer to revoke the consumer's consent under this section that is at least as easy as the mechanism by which the consumer provided the consumer's consent . . ."); California Privacy Protection Agency ("CPPA") Consent Order in In the Matter of Honda American Motor Co., Inc., at 9-11 (March 7, 2025) (finding Honda cookie management tool failed to provide symmetrical choice because "[w]hile Consumers can 'Accept All' cookies with one click, opting out of the cookies requires at least two clicks."); CPPA Enforcement Advisory No. 2024-02, Avoiding Dark Patterns: Clear and Understandable Language, Symmetry in Choice; Avoiding Dark Patterns, Clear and Understandable Language, Symmetry in Choice, September 4, 2024; FTC Staff Report, Bringing Dark Patterns to Light, September 2022.

[20] We have included this informal guidance to provide baseline expectations for businesses that choose to utilize cookie banners, but it is not intended to be exhaustive. This informal guidance does not confer any rights on any person and does not operate to bind the OAG or the public. This guidance further does not preempt federal, state, or local laws, or impact the OAG's enforcement authority under the CTDPA or other applicable statutes. Further, while this in-formal guidance focuses on the application of the CTDPA to the use of cookie banners, businesses utilizing such banners must ensure that they also comply with other applicable privacy and consumer protection laws, including CUTPA.



As of October 1, 2024, SB3 imposes new obligations on companies that offer any “online service, product or feature” to “minors” who are defined under the law to include consumers who are younger than eighteen years of age.²¹ Generally, these provisions require that covered entities use reasonable care to avoid causing a heightened risk of harm to minors. Further, these provisions prohibit: (1) the processing of a minor’s personal data without consent for purposes of targeted advertising, profiling, or sale; (2) using a system design feature to significantly increase, sustain, or extend a minor’s time online; and (3) collecting a minor’s precise geolocation data without consent. The provisions further require that covered entities put specific safeguards in place for direct messaging apparatuses and provide a signal to minors while collecting their precise geolocation data. Lastly, covered entities must conduct DPAs that include an assessment of whether the service, product, or feature causes a heightened risk of harm to minors.

We recently sent inquiry letters to three popular companies that are known to offer online services, products, or features to minors in which we seek additional information to better understand the steps that the companies have taken to comply with these new provisions. Our Office also sent an inquiry letter to a technology company that has been the subject of recent reporting regarding alleged harm to minors and the use of addictive design features, to determine, amongst other things, whether a violation of the minors’ data protection provisions, has occurred. In general, companies that offer online services, products, or features to minors should ensure that they have measures in place to comply with the CTDPA’s new provisions.

Consumer Health Data

SB3 also amended the CTDPA to add “consumer health data” to the definition of “sensitive data” requiring that a controller obtain a consumer’s opt-in consent before processing such data.²² Further, the amendments require, among other things, that companies (1) not sell, or offer to sell, consumer health data without first obtaining the consumer’s consent²³ and (2) not provide any processor with access to consumer health data without proper contracts in place, including requiring that the processor keep the data confidential.²⁴ Notably, these provisions apply to all consumer health data controllers who do business in Connecticut, regardless of their size or the nature of their data processing activities.²⁵

We sent inquiry letters to two telehealth companies raising concerns that they were transmitting sensitive health information to third-party platforms, such as Meta and Google, through their use of tracking technologies marketed by those platforms. We subsequently sent a cure notice to one of them, noting that the company’s mechanism for obtaining consent to process “consumer health data” was insufficient under the CTDPA. As a result of the cure notice, the company implemented an updated user consent process, added consumer disclosures specific to Connecticut law, and conducted a data protection assessment for “consumer health data” as defined by the CTDPA. Covered companies processing consumer health data must comply with the CTDPA’s protections.

Universal Opt-Out Preference Signals

As of January 1, 2025, businesses are now required to recognize universal opt-out preference signals (“OOPS”) indicating a consumer’s intent to opt out of targeted advertising and sales of personal data. The OOPS provisions provide a simpler, privacy-protective online experience for consumers. To send their “signal,” a consumer need only configure a setting on their internet browser or browser extension one time, which then automatically sends their choice to opt out to all websites they visit online. To date, the Global Privacy Control²⁶ (“GPC”) is the most widely adopted OOPS mechanism for consumers to send their signal. It has been previously supported by our sister agencies whose comprehensive privacy laws already require compliance with similar OOPS provisions, and we join in that support. The GPC can be effectuated through an increasing number of platforms and mechanisms, including internet browser extensions and privacy-protective browsers.

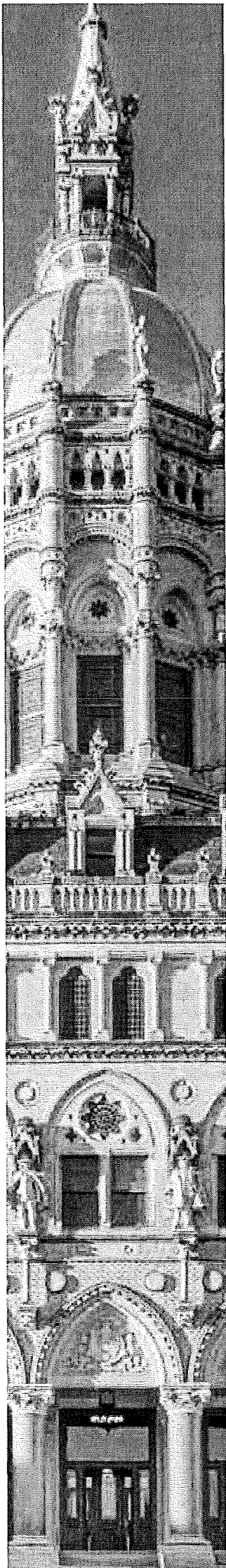
[21] Conn. Gen. Stat. §§ 42-529, et seq.

[22] Conn. Gen. Stat. §§ 42-515(9)(38), 42-520(a)(4).

[23] Conn. Gen. Stat. § 42-526(a)(1)(D).

[24] Conn. Gen. Stat. § 42-526(a)(1)(B), 42-521.

[25] Conn. Gen. Stat. § 42-526(a)(2) (citing Conn. Gen. Stat. § 42-516).



Throughout Connecticut's legislative process, our Office maintained that the OOPS provisions were critical to offset the heavy burden placed on consumers wishing to exercise their rights under the law. Going forward, we will be focused on examining whether businesses are complying with the OOPS provisions and expect to engage in efforts to ensure this key consumer right is upheld.

CTDPA Legislative Recommendations

As noted in our Initial Report, through our enforcement efforts, as well as our collaboration with other states who have passed consumer privacy laws, we continue to identify areas where legislative changes would strengthen or clarify privacy protections under the CTDPA. We have expanded on and added to our recommendations for future revisions to the law in detail below. The CTDPA has become a model for states considering and passing comprehensive consumer data privacy laws, so it is imperative that the CTDPA be updated to provide a strong foundation for future legislation.

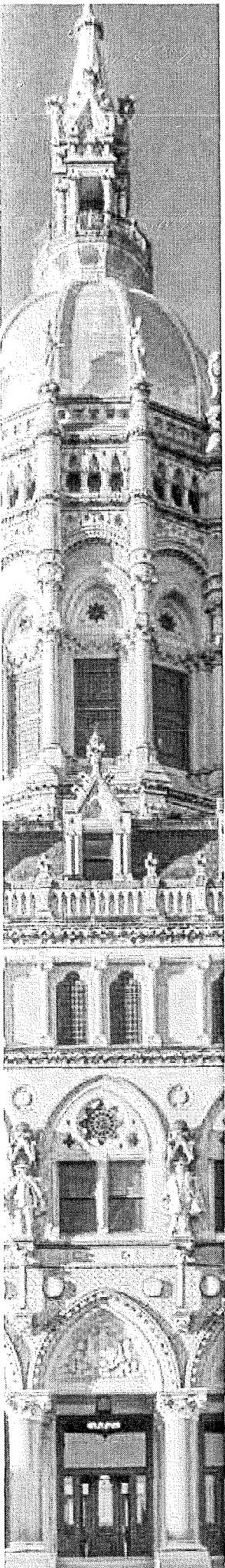
Scale Back Exemptions

We strongly urge the legislature to scale back exemptions in the CTDPA. First, the legislature should omit entity-level exemptions for GLBA (Gramm-Leach-Bliley-Act)- and HIPAA-covered entities. Various states have now passed laws without these exemptions— the CTDPA's wholesale carveouts not only put Connecticut residents at a disadvantage, but further impact the OAG's ability to uphold the CTDPA's protections and join forces with our sister states in their efforts to enforce consumer data privacy laws against large national entities. Moreover, with respect to the GLBA in particular, entities have raised the CTDPA exemption in contexts that we believe are far outside of the legislative intent. Further, we have seen telehealth companies use this HIPAA exemption to avoid having to comply with the CTDPA despite the fact that much of the data they process is not protected health information.

Second, we believe the legislature should narrow the FCRA (Fair Credit Reporting Act) data-level exemption. While the legislature's clear intent was to create a limited FCRA exemption, the current language is overly broad, and businesses have cited to this exemption in a manner resembling an entity-level carveout. The CFPB (Consumer Financial Protection Bureau) recently issued a report calling out these shortcomings in state consumer data privacy laws. The CFPB aptly noted that "while states have significant latitude to provide additional data privacy protections, many states exempt the data and financial institutions subject to GLBA or the FCRA. ... This means that such data often is not covered by the new state-law protections, such as the right under state law for consumers to fix or delete incorrect or outdated information, or the requirement that people opt in—instead of having to opt out—of the collection of especially sensitive data."²⁷

Third, we believe the legislature should also remove the entity-level exemption for nonprofit organizations. Other states, including California, Colorado, New Jersey, and Maryland, cover non-profits in recognition of the fact that many non-profits collect an extensive amount of sensitive data. Further, privacy laws in Delaware and Oregon exempt only nonprofits with specific missions. Connecticut should join in regulating nonprofit entities that process Connecticut residents' data.

[27] CFPB Report Details Carveouts for Financial Institutions in State Data Privacy Laws (November 12, 2024).



Lower Thresholds

The legislature should lower considerably the CTDPA's thresholds for applicability. While Connecticut is a small state, the CTDPA contains thresholds mirroring those in consumer data privacy laws passed by much larger states. The CTDPA's threshold should be updated to match Delaware and New Hampshire's language, to cover businesses that, during the preceding calendar year: (i) controlled or processed the personal data of not less than thirty-five thousand consumers; or (ii) controlled or processed the personal data of not less than ten thousand consumers and derived more than twenty per cent of their gross revenue from the sale of personal data. Importantly, we believe the legislature should fully remove applicability thresholds for the processing of sensitive data and minors' data as it did in 2023 for "consumer health data" in SB3. All sensitive data and minors' data processing should be covered by the CTDPA and fall within the ambit of regulation.

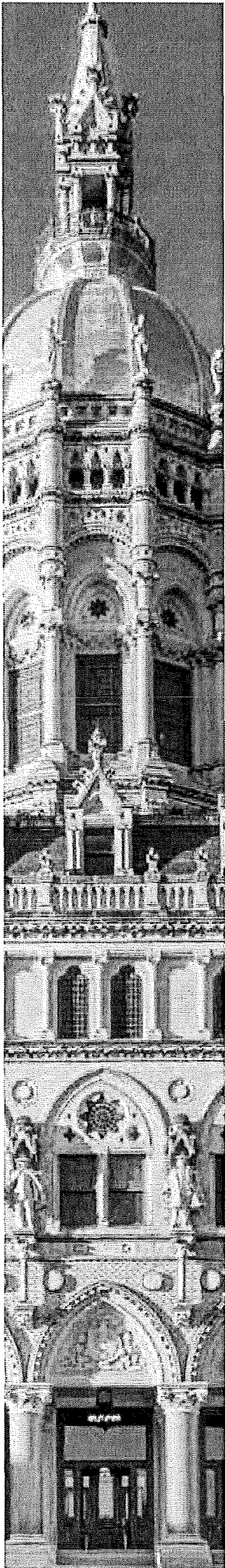
Strengthen Data Minimization Provisions

The legislature should enhance the CTDPA's data minimization standard. We cannot underscore enough the importance of these provisions— in many cases, serious privacy and data security concerns could have been offset— if not fully alleviated— if companies had properly minimized the data they collected and maintained. Unfortunately, the CTDPA's current notice-and-consent model sets an exploitable standard— businesses can seek to justify unnecessary data collection by deeming such collection "adequate, relevant and reasonably necessary" to the purposes disclosed to consumers. This standard contravenes data minimization principles outright— it allows businesses to collect data they simply do not need so long as it is disclosed in privacy notices that are often bulky, confusing, or worse, misleading. We believe the legislature should amend the CTDPA to mirror Maryland's law, which limits collection to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer. Further, the legislature should limit the collection and processing of sensitive data to only when strictly necessary to provide or maintain a specific product or service requested by the consumer.

Expand Sensitive Data Definition

The legislature should expand Connecticut's definition of "sensitive data" to incorporate a comprehensive list of elements added by other states since the CTDPA's passage, including data categories like Social Security numbers, government-issued identifiers, union membership, status as transgender or non-binary, income level or indebtedness, and neural data. The CTDPA's heightened protections for sensitive data are a cornerstone of the law, and Connecticut residents deserve to be on the same footing as residents of other states.

Hand in hand with these updates, we again recommend that the legislature amend the CTDPA's definition for biometric data, a sensitive data element under the law. As a growing number of states have recognized, biometric data is sensitive if it can be used to identify an individual, even in circumstances where it is not affirmatively used to do so. The collection, sale, and use of biometric data raises serious privacy concerns for consumers that should trigger elevated protections.



Additionally, to reflect the realities of the online marketplace more accurately, we recommend removing the “known child” sensitive data element and replacing it with the “knows or has reason to know” standard enacted in Maryland. We have observed the ease with which companies disavow processing minors’ data in their privacy notices, despite widely distributed press and reports describing consumer practices that contradict such statements.

Clarify and Strengthen Protections for Minors’ Data

In our Initial Report, we asked the legislature to clarify whether it intended to ban targeted advertising to minors wholesale, or whether it intended that the opt-in consent qualifier applied to both sale and targeted advertising.²⁸ Through our work under the CTDPA as well as our broader privacy work, it has become more and more clear that targeted advertising to children and teens, and the sale of their personal data, should be banned. Further, we believe the “actual knowledge or willful disregard” standard throughout the CTDPA is a weakness of the law. Connecticut’s protections should match those in Maryland, which prohibits businesses from sending targeted ads so long as the company “knew or should have known” that the individual is a minor. This “knew or should have known” standard is more fitting and mirrors the framework in CUTPA.

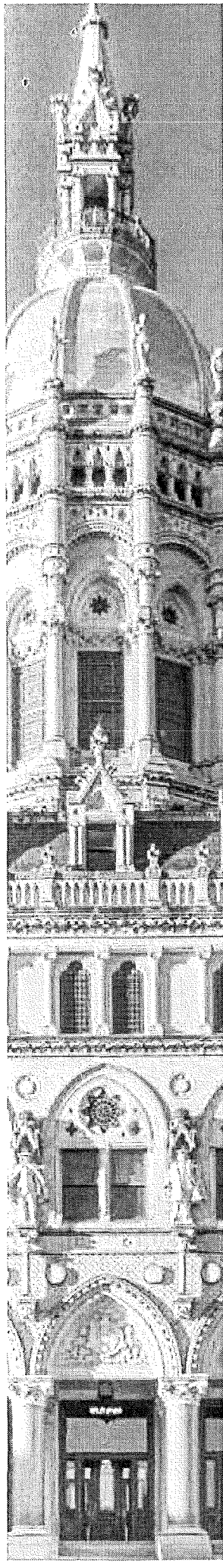
Further, we believe the legislature should update or remove other language in the CTDPA that jeopardizes privacy protections for minors. The rebuttable presumption framework creates an unnecessary hurdle for enforcement and is not appropriate in the context of minors’ privacy, especially given that children and teens are uniquely vulnerable to privacy harms. Even beyond this issue, we believe the current consent structure in the CTDPA is inadequate for privacy protections related to minors. Should minors be able to “consent” to a system designed to “significantly increase, sustain or extend” minors’ use of such online service, product or feature?²⁹ The fact that minors are not legally able to enter into contracts underscores why the consent structure should be removed.

Narrow “Publicly Available Information” Definition

As highlighted above, our Office continues to receive consumer complaints that unfortunately fall under the CTDPA’s too-broad exemption for “publicly available information.” In particular, these complaints involve websites that post individual profiles, combining public records like contact information and addresses, property records, court documents, and public social media posts, among others. While many individuals are understandably wary of this data being readily available to anyone online— all in one place— these companies allege that the profiles are pulled from publicly available information and, therefore, are not covered by the CTDPA. Further, data brokers routinely compile vast amounts of “public” consumer data to create inferences that are then sold to third parties. Consumers have little to no insight into how these profiles are used, but it has become increasingly clear that these practices can cause significant privacy harms.

We encourage the legislature to carve out from the definition of publicly available information: (i) information that is collated and combined to create consumer profiles on publicly available or subscription-based websites; (ii) information that is made available for sale; (iii) inferences generated from such information; and (iv) personal data that is created by combining personal data with publicly available information.

[28] The CTDPA states that businesses shall “not process the personal data of a consumer for purposes of targeted advertising, or sell the consumer’s personal data without the consumer’s consent, under circumstances where the business has actual knowledge, or willfully disregards, that the consumer is at least thirteen years of age but younger than sixteen years of age.” Conn. Gen. Stat. § 42-520(a)(7).



Add Right to Know Specific Third Parties

We urge the legislature to follow Oregon's lead by incorporating into the CTDPA a "right-to-know" the specific third parties that receive personal data from covered businesses. In addition, like Delaware, the legislature should update the CTDPA to provide Connecticut residents the ability to obtain a list of the categories of third parties to which the controller has disclosed that particular consumer's personal data. Through our investigations, we have learned that some controllers do not understand the breadth of third-party data sharing that happens through their online services and these heightened disclosure requirements would require more responsible data practices. Further, Connecticut residents must have insight into the third parties that gain access to their data so that they can track their data downstream and effectively exercise their rights under the CTDPA.

Expand the Utility of the OOPS Provisions and Enact a One-Stop-Shop Deletion Mechanism

Since January 1, 2025, Connecticut residents have had the right to opt out of targeted advertising and the sale of their personal data by sending their "opt out preference signal" to covered businesses. However, in practice, this right may only be exercised through certain privacy-protective browsers and browser extensions- none of which come preinstalled on consumer devices. This universal opt-out requirement should be readily available to all interested consumers. We recommend amending the CTDPA's OOPS provisions to require all browser vendors and mobile operating systems include a setting which allows users to affirmatively send opt out preference signals. Since 2024, the California Privacy Protection Agency has supported such an effort and we join in this important initiative.

Similar to the universal opt-out requirement, a mechanism that allows Connecticut residents to exercise deletion rights at scale is sorely needed. The legislature should consider enacting a "one-stop-shop" deletion mechanism such as that contained in California's Delete Act, in order to allow Connecticut residents to delete their personal information held by data brokers through a single, verified request.

Conclusion

Connecticut remains at the forefront of consumer data privacy. Since passage of the CTDPA, the Privacy Section has worked to educate companies and consumers alike as well as learn about the practical applications of the law as written. We are focused on ensuring compliance with the CTDPA, including in key areas like transparency, opt-out rights, and sensitive data processing. We have also expanded our enforcement efforts as new legislation related to minors' privacy and consumer health data took effect, and as our universal opt-out provisions came online. It is clear that there is much to be done, including amending the CTDPA to provide stronger protections for Connecticut residents. We will continue to be transparent about our efforts to uphold this important law.



May 5, 2025

Senator Anne Carney
3 State House Station
Augusta, Maine 04333
Anne.Carney@legislature.maine.gov

Representative Amy D. Kuhn
2 State House Station
Augusta, ME 04330
Amy.Kuhn@legislature.maine.gov

Representative Jennifer L. Poirier
2 State House Station
Augusta, ME 04330
Jennifer.Poirier@legislature.maine.gov

Re: Maine Consumer Data Privacy Act: H.P. 710, L.D. 1088, "An Act to Enact the Maine Consumer Data Privacy Act"; H.P. 799, L.D. 1224, "An Act to Comprehensively Protect Consumer Privacy"; H.P. 1220, L.D. 1822, "An Act to Enact the Maine Consumer Data Privacy Act."

Dear Chairpersons Carney and Kuhn, Ranking Member Poirier, and the other distinguished members of the Judiciary Committee:

National Futures Association (NFA) appreciates the opportunity to provide written testimony on the Maine Legislature's proposed data privacy bills, Bill H.P. 710, "An Act to Enact the Maine Consumer Data Privacy Act"; Bill H.P. 799, "An Act to Comprehensively Protect Consumer Privacy"; and Bill H.P. 1220, "An Act to Enact the Maine Consumer Data Privacy Act."

NFA generally supports increased privacy protections, but for the reasons discussed below, seeks a narrowly tailored exemption to enable it to continue performing its critical role in regulating derivatives markets and protecting investors.

NFA is a not-for-profit, registered futures association (RFA) under the Commodity Exchange Act.¹ NFA is the industrywide self-regulatory organization (SRO) for the derivatives industry, including futures, swaps, and retail off-exchange foreign currency (or forex). Every aspect of NFA's regulatory authority is overseen and monitored by the Commodity Futures Trading Commission (CFTC), the Congressionally authorized commodity derivatives regulator. NFA's responsibilities include registering firms and industry professionals on behalf of the CFTC,² passing rules to ensure fair dealing with customers, examining and investigating Members for compliance with those rules,

¹ See 7 U.S.C. § 21; 17 C.F.R. §§ 170.1 et seq.

² 17 CFR § 3.2(a) (stating that the registration functions of the CFTC shall be performed by NFA).

taking enforcement actions against those Members that violate NFA Rules, administering proficiency examinations for individuals engaged in derivatives activities, and providing a low-cost arbitration forum for members of the investing public to resolve their disputes with NFA Members.

In order for NFA to successfully carry out these regulatory functions, NFA must collect and process data. Importantly, NFA only uses the data it collects for regulatory purposes—data is not collected, shared, or sold for any commercial purpose.

NFA is concerned that the proposed legislation may interfere with NFA's efforts to safeguard financial markets and protect investors in Maine and throughout the nation. For example, the data NFA collects often includes financial account numbers, which H.P. 710 and H.P. 1220 would include in the definition of "sensitive data." However, because NFA regulates thousands of financial firms with millions of financial accounts, NFA cannot possibly obtain separate individual consents from accountholders before commencing a regulatory exam or investigation. Additionally, NFA must maintain the integrity of its investigative files and exam papers. Thus, NFA cannot typically disclose, modify or delete data upon the request of consumers.

Notably, the proposed bills already include exemptions for a closely analogous self-regulatory organization. All three proposed comprehensive data privacy bills under consideration by the Judiciary Committee today would provide a full exemption to the Financial Industry Regulatory Association (FINRA), which is a national securities association and the nationwide SRO for the securities markets. FINRA performs largely identical functions to NFA and is subject to similar federal supervision. While FINRA is the SRO for the nation's securities brokerage industry and operates under the comprehensive oversight of the SEC, NFA is the SRO for the nation's derivatives industry and operates under the comprehensive oversight of the CFTC.

Recognizing NFA and FINRA's analogous roles in safeguarding the financial markets, other states' comprehensive data privacy laws, such as the Delaware Personal Data Privacy Act and the Maryland Online Data Privacy Act of 2024, include entity-level exemptions both for registered futures associations and national securities associations, and do so in the same section.³

For these reasons, we respectfully request that the underlined language below be added to § 9603(3)(B) of the proposed Maine Consumer Data Privacy Act under H.P. 710 and 799, or to § 9604(1)(D) under H.P. 1220. Such language would not risk sweeping too broadly (as NFA is the nation's only RFA), would be consistent with other state comprehensive data privacy laws, and would ensure that NFA could continue to fulfill its role and responsibilities, which include protecting Maine investors.

³ See Del. Code Ann. tit. 6, § 12D-103(b)(4); Md. Code Ann., Com. Law § 14-4703(a)(2).

". . . Exempt entities . . .

A national securities association that is registered under the federal Securities Exchange Act of 1934, 15 United States Code, Section 78a et seq., or a registered futures association so designated pursuant to Section 17 of the Commodity Exchange Act, 17 United States Code, Section 21 et seq., as amended, or any regulations adopted thereunder;"

If you have any questions or there is any further information we may be able to provide, please reach out to Michael Schorsch at mschorsch@nfa.futures.org.

Very truly yours,

A handwritten signature in black ink, appearing to read 'Lucy C. Hynes', written in a cursive style.

Lucy C. Hynes
Managing Director
Government & Regulatory Affairs
National Futures Association



Taking healthcare personally.

April 30, 2025

The Honorable Senator Anne Carney
Co-Chair, Joint Standing Committee on Judiciary
Maine State House
2 State House Station
Augusta, Maine 04333-0002

The Honorable Representative Amy Kuhn
Co-Chair, Joint Standing Committee on Judiciary
Maine State House
2 State House Station
Augusta, Maine 04333-0002

Re: L.D. 1822 - An Act to Enact the Maine Online Data Privacy Act

Dear Chairs Carney and Kuhn,

On behalf of the Consumer Healthcare Products Association (CHPA), the Washington, D.C. based national trade organization representing the leading manufacturers of over-the-counter (OTC) medicines, dietary supplements, and OTC medical devices, thank you for the opportunity to comment on LD 1822. While we support the bill's goal of strengthening consumer control over personal data, we must oppose it in its current form. Specifically, the bill conflicts with federal regulations governing controlled substances data collection. Adding language to ensure compliance with these federal requirements would resolve our concerns.

Federal and State Law

The Controlled Substances Act (CSA), also referred to as the Comprehensive Drug Abuse Prevention and Control Act, was enacted by Congress in 1970 with the aim of regulating the production, distribution, and utilization of controlled substances. As per 21 U.S.C. Section 830 of this Act, individuals or entities involved in transactions concerning listed chemicals (such as pharmacies selling allergy medications containing ephedrine or pseudoephedrine) are obligated to gather and retain identifiable personal records pertaining to these transactions and to share the data with law enforcement as required. Building upon this federal framework, Maine enacted its own legislation in 2013 implementing the National Precursor Log Exchange (NPLEX) system, which provides real-time electronic monitoring of pseudoephedrine (PSE) sales across the state. Unfortunately, this bill does not provide an exemption for such transactions from its privacy provisions for either law.

Amendment Recommendations

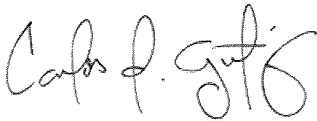
To avoid potential conflict with already existing federal law, CHPA recommends the following amendment to LD 1822 on page 8, line 40 as item (Q):

(Q) Personal data collected and used for purposes of the federal policy under the Controlled Substances Act Section on the Regulation of Listed Chemicals under 21 U.S.C. SEC. 830.

Conclusion

CHPA and its members are deeply committed to protecting our customers' privacy and data security. While we appreciate your focus on this important issue, the current version of this bill raises significant concerns. We remain open to constructive dialogue and collaboration to develop a more balanced approach that addresses all stakeholders' needs.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Carlos I. Gutierrez". The signature is fluid and cursive, with the first name "Carlos" and last name "Gutierrez" clearly distinguishable.

Carlos I. Gutiérrez
Vice President, State & Local Government Affairs
Consumer Healthcare Products Association
Washington, D.C.
cgutierrez@chpa.org | 202-429-3521

Cc: Member of the Joint Standing Committee on Judiciary



STATE OF VERMONT
HOUSE OF REPRESENTATIVES

May 21, 2025

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

RE: LD 1822, An Act to Enact the Maine Online Data Privacy Act

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

I write to express my strongest support for LD 1822, the Maine Online Data Privacy Act. As the lead sponsor of H.208 in Vermont — the Data Privacy & Online Surveillance Act — and the primary architect of Vermont's broader digital rights framework, I commend Maine's leadership in advancing legislation that protects constituents, respects autonomy, and challenges unchecked corporate power.

Alongside Maine Representative Amy Kuhn and Massachusetts Representative Tricia Farley-Bouvier, I serve on the National Conference of State Legislatures' Task Force on Artificial Intelligence, Cybersecurity, and Privacy. Through that work and beyond, we've built a regional alliance grounded in public service, transparency, and shared values. We are committed to building a true **New England Model Bill** — one that puts people before profits, delivers meaningful protections, and sets a national standard that others can follow.

This regional collaboration is more than symbolic. It's necessary. Our states are facing unprecedented pressure from some of the most powerful corporate lobbying forces in the world. In Vermont, we've witnessed millions of dollars in lobbying efforts aimed at gutting our privacy legislation — including the introduction of what's being branded as the "New England Model Bill." Let's be clear: this bill is not the product of a regional consensus. It is a coordinated Big Tech strategy, originally drafted by a Big Tech employee, carried through statehouses by Big Tech lobbyists, and designed to preempt strong state laws with weak language riddled with loopholes.

Their goal is simple: **to lock in a status quo that serves industry interests while giving people the illusion of privacy.** They want to use New England's reputation for pragmatism and leadership to rubber-stamp a model that removes long-standing consumer rights and prevents meaningful enforcement. We refuse to let that happen.

What Rep. Kuhn has introduced in Maine — like what we've proposed in Vermont and Massachusetts — is a different vision. One grounded in data minimization, transparency, and dignity. One that listens to our constituents, small businesses, civil rights advocates, and national experts. One that responds to the realities of today's digital harms — discrimination, manipulation, data breaches, surveillance — with the seriousness they deserve.

The people of Maine deserve control over their personal data, safeguards against predatory practices, and laws that evolve with technology rather than fall behind it. The Maine Online Data Privacy Act offers precisely that.

To my fellow legislators in Maine: I urge you to hold the line. You are not alone. Massachusetts and Vermont stand proudly beside you — and with you, we are shaping a New England model that reflects **our values, not Big Tech's**.

Thank you for your leadership and for your commitment to protecting the people of Maine. If I can be of any support to your work, please do not hesitate to reach out.

With deep respect,

Monique é. Priestley

Monique Priestley

Vermont State Representative, Orange-2 District

Clerk, House Commerce & Economic Development Committee

Joint Information Technology Oversight Committee

Co-Chair, Rural Caucus

NCSL Task Force on Artificial Intelligence, Cybersecurity & Privacy

NCSL Committee on Technology & Communications

NCSL Committee on Labor & Economic Development



The Commonwealth of Massachusetts
House of Representatives
State House, Boston 02133-1054

TRICIA FARLEY-BOUVIER
STATE REPRESENTATIVE
3RD BERKSHIRE DISTRICT

STATE HOUSE, ROOM 156
TEL: (617) 722-2240

May 21st, 2025

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

RE: LD 1822, An Act to Enact the Maine Online Data Privacy Act

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

I write today to register my wholehearted support for LD 1822, And Act to Enact the Maine Online Data Privacy Act, which would provide crucial protections to the people of Maine in order to stay safe in our digitized world.

As the House Chair of the Advanced Information Technology, the Internet and Cybersecurity Committee in Massachusetts, I have been happy to work with Chair Kuhn to further refine actionable privacy language to enhance interoperability across New England while preserving strong consumer protections. Working with fellow lawmakers across state lines has been crucial to developing harmonized data privacy frameworks that respect our constituents' rights while creating standards for businesses. By aligning key definitions and various compliance mechanisms through our multi-state coalition, we're reducing the regulatory patchwork that drives up costs and creates confusion for companies operating nationwide and mitigating the risks for unintended consequences.

In today's digital landscape, our personal information is continuously collected, processed, and sold with limited transparency or consumer protections, which has left states like Maine and Massachusetts to consider how best to protect the residents of their states. It is becoming more and more evident that the status quo model of notice and choice has failed to adequately protect the public's privacy. Companies rely on the fact that consumers do not have the time or expertise required to fully absorb and understand dense, complicated privacy policies. Rather than place all of the onus on the consumer, we need new privacy models that fairly balance the needs of industry against the privacy risks to ordinary people. Data protection laws like LD 1822 strike



TRICIA FARLEY-BOUVIER
STATE REPRESENTATIVE
3RD BERKSHIRE DISTRICT

The Commonwealth of Massachusetts
House of Representatives
State House, Boston 02133-1054

STATE HOUSE, ROOM 156
TEL: (617) 722-2240

that balance by establishing baseline standards for the collection of personal data and reserving the strongest protections for our most sensitive kinds of personal data.

The bill grants Maine residents critical rights over their personal data found in other state privacy laws, including the right to access, correct, delete, and transfer their information. The bill also requires meaningful data minimization. Data minimization is the practice of limiting the collection of personal data to what is reasonably necessary for the purposes the data was collected for, and it includes deleting or removing information when it is no longer needed. These provisions are essential to mitigate the risks associated with data breaches and the misuse of personal information.

This legislation arrives at a critical moment when many Mainers are increasingly concerned about their digital privacy but lack the tools to meaningfully protect their data. By passing this bill, Maine would join the growing number of states taking proactive measures to establish consumer privacy rights while setting reasonable standards for businesses.

I urge the committee to support this important legislation. The Maine Online Data Privacy Act represents a thoughtful, balanced approach to addressing one of the most significant consumer protection challenges of our time.

I hope that the Committee will advance LD 1822 with a favorable recommendation.

Thank you to the Committee for your thorough and thoughtful consideration of the legislation before you. If there are any additional questions, please do not hesitate to reach me via email at tricia.farley-bouvier@mahouse.gov.

Sincerely,

A handwritten signature in cursive script, reading "Tricia Farley-Bouvier".

Tricia Farley-Bouvier, Massachusetts State Representative
2nd Berkshire District

[BECOME A MEMBER](#) | [DONATE](#)[Media Room](#)

Consumer Reports investigation uncovers Kroger's widespread data collection of loyalty program members to create secret shopper profiles

Investigation reveals that profiles can be inaccurate and may result in customers not getting Kroger's best discounts

May 21, 2025 | Financial Fairness



Washington, DC - A new Consumer Reports (CR) investigation uncovered that Kroger grocery stores collect extensive customer data and use it to make detailed inferences, such as by using an “income predictor,” an estimate about a customer’s income level. Personal data is also used to determine whether the shopper is deemed a truly loyal Kroger shopper and predicted to purchase premium brands.

However, CR discovered that Kroger’s “income predictor” can be inaccurate, and differ markedly from reality. As a result, a shopper deemed to have less education or with a lower income, for example, could end up getting fewer of Kroger’s best discounts.

Justin Brookman, director of technology policy at CR said, “Regardless of whether these consumer profiles are accurate or not, we need to rein in the rampant overcollection and misuse of consumer data and ensure that companies like Kroger are held accountable when they violate the trust of consumers and harm their pocketbooks.”

One such customer profile, which CR obtained after a customer filed a formal request with Kroger through Oregon's new data and privacy law, found that his report may have been sent to more than 50 different U.S. companies. These companies included one of the country's largest data brokers; tobacco companies; financial institutions; and a host of analytics and marketing firms that could result in unwanted solicitations and spam. The report also included other companies such as Soda Health, a healthcare tech company that works with health insurers, and Solutran, a fintech payments platform that helps process Electronic Benefit Transfer, an electronic system that allows a Supplemental Nutrition Assistance Program participant to pay for food using SNAP benefits.

Kroger, one of the nation's largest grocery chains, which includes stores like Ralphs and Harris Teeter, is also one of the most advanced when it comes to tracking shoppers' purchases and behavior through analytics on its roughly 63 million customers. For years, Kroger has made a concerted effort to drive people to its loyalty program and more than 95 percent of customer transactions are tied to a Kroger loyalty card. Kroger leverages customer data into a lucrative business; Kroger's "precision marketing" division sells customer data to other companies for marketing and advertising purposes. Kroger's "alternative profit" business, which includes the precision marketing division, now represents more than 35% of the company's net income.

Brookman continued, "Thanks to some state privacy laws, we can now gain more insight into the data practices of companies. It's especially alarming to see Kroger distributing customers' personal information so broadly. We urge lawmakers at both the state and federal levels to enact strong privacy protections and to prohibit the practice of surveillance pricing."

Earlier this month, a separate CR investigation uncovered that shoppers at Kroger have been unknowingly paying full price for some items that have

been advertised as discounted or on sale.

CR's investigations into Kroger are part of its Make the Price Right campaign, which seeks to examine potential predatory pricing practices that are fueled by data collection and algorithms. CR launched a petition today calling on Kroger to give everyone in the loyalty program the same discount offers regardless of their level of income or education.

John Marshall, Capital Strategies Director at UFCW 3000, a union representing retail workers across Washington state, north-east Oregon, and northern Idaho, said "It's concerning when huge corporations like Kroger use erroneous data that results in consumers being charged more for groceries, but the bigger concern is the possibility that Kroger could use accurate data to target discounts at higher income shoppers while leaving lower income consumers to pay full price. The real problem isn't when the business model makes a mistake, it's when it works according to plan."

Lindsay Owens, Executive Director of Groundwork Collaborative, an economic policy think tank, added, "No longer content to merely overcharge you on groceries, Kroger is now selling your data too. Consumers should be able to go to the grocery store and put together a meal for their families without finding themselves on the menu."

MEDIA CONTACTS

Cyrus Rassool

+1 (914) 378-2786

cyrus.rassool@consumer.org

LATEST NEWS RELEASES

Pinette, Susan

LD 1822

From: Christy van Voorhees <cvanvoorhees@llbean.com>
Sent: Wednesday, May 14, 2025 4:22 PM
To: Cmte JUD
Subject: L.L.Bean's response regarding marketing

This message originates from outside the Maine Legislature.

Hi Janet and Susan,

Here is the answer to the question posed to L.L.Bean:

Consumers are twenty times more likely to make a purchase when exposed to targeted, personalized ads compared to generic ones.

L.L. Bean

Christy Van Voorhees

- Does L.L. Bean use both targeted ads?
How effective are these relative to ea

Thank you,
Christy

Christiana van Voorhees | Legal Counsel - Regulatory

L. L. Bean, Inc.

15 Casco Street, Freeport, ME 04033

**Bean
Outsider**



**Maine State Legislature
OFFICE OF POLICY AND LEGAL ANALYSIS**

www.mainelegislature.gov/opla
13 State House Station, Augusta, Maine 04333-0013
(207) 287-1670

BILL ANALYSIS

TO: Joint Standing Committee on Judiciary
FROM: Janet Stocco, Legislative Analyst
DATE: May 14, 2025
RE: LD 1088, An Act to Enact the Maine Consumer Data Privacy Act (Rep. Henderson)
LD 1224, An Act to Comprehensively Protect Consumer Privacy (Rep. Roberts)
LD 1822, An Act to Enact the Maine Online Data Privacy Act (Rep. Kuhn)

SUMMARY

These bills — LD 1088, LD 1224 and LD 1822 — propose comprehensive personal data privacy legislation for the State of Maine, each of which is designed to take effect on July 1, 2026. In brief, these proposals would:

- **Restrict the collection, processing, use, disclosure and sale** of Maine residents' **personal data** by persons (referred to as "controllers") who conduct business in Maine or target Maine residents and who collect the personal data of a minimum number, depending on the bill, of Maine residents in a calendar year.
 - Impose heightened protections on the collection, processing, use, disclosure and sale of Maine residents' **sensitive data**, which is a subset of personal data that includes genetic and biometric data; health data; personal data of minors (LD 1822) or children under age 13 (LD 1088, LD 1224); data revealing one's status as a victim of a crime; data revealing a Maine resident's racial, ethnic, religious, sexual, citizenship and immigration status; and other sensitive data specific to each of the legislative proposals.
 - These bills' protections include, depending on the bill, either prohibiting the use of personal data for certain purposes — for example, the use of personal data or sensitive data for targeted advertising or profiling of Maine residents or the sale of Maine residents' personal data — or requiring that a consumer either affirmatively consent to the controller's use of their data for that purpose or that the consumer be offered the option to opt-out of the controller's use of their data for that purpose.
- Establish that, at a minimum, **consumers have the right** (a) to confirm with each controller whether it processes personal data; (b) to access their personal data; (c) to correct inaccuracies in their personal data; (d) to require the controller to delete their personal data; and (e) to obtain a portable copy of their personal data.
- Require controllers to provide clear **privacy notices** disclosing, at a minimum, the categories of personal data the controller processes, the controller's purposes for processing that data, how consumers may exercise their rights, the categories of third parties with whom the controller shares personal data and the categories of personal data shared, as well as contact information for the controller.
- Require controllers to establish **data security** practices protecting the confidentiality and integrity of personal data and, in LD 1088 and LD 1822 but not LD 1224, to establish **data-retention schedules** for personal data.
- Require controllers to conduct **data protection assessments** if they process personal data in a manner that poses a heightened risk to Maine residents, including the processing of sensitive data and the processing of data for sale, targeted advertising and "profiling" of Maine residents.

- Require controllers that engage the services of other businesses to process personal data (referred to in these bills as “processors”) to formalize **contracts requiring processors** to protect data confidentiality, adhere to the controller’s instructions for data processing, destroy the data after conducting the requested processing activities and assist the controller in complying with the other requirements of the data privacy legislation.
- Two of the bills (LD 1088 and LD 1822) also prohibit the establishment of a **geofence** around a healthcare facility, other than by the facility itself, in order to track or send notices to individuals using the facility.
- **Exempt several types of entities and several types of data**, usually entities or data subject to other state or federal data privacy laws, from also complying with this new comprehensive data privacy legislation.
- Notwithstanding any other provision of the bills, **authorize controllers or processors to engage in certain activities**, including complying with federal or state laws (and local ordinances in LD 1822); complying with law enforcement investigations, court orders and subpoenas; taking immediate steps to protect an individual’s life or physical safety; preventing identity theft, fraud, deceptive or illegal activity, and security incidents; and performing certain activities for internal use, for example effectuating product recalls.
- Establish that the Attorney General has the **sole authority to enforce** violations of the comprehensive data privacy legislation under the Maine Unfair Trade Practices Act, with the bills varying on the amount and type of advance notice required before an enforcement action may be brought and whether the Attorney General has rulemaking authority regarding implementation of the comprehensive data privacy legislation.
 - Two of the bills (LD 1088 and LD 1224) would require that any monetary penalties recovered in actions brought by the Attorney General be set aside in a nonlapsing **Maine Privacy Fund** used to finance the Office of the Attorney General’s enforcement activities, including staff.
 - None of the bills would authorize a private action, or a private class action, to enforce their provisions.
- Require the Attorney General to **report to the Judiciary Committee** on the implementation of the new comprehensive data privacy law either 6 months or 18 months after it takes effect, depending on the bill, with committee authority to report out legislation in response to the report.

Additional detail about each of the proposals, including details on how the proposals differ from each other, is included in the attached side-by-side comparison chart. *See Attachment A*

ADDITIONAL INFORMATION

1. **Public records exception review.** Each of these bills includes a provision that makes the content of a data protection assessment that has been disclosed to the Office of the Attorney General confidential, *i.e.*, not subject to disclosure under the Freedom of Access Act. If a majority of the committee votes in favor of a version of any of these bills that includes this provision, the committee must conduct a review of that new proposed public records exception under 1 M.R.S. §434. *See Attachment B (FOAA evaluation rubric).*

AMENDMENTS PROPOSED IN TESTIMONY¹

1. “Small business” exemption

- a. Small businesses that collect data from $\leq 100,000$ Maine residents per calendar year should be exempt (*Retail Association of Maine; Maine Alliance of Boys & Girls Club; Maine Policy Institute*)
- b. Small data brokers that collect data from $\leq 25,000$ Maine residents per calendar year and derive $< 50\%$ of their annual revenue from selling personal data should be exempt (*Maine Policy Institute*)

¹ This bill analysis lists only specific, proposed amendments included in testimony on LD 1088, LD 1224 and LD 1822. Policy arguments for and against certain aspects of each bill, if not framed as proposed amendments, are not included.

2. Entity-level exemptions

- a. Exempt entities subject to GLBA, the federal Gramm-Leach Bliley Act (*American Council of Life Insurers; Maine Bankers Association; Maine Credit Union League; Receivables MGMT Assoc. Intl.*)
 - This exemption is in LD 1224; LD 1088 and LD 1822 have narrower financial institution exemptions
 - **By contrast** – *Consumer Reports* requests that entities subject to GLBA **not** be exempted
- b. Exempt all nonprofit organizations (*American Heart Association; Maine Policy Institute; the YMCA*)
 - This exemption is in LD 1822
- c. Exempt a nonprofit organization established to detect and prevent fraudulent insurance acts (*National Insurance Crime Bureau*)
 - This exemption is present in LD 1088; all nonprofits are exempt from LD 1822
- d. Exempt a registered futures association designated under Section 17 of the Commodity Exchange Act (*National Futures Association*)
 - This exemption is not in any of the bills; but, NFA is “not-for-profit” so may be exempt in LD 1822
- e. Exempt Maine automobile dealers (*Maine Automobile Dealers Association*)
- f. Exempt Maine’s postsecondary institutions (*Maine Community College & University of Maine Systems*)
- g. Exempt Maine hospitals and health care providers (*Maine Hospital Association, Maine Medical Association, Maine Osteopathic Association, Maine Health Care Association, Maine Ambulance Association and Spectrum Healthcare Partners*)
 - This exemption is in LD 1822, but not in LD 1088 or LD 1224
- h. Amend the exemption for Maine-licensed insurance companies to eliminate the Attorney General’s ability to require these companies to comply with the comprehensive data privacy law if the Attorney General believes the companies are not complying with state insurance law (*American Council of Life Insurers*)
- i. **Do not** exempt nonprofit entities & higher education institutions (*Attorney General; Internet Safety Labs*)
 - These entities are exempt in LD 1822 but not in LD 1088 (with 1 exception) and LD 1224
- j. **Do not** exempt health care facilities, practitioners or affiliates (*Attorney General; Consumer Reports*)

3. Data-level exemptions

- a. Exempt data collected under the Controlled Substances Act (*Consumer Healthcare Products Association*)
- b. Preserve the HIPAA “protected health information” exemption (*Healthcare Purchaser Alliance of Maine*)
 - This data-level exemption is present in all three bills
- c. **Do not** exempt data subject to FERPA, Family Education Rights and Privacy Act (*Internet Safety Labs*)

4. Enforcement mechanism

- a. Include a permanent right-to-cure period or a safe harbor for companies that demonstrate good-faith compliance with certain industry privacy standards—e.g., NIST or AICPA (*Maine Policy Institute*)
- b. Include a private right of action (*Attorney General; ACLU of Maine; Consumer Reports; Center for Democracy & Technology*).
 - The Attorney General suggests adding the following additional protections: (a) adding a right to cure provision to a private right of action, subject to a sunset; (b) exempting small businesses from the private right of action, subject to a sunset; (c) delaying the effective date of the private right of action.
 - Consumer Reports also supports proposal (b) from the Attorney General

5. Effective date

- a. Extend the effective date for nonprofits (*Maine Alliance of Boys & Girls Clubs*)
 - Nonprofits have an entity-level exemption under LD 1822 but not LD 1088 and LD 1224

6. Other proposed Amendments & Concerns – LD 1088 (Henderson)

- a. *Consumer Data Industry Association*
 - Replace the definition of “publicly available information” with the definition used in LD 1224—specifically do not exclude inferences derived from publicly available info. from this definition
- b. *ACLU of Maine; Attorney General; Electronic Frontier Foundation; Maine Broadband Coalition*
 - Do not repeal Maine’s existing ISP data-privacy law in Title 35-A

7. Other proposed Amendments & Concerns – LD 1822 (Kuhn)

- a. *Definition of “minor”*
 - Several organizations requested a definition of “minor” be included in LD 1822. However, pursuant to 1 M.R.S. §72(11-A), unless a particular statute adopts a different definition, ““minor or minors” means any person who has not attained the age of 18 years” throughout Maine’s statutes
- b. *ACLU of Maine, Center for Democracy and Technology, Consumer Reports*
 - §9608(2)(A): limits only the “collection” of non-sensitive personal data to what is “reasonably necessary and proportionate to provide or maintain a specific product or service.” Requests committee apply this same standard to the “processing” of non-sensitive personal data
- c. *Attorney General’s Office*
 - §9602(33): restrict the exception that exists in the definition of “sale of personal data” for the disclosure of data to an affiliate; this exception should instead be limited to the “disclosure of data for purposes of providing or maintaining a specific product or service requested by the consumer”
 - §9604(1): eliminate the following entity-level exemptions: (§B) nonprofit entities; (§C) institutions of higher education; and (§F) health care facilities, practitioners and their affiliates
 - §9606(1): allow consumers to request the publicly available information a controller has about them
 - §9608(6)(C)(2)(e-f): in the opt-out preference signal provision, do not prohibit the use of default settings or prohibit unfairly disadvantaging another controller
 - §9614: add a private right of action (see description above of the Attorney General’s proposal)
- d. *Advertising Trade Associations (see also concerns shared with Retail Assoc. of Maine, below)*
 - §9602(34) & §9608(1)(B): The definition of “sensitive data” should be amended to remove categories (like gender identity) not included in other state laws and the restriction on the sale of sensitive data should also be eliminated as it prevents most targeted advertising that consumers may appreciate
 - §9606(1)(F): Requiring controllers to disclose the names (not just the categories) of 3rd parties to whom they sell the consumer’s personal data is overly burdensome and should be removed
- e. *Center for Democracy and Technology (additional concern)*
 - §9608(34)(C): “sensitive data” includes data of a consumer that a controller “knows or reasonably should know is a minor.” Prefer a “knowledge fairly implied under objective circumstances” standard
- f. *Consumer Data Industry Association*
 - Replace the definition of “publicly available information” with the definition used in LD 1224—specifically, do not exclude inferences derived from publicly available info. from this definition
- g. *Electronic Privacy Information Center and Consumer Reports*
 - §9608(6)(C) – the word “or” on page 14, line 28 should be changed to “and” to require all controllers to provide a universal opt-out mechanism beginning July 1, 2026
- h. *Electronic Privacy Information Center (EPIC)*

- §9602(31)(A)(3): strike this part of the definition of “publicly available information”—which includes info. the consumer gave to another person—and replace it with language stating public available information does not include “data the consumer has restricted to a specific audience”
- §9602(33)(6): strike this part of the definition of “sale of personal data”—which excludes transfers after bankruptcy or mergers—instead, add language to the exempt activities list in §9613(1) allowing the transfer of data during a merger or acquisition as long as the controller gives advance notice to consumers and provides a reasonable opportunity to revoke consent or request deletion of their data
- §9608(1)(G): delete this provision, which would allow consumers to consent to processing data for purposes neither reasonably necessary to nor compatible with the disclosed purposes
- i. *Findhelp*
 - §9602(34): include within the “sensitive data” definition all “social care data” and define that term as it is proposed to be defined in House Bill No. 378, which is pending in Massachusetts. Attachment C
- j. *Internet Safety Labs*
 - §9606(1)(G)(2): consumers should not be limited to opting out of the sale of the personal data; instead they should be required to opt-in to the personal sale of their data
- k. *L.L. Bean*
 - §9608(2)(A): should be amended to allow controllers to collect and process data about consumers who visit their websites, even if they have not yet directly requested a product or service, to preserve the ability of controllers to provide targeted advertising. If providing a “service” is providing the retail website, then this should be made clear to clearly allow this type of advertising practice.
- l. *Retail Association of Maine and Maine Policy Institute*
 - §9608(3)(B): prohibiting the sale of personal data from being a condition of participation in a consumer loyalty program is overly restrictive given standard industry practices; the bill should be amended to clarify that “data sharing with a service provider or affiliate strictly for the purpose of administering the loyalty program” is not considered a “sale” if the data is not used or sold further
- m. *Retail Association of Maine and Maine State Chamber of Commerce and Advertising Trade Associations*
 - §9608(1)(A): the “strictly necessary” standard for the collection or processing of sensitive data is too strict of a data minimization standard and prohibits consumers from consenting to collection of sensitive data for example, for product recommendations or fraud-detection purposes
 - §9608(2)(A): the “reasonably necessary and proportionate to provide or maintain a specific product or service requested” standard for collecting personal data will prevent targeted advertising using common existing platforms and prevent measurement of the effectiveness of targeted advertising
- n. *Retail Association of Maine and Maine State Chamber of Commerce:*
 - §9602(34)(F): the phrase “billing, financial or payment method information” in the definition of “sensitive data” is too vague and may prevent the collection of sales and purchase price trend data.
 - §9610: the 3rd party responsibilities require 3rd parties to know details of initial privacy disclosures made to consumers, which is not feasible. 3rd parties may also not have a way to contact consumers
 - §9611(2): data protection assessments should not be required for “each algorithm that is used,” regardless of whether the algorithm involves a processing activity with a heightened risk
- o. *Retail Association of Maine and Hospitality Maine:*
 - §9602(34)(C): “sensitive data” should not include the personal data of all minors; instead, teens between the agencies of 15-17 should be excluded from this definition to avoid restricting their consumer activity or job opportunities. In addition, the phrase “should have known,” when related to a minor’s age, is ambiguous. Prefer “known to be a child” (<13)

8. Other general proposals for all three bills

a. *Maine Policy Institute (other recommendations not listed above)*

- Broaden the definition of “publicly available information” to include journalistic activities and widely disseminated information
- Clarify that “necessary” processing of sensitive data includes service personalization and internal analytics as long as customers can opt-out of these uses
- Do not require disclosure of 3rd parties with whom personal data is shared
- Allow targeted advertising with opt-in consent; including with parental consent for minors aged 13-15
- Further protect political speech and canvassing activities (Analyst Note: see LD 1822, §9613(5).)

TECHNICAL AND DRAFTING ISSUES

The analyst has identified a few technical drafting issues in each bill. If the committee votes in favor of an amended version of one or more of these bills, the analyst requests permission to work with a designated person on each report to address these technical issues.

REQUESTS FOR INFORMATION

Request made to	Information Requested
Rep. Henderson	• How does your bill compare to data privacy laws in New England? • What aspects of data privacy legislation should be uniform across states?
Rep. Roberts	• Please provide detail on the differences between LD 1088 and LD 1224? <i>Answer – see attached OPLA chart comparing the provisions of the 3 bills</i> • How does your bill compare to the data privacy laws in New Hampshire, Connecticut, Rhode Island, Minnesota and Virginia? • Why exempt small businesses from data privacy legislation? • Are you amenable to an entity-level exemption for higher education institutions?
AAG O’Neil	• Please attend the work session
Analyst	• When does the Maryland Online Data Privacy Act of 2024 take effect? <i>Answer: October 1, 2025</i> • Do any states provide a private cause of action for their data privacy laws? <i>Answer – see email from EPIC indicating that no state’s comprehensive data privacy legislation has a private cause of action. Attachment D.</i>
EPIC Caitriona Fitzgerald	• Is there a way to refine the targeted advertising prohibitions and data minimization standard in LD 1822 to allow targeted advertising based on a consumer’s search query, not only a specific consumer purchase? • How has Maryland proposed to interpret its newly enacted (but not yet effective) data minimization language with respect to targeted advertising?
L.L. Bean Christy Van Voorhees	• Does L.L. Bean use both targeted advertising and non-targeted advertising? How effective are these relative to each other?

Maine Automobile Dealers Association Bruce Gerrity	• Please provide a written copy of your testimony <i>Answer – MADA's testimony is now available online</i>
Maine Bankers' Ass'n Josh Steirman	• Please provide examples of the types of interactions banks have with Maine customers that would not be allowed under the exemption language in LD 1822
Stacey Stitham	• What provisions of LD 1224 do you believe provide for "data minimization"? • Please attend the work session
State Privacy & Security Coalition Andrew Kingman	• Please provide a written copy of your testimony <i>Answer – an electronic copy of SPSC's testimony on LD 1224 was emailed to the analyst and forwarded to the members of the committee</i>

FISCAL INFORMATION

LD 1099: See the preliminary fiscal impact statement (dated 4/8/25). Attachment E.

LD 1224 & LD 1822: Not yet determined by OFPR.

Public Records Exceptions Review
 Judiciary Committee — 132nd Legislature

LD _____ from _____ Committee

Proposed citation: _____ Brief description: _____

Statutory Review Criteria 1 M.R.S. §434(2), (2-A) & (2-B)	Notes
A. Whether a record protected by the proposed exception needs to be collected and maintained ;	
B. The value to the agency or official or to the public in maintaining a record protected by the proposed exception;	
C. Whether federal law requires a record covered by the proposed exception to be confidential;	
<i>Does the proposed public record exception meet one or more of the following (D, E, F, or G)?</i>	
D. Whether the proposed exception protects an individual's privacy interest and, if so, whether that interest substantially outweighs the public interest in the disclosure of records;	
E. Whether public disclosure puts a business at a competitive disadvantage and, if so, whether that business's interest substantially outweighs the public interest in the disclosure of records;	
F. Whether public disclosure compromises the position of a public body in negotiations and, if so, whether that public body's interest substantially outweighs the public interest in the disclosure of records;	
G. Whether public disclosure jeopardizes the safety of a member of the public or the public in general and, if so, whether that safety interest substantially outweighs the public interest in the disclosure of records;	
G-1. Whether public access to the record ensures or would ensure that members of the public are able to make informed health and safety decisions ;	
<i>This criterion applies to all reviews:</i>	
H. Whether the proposed exception is as narrowly tailored as possible;	
I. Any other criteria that assist the review committee in determining the value of the proposed exception as compared to the public's interest in the record protected by the proposed exception.	
<i>If the public records exception creates broad confidentiality for an agency:</i>	
2-A. Accountability review of agency or official. In evaluating each proposed public records exception, the review committee shall, in addition to applying the criteria [above], determine whether there is a publicly accountable entity that has authority to review the agency or official that collects, maintains or uses the record subject to the exception in order to ensure that information collection, maintenance and use are consistent with the purpose of the exception and that public access to public records is not hindered.	
2-B. Accessibility of public records. In reviewing and evaluating whether a proposal may affect the accessibility of a public record, the review committee may consider any factors that affect the accessibility of public records, including but not limited to fees, request procedures and timeliness of responses.	
ARCHIVES NOTE: 5 MRSA §95-C(1)(C) provides that records of archival value that are transferred to the Maine State Archives for permanent retention lose their confidential status, even if the statute designates such records as confidential, when they have been in existence for 75 years. <i>Note: The committee may suggest exempting specific types of public records from this law or suggest that a different time frame apply to specific types of public records under this law.</i>	

Public Records Exceptions Review
Judiciary Committee — 132nd Legislature

LD _____ from _____ Committee

Judiciary Committee Recommendation

Date _____

- ☐ The proposed public records exception meets the criteria listed in Title 1, section 434 and the Judiciary Committee approves the proposed language:

☐ Without change;

☐ With a suggestion that the records be exempt from Title 5, section 95-C(1)(C), under which records transferred to the Maine State Archives for permanent retention lose their confidential status when they have been in existence for 75 years.

Proposal (length of time to retain confidential status): _____

- ☐ The proposed public records exception does not meet the criteria listed in Title 1, section 434 for the following reasons:

and the Judiciary Committee recommends that the committee of jurisdiction consider making the following changes in the language of the proposed public records exception to address the(se) issue(s):

Vote: For:

Against:

Absent

Minority report(s):

HOUSE No. 378**The Commonwealth of Massachusetts**

PRESENTED BY:

Jessica Ann Giannino

To the Honorable Senate and House of Representatives of the Commonwealth of Massachusetts in General Court assembled:

The undersigned legislators and/or citizens respectfully petition for the adoption of the accompanying bill:

An Act for the protection and privacy of social care information.

PETITION OF:

NAME:	DISTRICT/ADDRESS:	DATE ADDED:
Jessica Ann Giannino	16th Suffolk	1/17/2025
Brian W. Murray	10th Worcester	4/3/2025

HOUSE DOCKET, NO. 3628 FILED ON: 1/17/2025

HOUSE No. 378

By Representative Giannino of Revere, a petition (accompanied by bill, House, No. 378) of Jessica Ann Giannino relative to the protection and privacy of information about an individual's social needs. Consumer Protection and Professional Licensure.

The Commonwealth of Massachusetts

In the One Hundred and Ninety-Fourth General Court
(2025-2026)

An Act for the protection and privacy of social care information.

Be it enacted by the Senate and House of Representatives in General Court assembled, and by the authority of the same, as follows:

SECTION 1. The General Laws, as appearing in the 2022 Official Edition, are hereby amended by inserting after chapter 93L the following chapter:

CHAPTER 93M. Protection and Privacy of Social Care Information

SECTION 2. Definitions

"Closed-Loop Referral System" or "CLRS" means any system that stores the social care information of one or more individuals; enables the sharing of social care information with and between participating entities for the purpose of referring individuals for social care; and is capable of updating or showing updated referral activity, including data related to participating organizations completing referrals.

"Participating organization" means any entity that has the ability to create, receive, or update referrals, or other social care information in a CLRS, including, but not limited to, healthcare providers, health plans, public agencies, charitable and nonprofit organizations, CLRS technology vendors, and entities that provide social care.

“Social care” means care, services, goods, or supplies related to an individual’s social needs. “Social care” includes, but is not limited to, support and assistance for an individual’s food stability and nutritional needs, housing, transportation, economic stability, employment, education access and quality, child care and family relationship needs, and environmental and physical safety.

“Social care information” means any information that relates to the need for, payment for, or provision of social care, and identifies the person receiving social care, or for which there is a reasonable basis to believe the information can be used to identify the individual receiving social care.

SECTION 3.

(a) In a manner that is consistent with federal and State law, a participating organization shall not sell or license social care information that is stored in or transmitted through a closed-loop referral system.

(b) In a manner that is consistent with federal and State law, social care information stored in or transmitted through a closed-loop referral system shall not be used for any purpose other than the purpose for which that information was collected or generated.

(c) A participating organization that sells, offers for sale, licenses, or otherwise furnishes, provides, or transmits to any other individual or entity social care information in violation of this section shall be liable to a civil penalty of \$1,000 for each violation.

(d) A civil penalty assessed pursuant to this section shall be collected and enforced by the attorney general.

SECTION 4. Implementation

The attorney general may adopt, amend, or repeal rules and regulations as shall be necessary for the implementation, administration, and enforcement of this chapter.

SECTION 5. Effective Date

This act shall take effect 90 days following the date of enactment.

Stocco, Janet

From: Stocco, Janet
Sent: Wednesday, May 7, 2025 9:33 AM
To: Legislature: Committee on Judiciary
Subject: FW: privacy laws & private rights of action & damages

Dear Judiciary Committee Members,

Please find below an answer from Caitriona Fitzgerald of EPIC to a question posed at the public hearing on the consumer data privacy bills — specifically whether any other state's consumer data privacy legislation provides a private right of action.

Sincerely, Janet

From: Caitriona Fitzgerald <fitzgerald@epic.org>
Sent: Tuesday, May 6, 2025 3:50 PM
To: Stocco, Janet <Janet.Stocco@legislature.maine.gov>
Subject: privacy laws & private rights of action & damages

This message originates from outside the Maine Legislature.

Janet,

Here's information for the question you received on for any states have that privacy legislation with private rights of action, what form of damages to they have:

No state has enacted a comprehensive privacy law with a private right of action. A few sectorial privacy laws have private rights of action:

- **Illinois Biometric Privacy Act:** originally passed in 2008, a number of cases have been brought under this law. Until recently, the law provided for statutory damages of up to \$1,000 per negligent violation and \$5,000 per intentional or reckless violation. After the Illinois Supreme Court ruled that each time an entity scanned or transmitted a biometric identifier was an individual violation, the Illinois Legislature last year passed a law limiting damages to \$5,000. A couple of examples of cases brought under BIPA:
 - <https://www.aclu.org/cases/aclu-v-clearview-ai>
 - <https://www.reuters.com/legal/legalindustry/facebook-pivots-facial-recognition-system-following-biometric-privacy-suit-2022-01-26/>
- **Washington My Health My Data Act:** passed in 2023, it provides that a private right of action may be brought under the Washington Consumer Protection Act for violations. The Consumer Protection Act states "It shall be presumed that damages to the consumer are equal to the cost of the service provided plus two hundred dollars. Additional damages must be proved."
 - The law only came into effect recently, and the first case was filed in February 2025: <https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20250220-first-lawsuit-filed-under-washingtons-my-health-my-data-act>

- **Virginia** just passed updates to its privacy law to protect reproductive and sexual health information and applied a private right of action to those sections. Penalties may include the greater of actual damages or \$500 (if violation is willful, this increases to the greater of treble actual damages or \$1,000), as well as attorney fees and costs.
- **New Jersey** passed Daniel's Law in 2020, a statute that prohibits public disclosure of home addresses or unpublished telephone numbers of certain law enforcement officers, judicial officers, and prosecutors, including by data brokers. Penalties include \$1,000 per violation.

Hope this helps!

Best,
Caitriona

--
Caitriona Fitzgerald (she/her)
Deputy Director
Electronic Privacy Information Center (EPIC)
202.483.1140 x105
epic.org | [@epicprivacy](https://twitter.com/epicprivacy)



132nd MAINE LEGISLATURE

LD 1088

LR 2064(01)

An Act to Enact the Maine Consumer Data Privacy Act

Preliminary Fiscal Impact Statement for Original Bill

Sponsor: Rep. Henderson of Rumford

Committee: Judiciary

Fiscal Note Required: Yes

Preliminary Fiscal Impact Statement

	FY 2025-26	FY 2026-27	Projections FY 2027-28	Projections FY 2028-29
Appropriations/Allocations				
Other Special Revenue Funds	\$500	\$500	\$500	\$500

Correctional and Judicial Impact Statements

This bill may increase the number of civil suits filed in the court system. The additional workload associated with the minimal number of new cases filed in the court system does not require additional funding at this time. The collection of additional filing fees will increase General Fund revenue by minor amounts.

Fiscal Detail and Notes

The bill establishes the Maine Privacy Fund within the Office of the Attorney General with a base Other Special Revenue Funds allocation of \$500 beginning in fiscal year 2025-26.

Any additional costs to the Office of the Attorney General associated with enforcing the Maine consumer data privacy act are expected to be minor and can be absorbed within existing budgeted resources.

Sec. Appropriations and allocations.

The following appropriations and allocations are made.

ATTORNEY GENERAL, DEPARTMENT OF THE

Maine Privacy Fund N530

Initiative: Establishes the Maine Privacy Fund with a base Other Special Revenue Funds allocation of \$500.

OTHER SPECIAL REVENUE FUNDS

All Other

2025-26

2026-27

\$500

\$500

OTHER SPECIAL REVENUE FUNDS TOTAL

\$500

\$500

**ATTORNEY GENERAL, DEPARTMENT OF THE
DEPARTMENT TOTALS**

2025-26

2026-27

OTHER SPECIAL REVENUE FUNDS

\$500

\$500

DEPARTMENT TOTAL - ALL FUNDS

\$500

\$500

132nd Maine Legislature
An Act to Enact the Maine Online Data Privacy Act
L.D. 1822

Amend LD 1822, Section 9604, to add a new section 9604(1)(I) as follows:

- I. A person or entity that is a motor vehicle dealer franchisee under 10 M.R.S. §1171(7)

Summary

LD 1822 contains exemptions from the proposed legislation. Franchised new car/truck dealers currently are subject to significant privacy obligations under both state and federal law. These include data and privacy protections under 10 M.R.S. §1174(3)(V) involving dealer/manufacturer privacy protection obligations with customer information, Gramm-Leach-Bliley; the Federal Trade Commission Act (15 USC § 41 et seq.), including the Fair Credit Reporting Act (15 USC §1681), The Fair and Accurate Credit Transactions Act (15 USC §150) and the FACT Act Identity Theft Rules; limited reporting of customer information to the Internal Revenue service regarding payment of cash or cash equivalents of more than \$10,000 (IRS Form 80: DSA E-FILING System); healthcare protections as a health insurer, including as a Multiple Employer Welfare Arrangement; the Maine Right to Repair Statute, 29-A M.R.S. §1801 et., which includes consumer privacy protections, safety protections and cyber security; new car warranty claims and recalls by the National Highway Traffic Safety Institute. Given the breadth of these obligations franchised motor vehicle dealers should be exempt.

Submitted by the
Maine
Automobile Dealers Association
May 29, 2025

May 29, 2025

Senator Anne Carney, Senate Chair
Representative Amy Kuhn, House Chair
Joint Standing Committee on Judiciary
100 State House Station
Augusta, ME 04333

Senator Carney, Representative Kuhn, and Members of the Joint Standing Committee on Judiciary:

While we appreciate the time and effort that the Judiciary Committee has put into LD 1822, as amended, the undersigned cannot support this bill. To focus on our predominant concerns, we limit this letter to two major issues with the proposed legislation—although we continue to have other objections that we have expressed and which have thus far gone unaddressed.¹

By way of reference and comparison, we address the following proposed language:

	LD 1088/LD 1224	LD 1822
<i>Data Minimization</i>	[9606(1)[A]] 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.	[9608(2)] A controller shall: A. Limit the collection of personal data to what is reasonably necessary and proportionate to provide or maintain a specific product or service requested by the consumer to which the data pertains including any routine administrative, operational, website, or account-servicing activity that is consistent with the reasonable expectations of the consumer. This subparagraph does not prevent a controller from processing personal data collected in accordance with this paragraph to provide advertising to a consumer based on the consumer's

¹ Specifically, we maintain our objection (carried over from the original draft) to: (1) the language around the processing of data from minors (both in its applicability to teenagers and in the standard applied for knowledge that the user is in fact a minor); and (2) the language around an exception for “the sale of personal data” within the discussion of loyalty programs. We also have concerns regarding: (1) the amended draft’s changes to the merger, bankruptcy, or other acquisition exception; and (2) the definition of publicly available information.

		activities within a controller's own websites or online applications.
<i>Sensitive Data</i>	[9606(3)[A]] A controller may not: A. Process sensitive data concerning a consumer unless the controller obtains the consumer's consent [<i>prior to processing</i>];	[9608(1)] A controller may not: A. Collect, process or share sensitive data concerning a consumer, unless the collection or processing is strictly necessary to maintain a specific product or service requested by the consumer;
		B. Sell sensitive data;

In advancing LD 1822, the Judiciary Committee seems to be pursuing two strands of logic which are in fundamental tension with another. On the one hand, there seems to be skepticism that the disclosure requirements around data collection in LD 1088/LD 1224 accomplish any meaningful restriction (an argument embodied by the position that consumers “don’t read” terms of use or privacy policies) and a concern that we should do more to hold websites to account in terms of what data they collect (including a discussion as to whether the phrase “reasonable expectations of the consumer” in the data minimization provision of LD 1822 should be strengthened). Yet at the same time, in order to avoid the conclusion that LD 1822 would negatively impact Maine businesses’ ability to reach potential customers, Committee members have repeatedly advanced the position that the data minimization provision in 9608(2)[A] would *not* impact a business’s ability to engage in targeted advertising.

The latter view appears to be based on the interpretation that a visitor to a website is “requesting a service” from the website’s owner, so that any cookies that fire to collect data from the visitor while on the website (and later used by the collecting business to market to that visitor, or shared with Google and other advertising platforms) are “reasonably necessary” to provide or maintain the company’s website. Even if you equate “website” with “service,” it is a very strained interpretation of what is “reasonably necessary and proportionate” to “provide or maintain” a “specific product or service” requested by a consumer to argue that the mere fact of visiting the website of a Bangor-based sports store and searching for bicycles is a “request” for ongoing advertising from the store at all, much less a request that the consumer’s data be collected for purposes of helping to build audience profiles that may be used by Google Ads and others to signal that the consumer is a good candidate to receive communications and marketing materials about outdoor gear, local bike tours, or other topics of interest to someone with an active lifestyle. More probably, this activity, visiting the website, is a time-bound request simply to show the consumer available bikes, and there is a real risk the language would be judicially interpreted and enforced by the Attorney General’s Office in that fashion—regardless of what is being floated around in the Committee room.

After the business community voiced alarm at the public hearing, we were assured that the intent of the data minimization clause in LD 1822 was not to ban targeted advertising and that the requested amendment would provide clarity. It did—language was added that clarified that the subparagraph “*does not prevent a controller* from processing personal data collected in accordance with this paragraph to provide advertising to a consumer *based on the consumer’s activities within a controller’s own websites or online applications.*” As pointed out, however, advertisements based on a consumer’s activities within a controller’s own websites or online applications are explicitly exempt from the definition of targeted advertising, *see* 9602(37)[B](2). So the provided clarity only indicates that the subparagraph isn’t intended to bar *other* forms of advertising done by the controller of the website the consumer has visited, and says nothing about targeted advertising or cross-site advertising. Indeed, the fact that language was added clarifying that *some* forms of (non)targeted advertising are *not* barred by the data minimization clause only adds fuel to the conclusion that other forms of advertising, targeted advertising, *are* barred by the clause.

In addition to the fact that the reassurance that this clause is not intended to affect targeted advertising doesn’t square with the statutory language, if we credit the interpretation offered by the Judiciary Committee, it is far *less* privacy protective than LD 1088 (or LD 1224). The data minimization clause in 9606(1)[A] of LD 1088/LD 1224 is simple and straightforward: “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.” In short, collection of data must be tied to disclosed purposes. As mentioned at the beginning of this letter, this language has been unfairly dismissed as not consumer protective, yet under the interpretation of the data minimization language presently circulating with respect to LD 1822, a business can seemingly collect any amount of data they want, as long as the consumer visited their website, because by visiting the website, the consumer has opened the door to advertising from the business, sharing with advertising platforms, and cross-site advertising. Put differently, a consumer to a website governed by LD 1088/LD 1224 (not to mention the more than a dozen other state laws in effect using precisely this standard) could only have their data collected for purposes and reasons disclosed to them by the website’s owner. Meanwhile, a consumer to a website governed by the Judiciary Committee’s interpretation of LD 1822, would have “requested” to the deployment of cookies, pixels, tags and other advertising-related data collection methods merely by arriving on the website, without any sort of limitation that this data collection be tied to purposes disclosed to them.

Finally, we should not overlook the fact that the retailer of religious books, or LBGTQ items, or other “sensitive” products from which inferences may be made still must worry about the additional restrictions in 9608(1)[A] & [B]. These companies cannot “sell” their data, period—including sharing it for “other valuable consideration” (a part of the statutory definition of sale), which may impact their ability to participate in co-op marketing databases where they receive something of value in return. And they cannot *process or share*, much less collect, sensitive data unless “*strictly necessary*” to provide or maintain a specific product or service requested by a consumer. Again, it is difficult to credit the concept that the mere fact that I place

a phone order with a reseller of Christian books, or browse their website, looking at books on Catholicism, means that I have “requested” that my purchase or search history be collected for marketing purposes. And it is impossible to conclude that collection of my data in order to process my order for black hair care products permits that data to be processed or shared for any advertising-related purposes, as those purposes are not “strictly necessary” to fulfill my order.

Returning once more to the professed goals of LD 1822, consumer protection, it is worth noting that nowhere in LD 1822 is the processing of sensitive data tied to customer consent—unlike other state laws as well as LD 1088/1224. Instead, the gathering, use, and sharing of sensitive data is limited by what the *business* deems strictly necessary to provide or maintain a specific product or service requested by the consumer. And, under the position the Judiciary Committee is entertaining in order to avoid concerns about the impact on targeted advertising, that “request” can be an open-ended call for marketing merely by landing on a website.

In short, in LD 1088/1224, we have straightforward, easy-to-understand bills already passed by numerous states which accomplish two things: (1) tie the processing of sensitive data to explicit, opt-in consent from the individual; and (2) limit data collection to clearly-disclosed purposes. This well-trodden path would offer consumer protections while at the same time ensuring that Maine businesses do not face a competitive disadvantage against out-of-state businesses. In contrast, in LD 1822, we have a novel bill that *either* jeopardizes the ability of Maine’s small businesses to engage in targeted advertising (if you conclude that the mere visit to a website may not be deemed a “request” for targeted advertising) *or* allows for virtually unfettered use of cookies by a website’s owner (if you conclude that landing on a website is a “request” for advertising services). Either way, the bill is fraught with unintended consequences.

We appreciate the opportunities given to provide input throughout the process and thank you for your consideration.

Sincerely,

HospitalityMaine
Maine Bankers Association
Maine Golf
Maine Grocers & Food Producers Association
Maine State Chamber of Commerce
Maine Tourism Association
Manufacturers Association of Maine
NFIB Maine
Portland Regional Chamber of Commerce
Retail Association of Maine
Ski Maine Association

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Protected Data	❖ “Personal data”: § 9602 (17) p 3 - Data linked or reasonably linkable to an identifiable individual (a “consumer”) who is a Maine resident <u>Excludes:</u> § 9602 (16) p 3 “Publicly available information” (excludes biometric data, genetic data not revealed to the general public by the consumer; inferences from a combination of publicly available information and personal data; obscene visual depictions or intimate images created or shared without consent); and “de-identified data” § 9602 (15) p 2	❖ “Personal data”: § 9602 (16) p 3 - Data linked or reasonably linkable to an identifiable individual (a “consumer”) who is a Maine resident <u>Excludes:</u> “Publicly available information” (defined in a way that does not exclude the categories of information excluded in LD 1088 and LD 1822 as described in left-hand column of this table), and § 9602 (23) p 34 “de-identified data” § 9602 (13) p 2	❖ “Personal data”: § 9602 (24) p 4 - Data linked or reasonably linkable to (a) an identifiable individual (a “consumer”) who is a Maine resident or (b) a device linked or reasonably linked to a consumer <u>Excludes:</u> “Publicly available information” (defined differently than LD 1088 but excludes all of the same categories of information excluded in LD 1088 as described in the left-hand column of this table); and § 9602 (31) p 45 “de-identified data” § 9602 (14) p 2
	❖ “Sensitive data”: subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs, mental or physical health conditions/diagnoses; sexual orientation; citizenship or immigration status - Genetic or “biometric data” (defined on as certain data “capable of being used” to ID a specific individual) - Consumer health data (reveals condition or diagnosis) - Personal data of a person known to be a child (<13) - Precise geolocation data (within 1,750 feet) - Social security, driver’s license or nondriver ID number (except last 4 digits of these numbers); - Account number, log-in info, or credit or debit card number that, in combination with a security code or password, permits access to a financial account - Data concerning individual’s status as a crime victim § 9602 (20) p 5	❖ “Sensitive data”: subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs, medical history, mental or physical health conditions or diagnoses by a medical professional; sexual orientation; citizenship or immigration status - The processing of genetic or “biometric data” to uniquely ID an individual (“biometric data” defined as certain data “used” to ID a specific individual) - Personal data of a person known to be a child (<13) - Precise geolocation data (within 1,750 feet) - Data concerning individual’s status as a crime victim § 9602 (25) p 4	❖ “Sensitive data”: subset of personal data including: - Data revealing racial or ethnic origins, religious beliefs; sexual activity; sexual orientation; gender identity; national origin, citizenship or immigration status “Genetic”/ “biometric data” (biometric: defined as data that “can be used” to uniquely identify an individual) - Consumer health data (used to ID physical or mental health status, e.g., gender-affirming or reproductive care) - Personal data of a person the controller knows or should know is a minor (<18) - Precise geolocation data (within 1,750 feet) - Social security, driver’s license or nondriver ID number (including the last 4 digits of these numbers); - Billing, financial or payment method information (Except last 4 digits of credit card or similar number) - Account or device log-in, security codes or passwords - Data concerning consumer’s status as a crime victim § 9602 (34) p 5
	❖ <u>Exception</u> (both types of data above): p 2 “Consumer” is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	❖ <u>Exception</u> (both types of data above): p 1-2 “Consumer” is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context	❖ <u>Exception</u> (both types of data above): p 2 “Consumer” is defined to exclude an employee, contractor, etc. interacting with a controller solely in an employment context
	❖ Controller: person that alone or jointly with others determines purpose and means of processing personal data p 2 ❖ Processor: person that processes (collects, uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller p 3	❖ Controller: person that alone or jointly with others determines purpose and means of processing personal data p 2 ❖ Processor: person that processes (collects, uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller p 3	❖ Controller: person that alone or jointly with others determines purpose and means of processing personal data p 2 ❖ Processor: person that processes (uses, stores, discloses, analyzes, modifies or deletes) personal data for a controller p 7

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Consumer Rights <u>LD 1088</u> §9604 p 8 §9609 (3,4) p 15-16 <u>LD 1224</u> §9604 p 7-8 §9609 (3,4) p 14 <u>LD 1822</u> §9606 p 7-10 §9612 (2) p 17	❖ A consumer (or parent if child <13, guardian or conservator) has a right, upon making an authenticated request, to: • Confirm whether controller processes personal data • Access own personal data processed by controller • Correct inaccuracies in own personal data • Delete personal data about the consumer • Obtain a portable copy of own personal data from a controller; and, if technically feasible, in a way that can be transmitted to another controller <u>Exceptions:</u> • Controller need not disclose: (a) info. that would reveal a trade secret; (b) de-identified data or data controller is not reasonably capable of associating w/the consumer; (c) data it does not use to recognize the consumer; or (d) pseudonymous data if the information necessary to associate it with consumer is kept separately • If the controller does not sell the personal data or voluntarily disclose the data to anyone other than a processor, it need not respond to a consumer request • If controller did not itself collect the data the consumer requests be deleted, it may retain the minimum data necessary to ensure data remains deleted in its system and not use it for any other purpose	❖ A consumer (or parent if child <13, guardian or conservator) has a right, upon making an authenticated request, to: • Confirm whether controller processes personal data • Access own personal data processed by controller • Correct inaccuracies in own personal data • Delete personal data about the consumer • Obtain a portable copy of own personal data from a controller; and, if technically feasible, in a way that can be transmitted to another controller <u>Exceptions:</u> • Controller need not disclose: (a) info. that would reveal a trade secret; (b) de-identified data or data controller is not reasonably capable of associating w/the consumer; (c) data it does not use to recognize the consumer; or (d) pseudonymous data if the information necessary to associate it with consumer is kept separately • If the controller does not sell the personal data or voluntarily disclose the data to anyone other than a processor, it need not respond to a consumer request • If controller did not itself collect the data the consumer requests be deleted, it may retain the minimum data necessary to ensure data remains deleted in its system and not use it for any other purpose or opt the consumer out of processing that personal data	❖ A consumer (or parent if child <13, guardian or conservator) has a right, upon making an authenticated request, to: • Confirm whether controller processes personal data • Access own personal data processed by controller • Correct inaccuracies in own personal data • Delete personal data about the consumer — unless the controller is required by law to retain the personal data • When processing is by automatic means, obtain a portable copy of own personal data from a controller; if technically feasible, in a way that can be transmitted to another controller • Obtain a list of 3rd parties to which controller sold the consumer's personal data (or anyone's personal data) <u>Exceptions:</u> • Controller need not disclose: (a) info. that would reveal a trade secret; (b) de-identified data or data controller is not reasonably capable of associating w/the consumer; or (c) data it does not use to recognize the consumer • If the controller does not sell the personal data or voluntarily disclose the data to anyone other than a processor, it need not respond to a consumer request • If controller did not itself collect the data the consumer requests be deleted, it may retain the minimum data necessary to ensure data remains deleted in its system and not use it for any other purpose
Exercising consumer rights	❖ Request / appeal process: §9604 (3,4) p 9 • Each consumer may make one free request per year <u>except</u> controller may charge a reasonable fee or decline manifestly unfounded, excessive or repetitive requests • Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request • Controller must respond without undue delay and within 45 days of request (may extend once for 45 days) • If declines a request, must do so within 45 days, giving a justification and info. on how to appeal the decision	❖ Request / appeal process: §9604 (3,4) p 9 • Each consumer may make one free request per year <u>except</u> controller may charge a reasonable fee or decline manifestly unfounded, excessive or repetitive requests • Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request • Controller must respond without undue delay and within 45 days of request (may extend once for 45 days) • If declines a request, must do so within 45 days, giving a justification and info. on how to appeal the decision	❖ Request / appeal process: §9606 (5,6) p 10 • Each consumer may make one free request per year <u>except</u> controller may charge a reasonable fee or decline a manifestly unfounded, excessive, technically infeasible or repetitive requests • Controller need not fulfill unauthenticated request, but must notify consumer of the unauthenticated request • Controller must respond without undue delay and within 45 days of request (may extend once for 45 days) • If declines a request, must do so within 45 days, giving a justification and info. on how to appeal the decision

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	• Appeal: Consumer may appeal controller's inaction or denial within a reasonable time and decision in response to appeal (with reasoning) is required within 60 days • If appeal is denied, must provide online mechanism (if any) for consumer to submit a complaint to the AG	• Appeal: Consumer may appeal controller's inaction or denial within a reasonable time and decision in response to appeal (with reasoning) is required within 60 days • If appeal is denied, must provide online mechanism (if any) for consumer to submit a complaint to the AG	• Appeal: Consumer may appeal controller's inaction or denial within a reasonable time and decision in response to appeal (with reasoning) is required within 60 days • If appeal is denied, must provide online mechanism (if any) for consumer to submit a complaint to the AG
Required privacy notice <u>LD 1088</u> § 9605(5) p. 11 <u>LD 1224</u> § 9606(5) p. 10 <u>LD 1822</u> § 9608(4) p. 13	❖ Controller must provide accessible, clear privacy notice in plain language understandable by reasonable consumer stating: • Categories of personal data processed (remember, process includes collection) by controller • Purpose for processing personal data • How consumers may exercise their consumer rights • Categories of personal data shared with 3rd parties • Categories of 3rd parties personal data is shared with • Controller's contact information (active e-mail or other)	❖ Controller must provide accessible, clear privacy notice in plain language understandable by reasonable consumer stating: • Categories of personal data processed (remember, process includes collection) by controller • Purpose for processing personal data • How consumers may exercise their consumer rights • Categories of personal data shared with 3rd parties • Categories of 3rd parties personal data is shared with • Controller's contact information (active e-mail or other)	❖ Controller must provide accessible, clear privacy notice in plain language understandable by reasonable consumer stating: • Categories of personal data, including sensitive data, processed (does not include collecting) by controller • Purpose for processing personal data • How long controller intends to retain each category of personal data (or criteria for deciding how long) • How consumers may exercise their consumer rights • Categories of personal data, including sensitive data, shared with 3rd parties • Categories of 3rd parties personal data is shared with — with level of detail to allow consumer to understand type of processing conducted by each category • Controller's contact information (active e-mail or other)
Targeted Advertising Definition	"Targeted advertising" means displaying an advertisement to a consumer when the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated publicly accessible websites or online applications to predict that consumer's preferences or interests. "Targeted advertising" does not include: A. Advertisements based on activities within a controller's own publicly accessible websites or online applications; B. Advertisements based on the context of a consumer's current search query, visit to a publicly accessible website or online application; C. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or D. Processing personal data solely to measure or report advertising frequency, performance or reach. p5	"Targeted advertising" means displaying an advertisement to a consumer when the advertisement is selected based on personal data obtained or inferred from that consumer's activities over time and across nonaffiliated publicly accessible websites or online applications to predict that consumer's preferences or interests. "Targeted advertising" does not include: A. Advertisements based on activities within a controller's own publicly accessible websites or online applications; B. Advertisements based on the context of a consumer's current search query, visit to a publicly accessible website or online application; C. Advertisements directed to a consumer in response to the consumer's request for information or feedback; or D. Processing personal data solely to measure or report advertising frequency, performance or reach. p4	"Targeted advertising": A. Means displaying advertisements to a consumer or on a device identified by a unique identifier when the advertisement is selected based on personal data obtained or inferred from the consumer's activities over time and across nonaffiliated websites or online applications that are unaffiliated with each other in order to predict the consumer's preferences or interests; and B. Does not include: (1) Advertisements based on the context of a consumer's current search query or visit to a website or online application; (2) Advertisements based on a consumer's activities within a controller's own websites or online applications; (3) Advertisements directed to a consumer in response to the consumer's request for information or feedback; or (4) Processing personal data solely to measure or report advertising frequency, performance or reach. p6

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Data minimization	❖ Must limit collection of personal data to what is §9606(1) P.10 “adequate, relevant and reasonably necessary” to the processing purpose disclosed to the consumer (in the privacy notice) ❖ Must process minimum amount of personal data “reasonably necessary, adequate or relevant” to each disclosed purpose (in the privacy notice)	❖ Must limit collection of personal data to what is §9606(1) P.9 “adequate, relevant and reasonably necessary” to the processing purpose disclosed to the consumer (in the privacy notice)	❖ Must limit collection of personal data to what is §9605(2)(b) P.12 “reasonably necessary and proportionate to provide or maintain the specific product or service requested by the consumer” ❖ Must limit collection and processing of sensitive data to what is “strictly necessary” to provide or maintain the specific product or service requested by the consumer §9605(1)(A) P.12
Consent requirements	<u>LD 1088</u> §9606(1-3) P.10-11 §9604(1)(E) P.8 ❖ Prohibited activities (regardless of consent) - Process personal data of a minor known (or willfully disregarded) to be 13-15 for targeted advertising - Process data of a known child <13 years old in violation of federal COPPA law/regulation requirements ❖ Activities permitted only with consent (opt-in) - Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose — as a matter of law, sale of sensitive data is not “reasonably necessary [or] compatible” - Process sensitive data for any purpose (this consent requires disclosure of specific processing purpose, categories of sensitive data to be processed, and identity of any 3rd parties to whom the data is sold. If there is no contact for 24 months, customer must opt-in again). - Sell personal data of a minor known (or willfully disregarded) to be age 13-15 <u>Exceptions:</u> “sale” defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate; (d) 3rd party consumer intentionally wants controller to interact with; or (d) successor in interest after merger, bankruptcy, other transaction. ❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <16) - For targeted advertising - For sale (see exceptions to “sale” above) - For profiling in furtherance of automated decisions producing legal or similarly significant effects	<u>LD 1224</u> §9606(1-3) P.9-10 §9604(1)(E) P.7-8 ❖ Prohibited activities (regardless of consent) - Process personal data of a minor known (or willfully disregarded) to be 13-15 for targeted advertising - Process data of a known child <13 years old in violation of federal COPPA law/regulation requirements ❖ Activities permitted only with consent (opt-in) - Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose - Process sensitive data for any purpose - Sell personal data of a minor known (or willfully disregarded) to be age 13-15 <u>Exceptions:</u> “sale” defined to exclude sharing personal data with (a) processor; (b) 3rd party for purpose of providing requested product or service; (c) affiliate; (d) 3rd party consumer intentionally wants controller to interact with; or (d) successor in interest after merger, bankruptcy, other transaction. ❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <16) - For targeted advertising - For sale (see exceptions to “sale” above) - For profiling in furtherance of automated decisions producing legal or similarly significant effects	<u>LD 1822</u> §9608(1-2) P.12-13 §9606(1)(G) P.9 ❖ Prohibited activities (regardless of consent) - Sell any consumer’s sensitive data (includes all personal data of known (should know) minor (<18)) - Process personal data of a person known (should know) to be a minor (<18) for targeted advertising ❖ Activities permitted only with consent (opt-in) - Process personal data for purpose “neither reasonably necessary for, nor compatible with” a disclosed purpose - Retain personal data past the time “when it is no longer necessary for the purpose for which the data was processed” ❖ Activities permitted unless consumer objects (opt-out) Processing personal data (of person not known to be <18) - For targeted advertising - For sale (same exceptions to “sale” as in LD 1088 & 1224) - For profiling in furtherance of automated decisions producing legal or similarly significant effects

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Consent Mechanisms <i>Opt-In</i> <i>See "consent" definitions p. 1 all bills</i> <i>Revoke</i> <i>1088 - p. 10</i> <i>1224 - p. 9-10</i> <i>1822 - p. 13</i>	❖ Opt-In "consent" mechanism / requirements: - Opt-in consent may be provided by (a) consumer or (b) parent or legal guardian of minor consumer <13 years old (in accordance with federal COPPA law) p. 8 - Clear, affirmative act unambiguously signaling consent - In language consumer uses to obtain the product or service and reasonably accessible to those w/disabilities May not be based on: (a) Accepting a terms of use agreement (containing info. unrelated to consenting); (b) hovering over, muting, pausing or closing content; or (c) use of dark pattern to obtain agreement Mechanism to revoke consent must be at least as easy as mechanism to provide consent and controller must cease processing within 15 days of revocation	❖ Opt-In "consent" mechanism / requirements: - Opt-in consent may be provided by (a) consumer or (b) parent or legal guardian of minor consumer <13 years old (in accordance with federal COPPA law) p. 7 - Clear, affirmative act unambiguously signaling consent May not be based on: (a) Accepting a terms of use agreement (containing info. unrelated to consenting); (b) hovering over, muting, pausing or closing content; or (c) use of dark pattern to obtain agreement Mechanism to revoke consent must be at least as easy as mechanism to provide consent and controller must cease processing within 15 days of revocation	❖ Opt-In "consent" mechanism / requirements: - Opt-in consent may be provided by (a) consumer or (b) parent or legal guardian of minor consumer <13 years old (in accordance with federal COPPA law) p. 6 - Clear, affirmative act unambiguously signaling consent to process personal data for a particular purpose May not be based on: (a) Accepting a terms of use agreement (containing info. unrelated to consenting); (b) hovering over, muting, pausing or closing content; or (c) use of dark pattern to obtain agreement Mechanism to revoke consent must be at least as easy as mechanism to provide consent and controller must cease processing within 30 days of revocation
	❖ Opt-out notice: Controller must clearly and conspicuously disclose on website the following & the method for opting out: - That it sells personal data to 3rd parties - That it processes personal data for targeted advertising § 9606(7) p. 12	❖ Opt-out notice: Controller must clearly and conspicuously disclose on website the following & the method for opting out: - That it sells personal data to 3rd parties - That it processes personal data for targeted advertising § 9606(7) p. 11	❖ Opt-out notice: Controller must clearly and conspicuously disclose on website the following & the method for opting out: - That it sells personal data to 3rd parties - That it processes personal data for targeted advertising - That it processes personal data for profiling § 9606(5) p. 13-14
	❖ Opt-Out mechanism / requirements: - Consumer (or parent if child <13 or a guardian or conservator) or designated agent may exercise opt-out rights (e.g., via browser or global device setting) § 9605 p. 10 - Must be secure and reliable and may not require new account. Must use links similar to "Do not sell my personal data" or "Opt me out of targeted advertising" or a single link similar to "Your Privacy Choices" By Dec. 1, 2027 – Universal Opt-Out: must allow consumer to use an opt-out signal sent by a platform, technology or other mechanism used by the consumer that is consumer friendly; does not unfairly disadvantage another controller; does not use a default setting; is consistent with other opt-out mechanisms required by federal or state law; and allows controller to reasonably determine the consumer is a Maine resident	❖ Opt-Out mechanism / requirements: - Consumer (or parent if child <13, or a guardian or conservator) or – to opt out of only sale or targeted advertising, but not profiling: designated agent may exercise opt-out rights (e.g., via browser setting or global device setting) § 9605 p. 9 - Must be secure and reliable and may not require new account By Dec. 1, 2027 – Universal Opt-Out: must allow consumer to use an opt-out signal sent by a platform, technology or other mechanism used by the consumer that is consumer friendly; does not unfairly disadvantage another controller; does not use a default setting; is consistent with other opt-out mechanisms required by federal or state law; and allows controller to reasonably determine the consumer is a Maine resident	❖ Opt-Out mechanism / requirements: - Consumer (or parent if child <13 or a guardian or conservator) or designated agent may exercise opt-out rights (e.g., via browser or global device setting) § 9607 p. 12 - Must be secure and reliable and may not require new account. § 9603(6) p. 14 By July 1, 2026 – Universal Opt-Out: must allow consumer to use an opt-out signal sent by a platform, technology or other mechanism used by the consumer that is consumer friendly and in easy-to-understand language; does not unfairly disadvantage another controller; does not use a default settings; is consistent with other opt-out mechanisms required by federal or state law; and allows controller to reasonably determine the consumer is a Maine resident — if conflicts with loyalty program, may notify and ask to confirm opt-out
	§ 9606 (6-8) p. 12-13	§ 9606 (6-8) p. 10-11	§ 9606 (6)(c)(2) p. 14-15

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Retaliation prohibition § 9606(3)(D)+(4) p.11 LD 1224 § 9606(3)(D)+(4) p.10 LD 1822 § 9608(1)(E)+(3) p.12	❖ Controller may not discriminate against consumer for exercising a right under this law, including by: - Denying or charging different prices for goods/services - Providing different level or quality of goods or services <u>Exceptions:</u> - Need not offer product or service without having required personal data - May offer different price, quality or selection of goods or services via a voluntary consumer loyalty program	❖ Controller may not discriminate against consumer for exercising a right under this law, including by: - Denying or charging different prices for goods/services - Providing different level or quality of goods or services <u>Exceptions:</u> - Need not offer product or service without having required personal data - May offer different price, quality or selection of goods or services via a voluntary consumer loyalty program	❖ Controller may not discriminate against consumer for exercising a right under this law, including by: - Denying or charging different prices for goods/services - Providing different level or quality of goods or services <u>Exceptions:</u> - Need not offer product or service without having required personal data - May offer different price, quality or selection of goods or services via a voluntary consumer loyalty program - sale of personal data may not be a program condition
Discrimination prohibitions	❖ Controller may not: § 9606(3)(E) p.11 Process (collect, use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers	❖ Controller may not: § 9606(3)(E) p.10 Process (collect, use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers	❖ Controller may not: § 9603(1)(C)(F) p.12 - Process (use, disclose, analyze, delete) personal data in manner that violates state and federal laws prohibiting unlawful discrimination against consumers - Collect, process or disclose personal data or publicly available info. in a way that unlawfully discriminates or prevents equal enjoyment of goods or services on basis of individual's actual or perceived protected class status <u>Except:</u> may self-test to prevent discrimination or diversify applicant pool. Does not apply to a private club exempt from Title II of the Civil Rights Act.
Geofence prohibition	❖ Person may not use geofence (1,750 foot virtual perimeter) around health care facility for purpose of identifying, tracking, collecting data from or sending notices regarding consumer health data to a consumer who enters the virtual perimeter § 9606 p.16 <u>Exception:</u> Facility operator's geofence (ex: to check in patients)	No geofence prohibition	❖ Person may not use geofence (1,750 foot virtual perimeter) around health care facility for purpose of identifying, tracking, collecting data from or sending notices regarding consumer health data a consumer § 9605(3) p.11 <u>Exception:</u> Facility operator's geofence (ex: to check in patients)
Data Security and Retention § 9606(2)(B) p.10	❖ Controller must establish and implement reasonable data security practices to protect confidentiality, accessibility and integrity of data appropriate to the volume and nature of data ❖ Controller must establish and implement a data retention schedule requiring deletion or de-identification when retention of the data is "no longer reasonably necessary and relevant" to disclosed purposes for processing data—unless controller is required to retain the personal data longer by law § 9606(2)(A) p.10	❖ Controller must establish and implement reasonable data security practices to protect confidentiality, accessibility and integrity of data appropriate to the volume and nature of data § 9606(2)(A) p.9 No data retention schedule required	❖ Controller must establish and implement reasonable data security practices to protect confidentiality, accessibility and integrity of data appropriate to the volume and nature of data ❖ Controller must establish and implement a data retention schedule requiring destruction or permanent deletion of data when retention of the data is "no longer necessary" for the processing purpose — unless consumer consents to longer time or controller is required to retain the personal data longer by law § 9603(2)(B) p.12-13

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Data Protection Assessments <u>LD 1088</u> §9608 p. 14-15 <u>LD 1224</u> §9608 p. 12-13 <u>LD 1822</u> §9611 p. 17-18	❖ Controller must conduct and document data protection assessment(s) weighing direct and indirect benefits to controller, consumer and public of processing the data against the risks to consumers of processing the data, as mitigated by safeguards employable by the controller What activities must be assessed? All activities presenting a heightened risk to consumers that are created or initiated after July 1, 2026, including: - Processing of sensitive data - Processing personal data for targeted advertising - Sale of personal data - Processing of personal data for profiling that presents a reasonably foreseeable risk of unfair treatment of consumers, of physical, reputational or financial injury to consumers, offensive intrusion on consumer's private affairs; or other "substantial injury" Copy to AG: Must provide copy of assessment to AG on request (if relevant to an investigation). - Assessment is confidential (for FOAA purposes) - Disclosure to AG as required by law doesn't waive attorney-client or work-product privileges	❖ Controller must conduct and document data protection assessment(s) weighing direct and indirect benefits to controller, consumer and public of processing the data against the risks to consumers of processing the data, as mitigated by safeguards employable by the controller What activities must be assessed? All activities presenting a heightened risk to consumers that are created or initiated after July 1, 2026, including: - Processing of sensitive data - Processing personal data for targeted advertising - Sale of personal data - Processing of personal data for profiling that presents a reasonably foreseeable risk of unfair treatment of consumers, of physical, reputational or financial injury to consumers, offensive intrusion on consumer's private affairs; or other "substantial injury" Copy to AG: Must provide copy of assessment to AG on request (if relevant to an investigation). - Assessment is confidential (for FOAA purposes) - Disclosure to AG as required by law doesn't waive attorney-client or work-product privileges	❖ Controller must conduct and document data protection assessment(s) weighing direct and indirect benefits to controller, consumer and public of processing the data against the risks to consumers of processing the data, as mitigated by safeguards employable by the controller and the necessity and proportionality of processing vs stated processing purpose What activities must be assessed? All activities presenting a heightened risk to consumers, including each algorithm that is used, that occur after July 1, 2026, including: - Processing of sensitive data - Processing personal data for targeted advertising - Sale of personal data - Processing of personal data for profiling that presents a reasonably foreseeable risk of unfair treatment of consumers, of physical, reputational or financial injury to consumers, offensive intrusion on consumer's private affairs; or other "substantial injury" When required? Within 6 months of first engaging in the activity or of making a material change to that activity Copy to AG: Must provide copy of assessment to AG on request (if relevant to an investigation). - Assessment is confidential (for FOAA purposes) - AG may use the assessment in an enforcement action - Disclosure to AG as required by law doesn't waive attorney-client or work-product privileges
Processor duties and prohibitions	❖ Processor must: §9607 p. 13-14 - Assist controller with meeting obligations of this law - Assist controller with responding to consumer requests - Notify controller of any security breach in processor's system (when notice to consumer of a security breach is required by current Maine law: Title 10, chapter 210-B) - Provide necessary information to enable controller to conduct data protection assessments - Act only under contract with controller requiring it to: - Ensure each person processing personal data is subject to a duty of confidentiality	❖ Processor must: §9607 p. 11-12 - Assist controller with meeting obligations of this law - Assist controller with responding to consumer requests - Notify controller of any security breach in processor's system (when notice to consumer of a security breach is required by current Maine law: Title 10, chapter 210-B) - Provide necessary information to enable controller to conduct data protection assessments - Act only under contract with controller requiring it to: - Ensure each person processing personal data is subject to a duty of confidentiality	❖ Processor must: §9609 p. 15-16 - Assist controller with meeting obligations of this law - Assist controller with responding to consumer requests - Notify controller of any security breach in processor's system (when notice to consumer of a security breach is required by current Maine law: Title 10, chapter 210-B) - Provide necessary information to enable controller to conduct data protection assessments - Act only under contract with controller requiring it to: - Ensure each person processing personal data is subject to a duty of confidentiality

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	○ Delete or return personal data at end of processing activity, unless retention required by law ○ Give controller requested information to demonstrate processor's compliance with law ○ Cooperate with controller assessments or share independent assessments of its own services ○ Require all subcontractors (if any) to comply with processor's obligations related to personal data via written contract ❖ Processor may <u>not</u>: §9607(4) p.14 • Process personal data beyond directions in contract with controller (otherwise, it assumes all responsibilities and liabilities of a controller under LD 1088)	○ Delete or return personal data at end of processing activity, unless retention required by law ○ Give controller requested information to demonstrate processor's compliance with law ○ Cooperate with controller assessments or share independent assessments of its own services ○ Require all subcontractors (if any) to comply with processor's obligations related to personal data via written contract ❖ Processor may <u>not</u>: §9607(4) p.12 • Process personal data beyond directions in contract with controller (otherwise, it assumes all responsibilities and liabilities of a controller under LD 1224)	○ Delete or return personal data at end of processing activity, unless retention required by law ○ Give controller requested information to demonstrate processor's compliance with law ○ Cooperate with controller assessments or conduct independent assessments of its own services ○ After giving controller opportunity to object to use of subcontractor, require all subcontractors (if any) to comply with processor's obligations related to personal data via written contract ○ Establish and implement reasonable data security practices for data confidentiality and integrity ○ Stop processing data on request of controller in response to consumer's authenticated request ❖ Processor may <u>not</u>: §9607(4) p.16-17 • Process personal data beyond directions in contract with controller (otherwise, it assumes all responsibilities and liabilities of a controller under LD 1822)
Third-party responsibilities	n/a	n/a	❖ Third party that receives personal data must: §9610 p.17 • Notify consumer if it intends to use or share the data in a manner inconsistent with disclosures made at the time the data was collected — with enough time to permit the consumer to exercise the consumer's rights
Duties involving de-identified data	❖ Controller in possession of de-identified data must: • Take reasonable measures to prevent re-identifying data • Publicly commit to not attempting to re-identify data §9609(4) p.15 Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations	❖ Controller in possession of de-identified data must: • Take reasonable measures to prevent re-identifying data • Publicly commit to not attempting to re-identify data §9609(4) p.14 Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations	❖ Controller in possession of de-identified data must: • Contractually obligate recipients of the de-identified data to comply with this law & exercise reasonable oversight, including taking steps to address violations — whether the steps are reasonable depends in part on whether the data would be sensitive data if re-identified §9612 p.19
Additional Consumer health data Requirements	n/a	n/a	❖ Person may not provide employee or contractor with access to consumer health data unless: • Employer or contractor is subject to contractual or statutory duty of confidentiality; or • Confidentiality is a condition of employment ❖ Person may not provide processor with access to consumer health data unless the person requires the processor to protect the data via the processing contract described above

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
"Small business" exception <u>LD 1088</u> §9603(1-2) p. 6 <u>LD 1224</u> §9603(1-2) p. 5 <u>LD 1822</u> §9603 p. 6	From July 1, 2026, to December 31, 2027: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥100,000 Maine residents (except solely for purposes of payment transactions) or ○ Of ≥25,000 Maine residents and derived >25% of gross revenue from the sale of personal data Beginning January 1, 2028: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥50,000 Maine residents (except solely for purposes of payment transactions) or ○ Of ≥25,000 Maine residents and derived > 25% of gross revenue from the sale of personal data	From July 1, 2026, to December 31, 2027: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥100,000 Maine residents (except solely for purposes of payment transactions) or ○ Of ≥25,000 Maine residents and derived >25% of gross revenue from the sale of personal data Beginning January 1, 2028: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥50,000 Maine residents (except solely for purposes of payment transactions) or ○ Of ≥25,000 Maine residents and derived > 25% of gross revenue from the sale of personal data	Beginning July 1, 2026: ❖ Law only applies to persons that: • Conduct business in Maine or target Maine residents & • Last calendar year, controlled/processed personal data: ○ Of ≥35,000 Maine residents (except solely for purposes of payment transactions) or ○ Of ≥10,000 Maine residents and derived >20% of gross revenue from the sale of personal data
Exempt entities <u>LD 1088</u> §9603(3) p. 6 <u>LD 1224</u> §9603(3) p. 5 <u>LD 1822</u> §9604(1) p. 7	❖ Law not applicable to (types of entities): • State or its political subdivisions or boards or agencies; • Federally recognized Indian tribes in the State; • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA) • Financial institution, affiliate or "service corporation" (defined in Title 9-B) subject to the federal Gramm-Leach-Bliley Act — only if it is directly and solely engaged in financial activities described in GLBA • A "licensee" under Maine's insurance laws — to the extent it is complying with any applicable data security and privacy requirements in Maine insurance law	❖ Law not applicable to (types of entities): • State or its political subdivisions or boards or agencies; • Federally recognized Indian tribes in the State; • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA) • Financial institution, affiliate or "service corporation" (defined in Title 9-B) subject to the federal Gramm-Leach-Bliley Act • A "licensee" under Maine's insurance laws — to the extent it is complying with any applicable data security and privacy requirements in Maine insurance law • A nonprofit organization established to detect and prevent fraudulent acts in connection with insurance (NICB)	❖ Law not applicable to (types of entities): • State or its political subdivisions or boards or agencies; • Federally recognized Indian tribes in the State; • Nonprofit corporation (501(c)(3), (4), (6), and (12)); • Institution of higher education; • National securities associations registered under the federal Securities Exchange Act of 1934 (ex: FINRA); • A supervised financial organization or service corp. (defined in Title 9-A & 9-B of Maine banking laws); • A health care facility or practitioner (as defined in state law) or affiliate that qualifies as a business associate serving only covered entities under HIPAA; • A "licensee" under Maine's insurance laws — to the extent it is complying with any applicable data security and privacy requirements in Maine insurance law • An ISP covered by 35-A M.R.S. §9301 — but only to the extent it is providing ISP services
Exempt data	❖ Law not applicable to (types of data): §9603(4) p. 7 • Data regulated by GLBA if it is collected, processed, sold or disclosed in accordance with the GLBA	❖ Law not applicable to (types of data): §9603(4) p. 7 • Data regulated by GLBA if it is collected, processed, sold or disclosed in accordance with the GLBA	❖ Law not applicable to (types of data): §9604(2) p. 7 • Data regulated by GLBA if it is collected, processed, sold or disclosed in accordance with the GLBA

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	- HIPAA: (a) “protected health information” (b) info. de-identified in accordance with HIPAA; and (c) info. for public health activities as authorized by HIPAA - Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) - Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines - Information intermingled with certain health info. listed above held by HIPAA-regulated entities and protected in accordance with HIPAA or 42 USC §290dd-2 - Info. created for purposes of or info. regulated by: - Health Care Quality Improvement Act of 1986 - Family Educational Rights and Privacy Act of 1974 - Airline Deregulation Act of 1978 - Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: - Fair Credit Reporting Act - Driver’s Privacy Protection Act of 1994 - Farm Credit Act of 1971 - Information of those applying to or employed by a controller, processor or third party to administer benefits to these employees and their relatives	- HIPAA: (a) “protected health information”(b) info. de-identified in accordance with HIPAA; and (c) info. for public health activities as authorized by HIPAA - Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) - Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines - Information intermingled with certain health info. listed above held by HIPAA-regulated entities and protected in accordance with HIPAA or 42 USC §290dd-2 - Health care information defined in 22 M.R.S. §1711-C Info. created for purposes of or regulated by: - Health Care Quality Improvement Act of 1986 - Family Educational Rights and Privacy Act of 1974 - Airline Deregulation Act of 1978 - Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: - Fair Credit Reporting Act - Driver’s Privacy Protection Act of 1994 - Farm Credit Act of 1971 - Information of those applying to or employed by a controller, processor or third party to administer benefits to these employees and their relatives	- HIPAA: (a) “protected health information” (b) info. de-identified in accordance with HIPAA; and (c) info. for public health activities as authorized by HIPAA - Patient-identifying info. related to substance-use disorder treatment (under 42 USC §290dd-2) - Identifiable information collected as part of human subject research conducted under certain federal laws or international guidelines - Information intermingled with certain health info. listed above held by HIPAA-regulated entities and protected in accordance with HIPAA or 42 USC §290dd-2 - Info. created for purposes of or regulated by: - Health Care Quality Improvement Act of 1986 - Family Educational Rights and Privacy Act of 1974 - Airline Deregulation Act of 1978 - Info. created, collected, processed, sold or disclosed in compliance with the following federal laws: - Fair Credit Reporting Act - Driver’s Privacy Protection Act of 1994 - Farm Credit Act of 1971 - Information of those applying to or employed by a controller, processor or third party to administer benefits to these employees and their relatives
Exempt activities <u>LD 1088</u> §9A-11 (1-2) p.16-17 <u>LD 1224</u> §9A-10 (1-2) p.14-15 <u>LD 1822</u> §9A-13 (1-2) p.19-20	❖ Controller / Processor activities <u>not</u> affected by LD 1088: - Complying with federal or Maine laws or rules - Complying with investigations, subpoenas or summonses by federal, Maine or tribal authorities - Cooperating with federal, Maine or tribal law enforcement concerning conduct the entity believes in good faith may violate federal or Maine laws or rules - Investigating, exercising or defending legal claims - Providing product or service requested by consumer, including performing contracted services (ex: warranty) - Taking requested steps prior to entering a contract - Taking immediate steps to protect life or physical safety of a consumer or other individual	❖ Controller / Processor activities <u>not</u> affected by LD 1224: - Complying with federal, any state or local laws - Complying with investigations, subpoenas or summonses by federal, any state or tribal authorities - Cooperating with federal, state or tribal law enforcement conduct the entity believes in good faith may violate federal or state laws or rules - Investigating, exercising or defending legal claims - Providing product or service requested by consumer, including performing contracted services (ex: warranty) - Taking requested steps prior to entering a contract - Taking immediate steps to protect the life or physical safety of a consumer or other individual	❖ Controller / Processor activities <u>not</u> affected by LD 1224: - Complying with federal, Maine or local laws or rules - Complying with investigations, subpoenas or summonses by federal, Maine or tribal authorities - Cooperating with federal, Maine or tribal law enforce. concerning conduct the entity believes in good faith may violate federal, Maine or local laws or rules - Investigating, exercising or defending legal claims - Providing product or service requested by consumer, including performing contracted services (ex: warranty) - Taking requested steps prior to entering a contract - Taking immediate steps to the life or physical safety of a consumer or other individual

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
	- Preventing or responding to security incidents, identity theft, fraud, harassment, deceptive or illegal activity, system integrity or reporting those incidents - Engaging in scientific or statistical research in the public interest that adheres to all other ethics and privacy laws and is overseen by an Institutional Review Board (IRB) - Assisting another controller, processor or 3rd party with its compliance with this law - Process personal data for public health purposes subject to confidentiality obligations of federal or state laws - Collection, use or retention of data for internal use: - Internal R&D to improve or repair products, - Product recalls, - Identifying and repairing technical errors, and - Internal operations reasonably aligned with expectations of the consumer or compatible with processing data to provide a product or service specifically requested by the consumer	- Preventing or responding to security incidents, identity theft, fraud, harassment, deceptive or illegal activity, system integrity or reporting those incidents - Engaging in scientific or statistical research in the public interest that adheres to all other ethics and privacy laws and is overseen by an IRB - Assisting another controller, processor or 3rd party with its compliance with this law - Process personal data for public health purposes subject to confidentiality obligations of federal or state laws - Collection, use or retention of data for internal use: - Internal R&D to improve/repair products, - Product recalls, - Identifying and repairing technical errors, and - Internal operations reasonably aligned with expectations of the consumer or compatible with processing data to provide a product or service specifically requested by the consumer	- Preventing or responding to security incidents, identity theft, fraud, harassment, deceptive or illegal activity, system integrity or reporting those incidents (<i>slightly different wording from LD 1088 and LD 1224</i>) - Assisting another controller, processor or 3rd party with its compliance with this law - Collection, use or retention of data for internal use: - Product recalls, - Identifying and repairing technical errors, and - Internal operations reasonably aligned with expectations of the consumer or compatible with processing data to provide a product or service specifically requested by the consumer
Remedies for violations LD 1088 § 9612 p.18-19 LD 1224 § 9611 p.17 LD 1822 § 9614 p.21-22	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: Must provide at least 30-days advance notice and opportunity to confer with AG's Office — unless show facts in affidavit demonstrating immediate irreparable harm to consumers in the State if notice is given ❖ No private right of action ❖ No AG rulemaking authority under UTPA to interpret law	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: - Must provide at least 30-days advance notice - AG may not bring action unless controller fails to cure an alleged violation listed in the notice within 30 days ❖ No private right of action ❖ No AG rulemaking authority under UTPA to interpret law	❖ Attorney General may bring an action under Unfair Trade Practices Act (UTPA) against anyone who violates this law: Until April 1, 2027, if AG believes it is possible for a controller or processor to cure a violation, may choose to give notice of the violation prior to initiating suit - If notice is given, AG may not bring action unless violation is not cured within 60 days - Factors regarding whether to give notice: number of violations, size and complexity of defendant, nature and extent of defendant's processing activities, likelihood of injury to public, degree to which violations affect safety, whether the alleged violation was likely a human or technical error, and past violations by defendant of this or similar laws ❖ No private right of action ❖ AG rulemaking authority under UTPA to interpret law

Detailed comparison of Comprehensive Data Privacy Proposals — LD 1088 (Henderson), LD 1224 (Roberts) and LD 1822 (Kuhn)

	LD 1088 (Henderson)	LD 1224 (Roberts)	LD 1822 (Kuhn)
Other exemptions	❖ Law does not / may not be construed to: §9611(3.5) p. 17 - Apply if compliance requires violation of an evidentiary privilege under Maine law - Apply to processing of personal data by person purely for own household use - Impose an obligation that adversely affects rights of freedom of speech or of the press (including state law on confidentiality of journalist's confidential sources)	❖ Law does not / may not be construed to: §9610(3.5) p. 16 - Apply if compliance requires violation of an evidentiary privilege under Maine law - Apply to processing of personal data by person purely for own household use - Impose an obligation that adversely affects rights of freedom of speech or of the press (including state law on confidentiality of journalist's sources)	❖ Law does not / may not be construed to: §9613(3.5) p. 20 - Apply if compliance requires violation of an evidentiary privilege under state law - Apply to processing of personal data by person purely for own household use - Impose an obligation that adversely affects the rights or freedoms of any person, including freedom of speech or of the press or freedom to engage in political activity
Exceptions to liability	❖ Exceptions to liability: §9611(4) p. 18 - Controller not liable if processor or 3rd party violates law absent actual knowledge that it would do so - Processor/3rd party not liable for controller's violations	❖ Exceptions to liability: §9610(4) p. 16 - Controller not liable if processor or 3rd party violates law absent actual knowledge that it would do so - Processor/3rd party not liable for controller's violations	❖ Exceptions to liability: §9613(4) p. 20 - Controller not liable if both (1) processor or 3rd party violates law absent actual knowledge that it would do so <u>and</u> (2) controller has remained in compliance with law - Processor/3rd party not liable for controller's violations
Maine Privacy Fund 1088 - §9613 p. 19 1224 - §9612 p. 17	❖ Establishes nonlapsing Maine Privacy Fund consisting of: - All monetary penalties, attorneys fees or costs - Any appropriations, donations and interest earned ❖ Uses: funds must be used to provide funding for the staff and activities necessary to the Attorney General under this law	❖ Establishes nonlapsing Maine Privacy Fund consisting of: - All monetary penalties, attorneys fees or costs - Any appropriations, donations and interest earned ❖ Uses: funds must be used to provide funding for the staff and activities necessary to the Attorney General under this law	Does not establish a Maine Privacy Fund
Effect on current Maine ISP Law	❖ Repeals 35-A M.R.S. §9301, which generally requires Internet Service Providers (ISPs) to obtain consent before using, disclosing or selling a customer's personally identifying info. p. 19	Does not repeal ISP law	Does not repeal ISP law (but exempts ISPs to extent they are acting solely as ISPs)
Preemption of local laws	n/a	❖ Law preempts any ordinance or other regulation adopted by a political subdivision of the State re: processing (includes collection) of personal data by controllers/processors §9611(4) p. 17	n/a
Effective Date	July 1, 2026 p. 20	July 1, 2026 p. 18	July 1, 2026 p. 22
Reporting Requirement	❖ Attorney General must submit report by January 1, 2028, to the Judiciary Committee containing: - Data on number of 30-day notices of violation sent; nature of the alleged violations; number that conferred with OAG to prevent enforcement action; number of civil actions brought to enforce the law - Any recommendations for improving the law Committee may report out legislation in 133rd Legislature (R2)	❖ Attorney General must submit report by February 1, 2027, to the Judiciary Committee containing: - Data on number of notices of violation sent; nature of the alleged violations; number that conferred with OAG to prevent enforcement action; number of civil actions brought to enforce the law - Any recommendations for improving the law Committee may report out legislation in 133rd Legislature (R1)	❖ Attorney General must submit report by February 1, 2027, to the Judiciary Committee containing: - Data on number of notices of violation sent; nature of the alleged violations; number that conferred with OAG to prevent enforcement action; number of civil actions brought to enforce the law - Any recommendations for improving the law Committee may report out legislation in 133rd Legislature (R1)