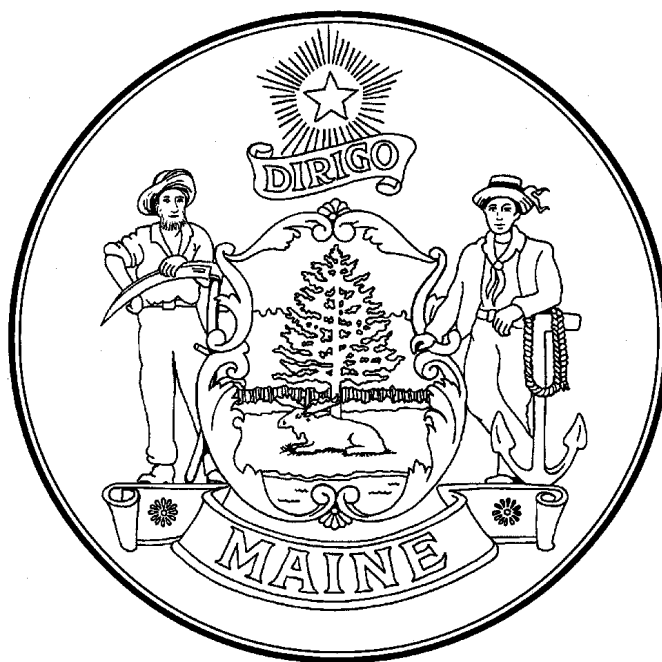


MAINE STATE LEGISLATURE

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)

**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.

LD 1088

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



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. 1088 - 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 1088. 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

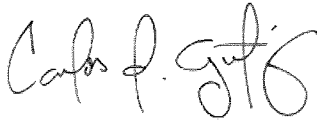
To avoid potential conflict with already existing federal law, CHPA recommends the following amendment to LD 1088 on page 8, line 9 as item (Q):

(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

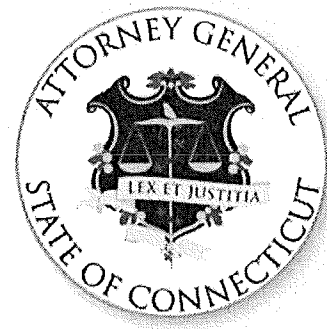
CHPA and its members are deeply committed to protecting our customers' privacy and data security. While we appreciate your focus on this important issue, the current version of this bill raises significant concerns. We remain open to constructive dialogue and collaboration to develop a more balanced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

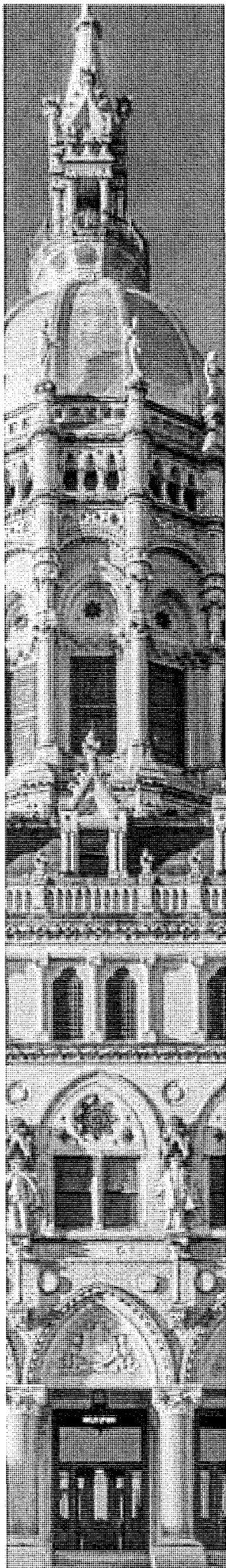
Carlos I. Gutiérrez
Vice President, State & Local Government Affairs
Consumer Healthcare Products Association
Washington, D.C.
cgutierrez@chpa.org | 202-429-3521

Cc: Member of the Joint Standing Committee on Judiciary

A black and white photograph of the Connecticut State Capitol building, showing its ornate architecture, including a tall steeple and classical columns with statues.

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.

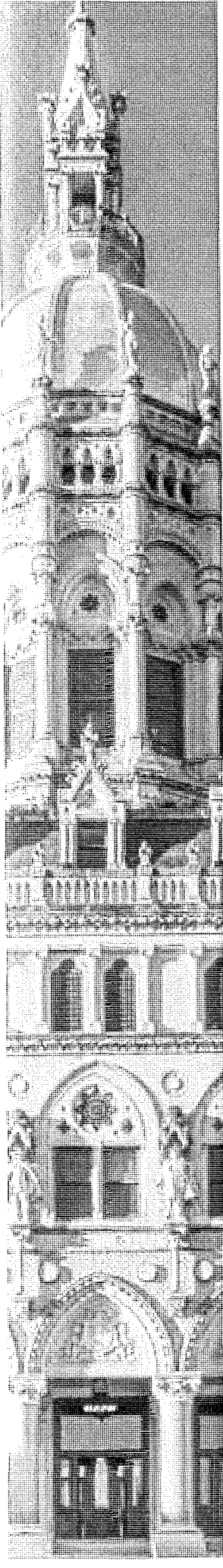
Breach Notice Review

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.

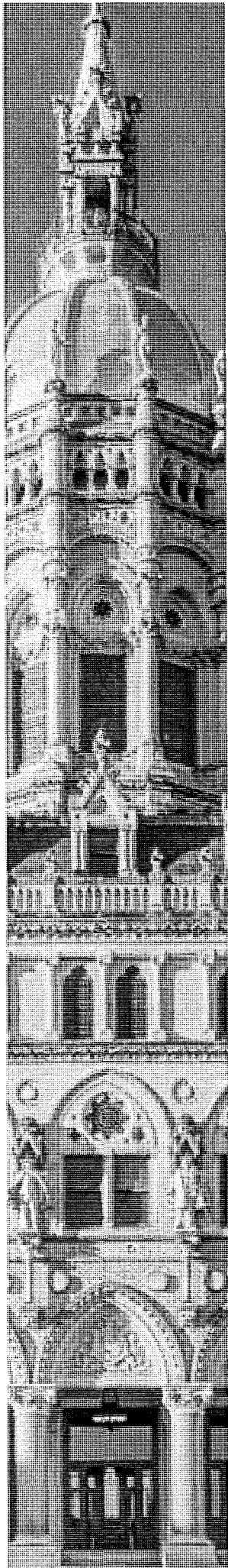
Most recently, we have updated our CTDPA FAQ page to highlight the Act’s consumer health data, minors’ privacy, and the universal opt-out provisions. We have also developed additional resources for consumers to learn how to send their opt-out preference signal (“OOPS”), and for businesses seeking to 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/ T-Mobile, 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-requirements>.



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

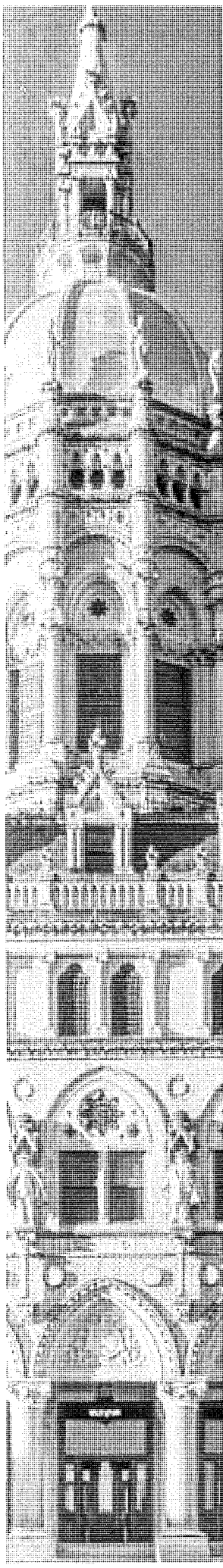
While many of the matters highlighted in our Initial Report remain ongoing, including investigations related to genetic information, geolocation data, and minors' data, we wanted to take this opportunity to highlight several key takeaways from our early enforcement efforts that we hope will provide insight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

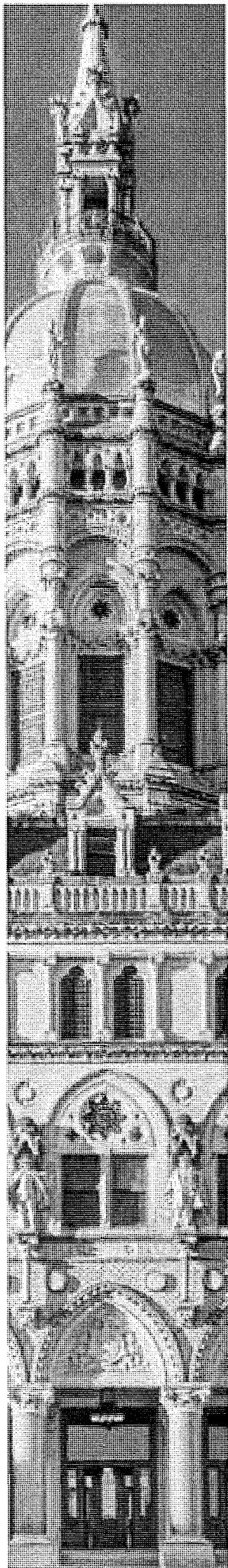
By its nature, FRT involves the collection, use, and sometimes sharing of consumers' biometric information. The CTDPA defines sensitive data to expressly include biometric data⁸ and appropriately sets forth heightened protections for such data. While the CTDPA contains a so-called crime/fraud exception, 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(i).



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 CUIBPA.



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

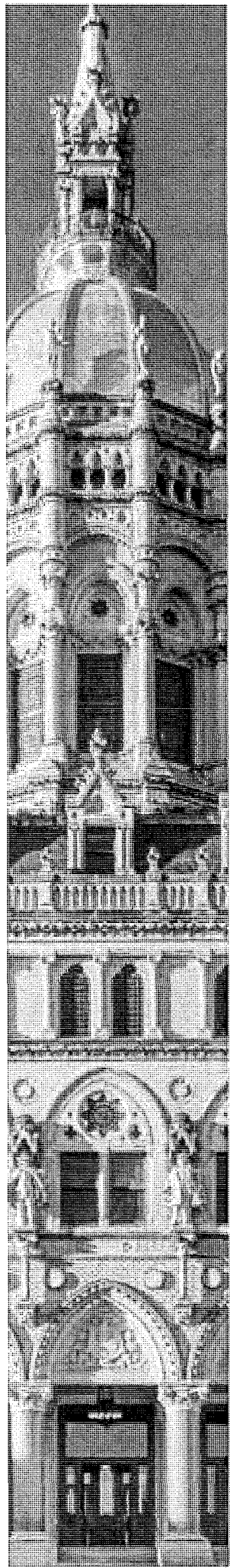
As noted in our Initial Report, the OAG sent a cure notice, as well as broader inquiries, to a large car manufacturer after public reports raised concerns that connected vehicles were collecting and sharing a range of highly personal data about consumers. As a result of our cure notice, the company quickly 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.

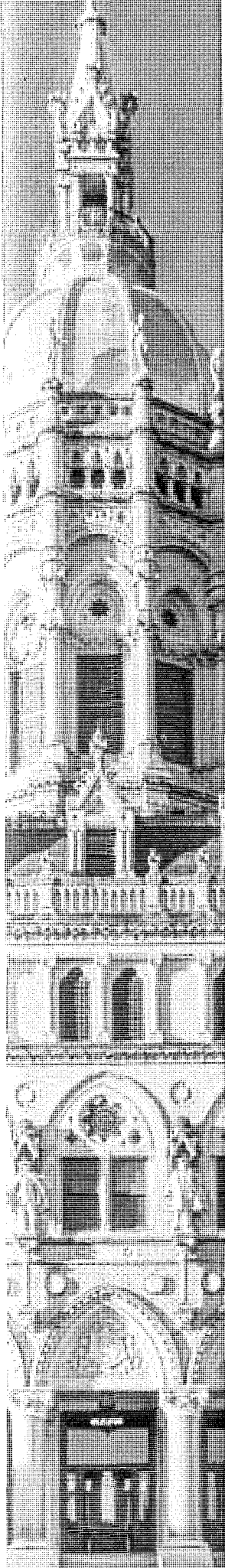
To comply with the CTDPA, companies that utilize cookie banners that provide consumers with the option to accept all cookies, should also offer a symmetrical option to reject all cookies. Both options should be displayed on the screen at the same time, and in the same color, font, and size. Whenever 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.

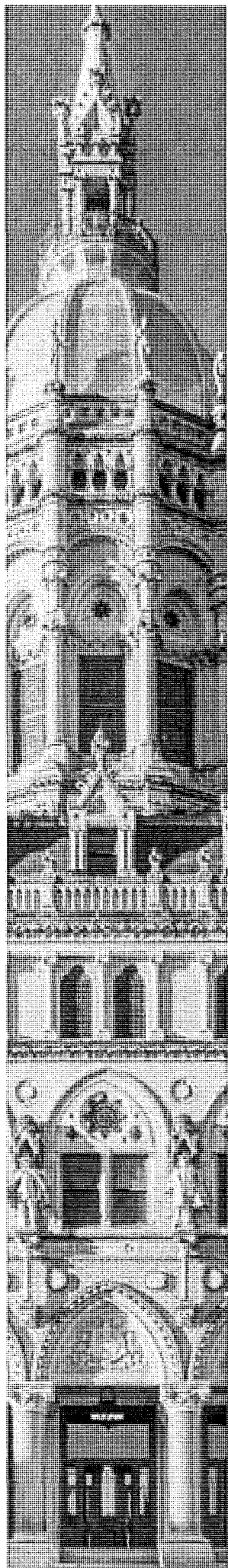
[22] Conn. Gen. Stat. §§ 42-515(9)(38), 42-520(a)(4).

[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

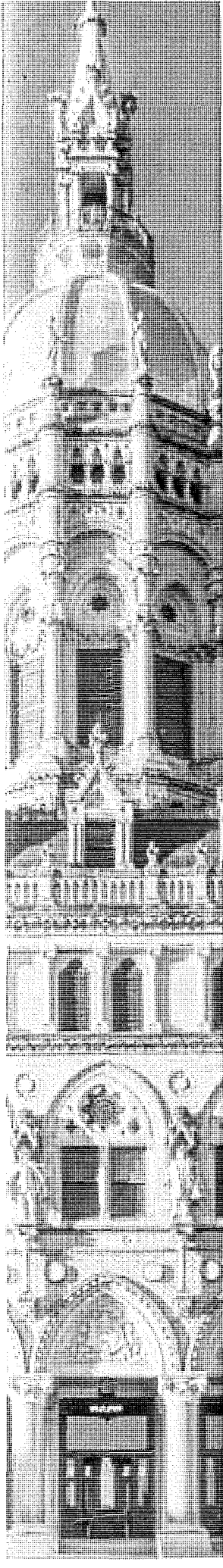
We strongly urge the legislature to scale back exemptions in the CTDPA. First, the legislature should omit entity-level exemptions for GLBA (Gramm-Leach-Bliley-Act)- and HIPAA-covered entities. Various states have now passed laws without these exemptions— the CTDPA's wholesale carveouts not only put 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.

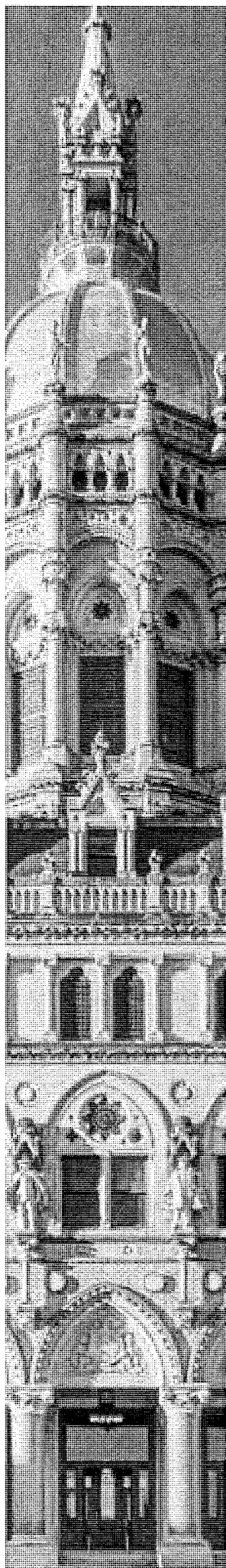
Strengthen Data Minimization Provisions

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.

**MAINE COMMUNITY COLLEGE SYSTEM
UNIVERSITY OF MAINE SYSTEM**

**MEMORANDUM TO
JOINT STANDING COMMITTEE ON JUDICIARY**

TO: The Honorable Anne Carney, Senate Chair; The Honorable Amy Kuhn, House Chair
Joint Standing Committee on Judiciary

FROM: William Fletcher, General Counsel, Maine Community College System on behalf of
the Maine Community College System and the University of Maine System

RE: L.D. 1224, *An Act to Comprehensively Protect Consumer Privacy*
L.D. 1088, *An Act to Enact the Maine Consumer Privacy Act*

DATE: May 5, 2025

Senator Carney, Representative Kuhn, and Members of the Joint Standing Committee on Judiciary, please accept this memorandum on behalf of the Maine Community College System ("MCCS") and the University of Maine System ("UMS") regarding L.D. 1224, *An Act to Comprehensively Protect Consumer Privacy* and L.D. 1088, *An Act to Enact the Maine Consumer Privacy Act*.

As public postsecondary education institutions, we appreciate the intent of this bill and recognize the importance of data privacy. MCCS and UMS already maintain data privacy and safeguarding of personal data, consistent with a robust set of existing federal laws and regulations, and we are committed to doing all that we can to protect the privacy of the data of the students we serve, our faculty, and staff. However, we believe adding another regulatory framework over the existing layers of federal law and regulation will complicate and undermine our ability to serve our students.

Therefore, we respectfully request that this Committee expressly exempt Maine's public postsecondary institutions from the applicability of LD 1224 and LD 1088, just as many other states with data privacy laws have provided exemptions to their institutions of higher education, and as provided for in LD 1822.

Thank you for your consideration. Should you have any questions, please contact Becky Smith, Director of Government and Community Relations for the Maine Community College System at **bsmith@mainecc.edu** or (207) 629-4015.

132nd Maine Legislature
An Act to Enact the Maine Online Data Privacy Act
L.D. 1088

Amend LD 1088 Section 9603 to add a new section 1903(3)(E) as follows:

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

Summary

LD 1088 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/manufacture 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



**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 ages 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.

Amend the bill by striking out everything after the enacting clause and before the summary and inserting in its place the following:

Note: This amendment is based on the language of LD 1224, with changes to LD 1224 shown highlighted.

Sec. 1. 10 MRSA c. 1057 is enacted to read:

CHAPTER 1057

MAINE CONSUMER DATA PRIVACY ACT

§9601. Short title

This chapter may be known and cited as "the Maine Consumer Data Privacy Act."

§9602. Definitions

As used in this chapter, unless the context otherwise indicates, the following terms have the following meanings.

1. Affiliate. "Affiliate" means a business or nonprofit organization that shares common branding with another business or nonprofit organization or controls, is controlled by or is under common control with another business or nonprofit organization.

2. Biometric data. "Biometric data" means data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, retina, iris or other unique biological pattern or characteristic that is used to identify a specific individual. "Biometric data" does not include:

A. A digital or physical photograph;

B. An audio or video recording;

C. Any data generated from a digital or physical photograph or an audio or video recording, unless the data is generated to identify a specific individual; or

D. Data collected, used or stored for health care treatment, payment or operations under the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and exemptions adopted pursuant to that Act.

3. Business associate. "Business associate" has the same meaning as in 45 Code of Federal Regulations, Section 160.103.

4. Child. "Child" means an individual who has not attained 13 years of age.

5. Consent. "Consent" means a clear affirmative act signifying a consumer's freely given, specific, informed and unambiguous agreement to allow the processing of personal data relating to the consumer. "Consent" may include a written statement, including by electronic means, that is made in the language that the consumer uses to obtain a product or service from the controller and in a format that is reasonably accessible to and usable by consumers with disabilities or any other unambiguous affirmative act. "Consent" does not include:

A. Acceptance of a terms of use document or similar document that contains descriptions of personal data processing along with other unrelated information;

B. Hovering over, muting, pausing or closing a given piece of content; or

C. Agreement obtained through the use of a dark pattern.

6. Consumer. "Consumer" means an individual who is a resident of this State. "Consumer" does not include an individual acting in a commercial or employment context or as an employee, owner, director, officer or contractor of a company, partnership, sole proprietorship, nonprofit organization or government agency whose

communications or transactions with the controller occur solely within the context of that individual's role with the company, partnership, sole proprietorship, nonprofit organization or government agency.

7. Control. "Control" means:

A. Ownership of, or the power to vote, more than 50% of the outstanding shares of any class of voting security of a company;

B. Control in any manner over the election of a majority of the directors of a company or of individuals exercising similar functions in a company; or

C. Power to exercise controlling influence over the management of a company.

8. Controller. "Controller" means a person that, alone or jointly with other persons, determines the purpose and means of processing personal data.

9. COPPA. "COPPA" means the federal Children's Online Privacy Protection Act of 1998, 15 United States Code, Section 6501 et seq. and the regulations, rules, guidance and exemptions adopted pursuant to that Act, as that Act and such regulations, rules, guidance and exemptions may be amended from time to time.

10. Covered entity. "Covered entity" has the same meaning as in 45 Code of Federal Regulations, Section 160.103.

11. Dark pattern. "Dark pattern" means a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making or choice and includes, but is not limited to, any practice the Federal Trade Commission refers to as a dark pattern.

12. Decisions that produce legal or similarly significant effects concerning the consumer. "Decisions that produce legal or similarly significant effects concerning the consumer" means decisions that result in the provision or denial to the consumer of financial or lending services, housing, insurance, education enrollment or opportunity, criminal justice, employment opportunities, health care services or access to essential goods or services.

13. De-identified data. "De-identified data" means data that cannot reasonably be used to infer information about or otherwise be linked to an identified or identifiable individual, or a device linked to an individual, if the controller that possesses the data:

A. Takes reasonable measures to ensure that the de-identified data cannot be associated with an individual;

B. Publicly commits to process the de-identified data only in a de-identified fashion and not attempt to re-identify the data; and

C. Contractually obligates recipients of the de-identified data to satisfy the criteria set forth in paragraphs A and B.

14. Federally recognized Indian tribe in this State. "Federally recognized Indian tribe in this State" means the Houlton Band of Maliseet Indians, the Mi'kmaq Nation, the Passamaquoddy Tribe or the Penobscot Nation when the band, nation or tribe is acting in a governmental capacity and not in a business capacity. "Federal recognized Indian tribe in this State" does not include a business entity, including any federally chartered tribal corporation or other business entity owned or partly owned by the Houlton Band of Maliseet Indians, the Mi'kmaq Nation, the Passamaquoddy Tribe or the Penobscot Nation.

15. Nonprofit organization. "Nonprofit organization" means an organization that is exempt from taxation under Section 501(c)(3), Section 501(c)(4), Section 501(c)(6) or Section 501(c)(12) of the United States Internal Revenue Code of 1986, as amended.

16. Personal data. "Personal data" means information that is linked or reasonably linkable to an identified or identifiable individual consumer or that is linked or reasonably can be linked to a device that is linked or reasonably can be linked to an identified or identifiable consumer. "Personal data" does not include de-identified data or publicly available information.

17. Precise geolocation data. "Precise geolocation data" means information derived from technology, including, but not limited to, global positioning system level latitude and longitude coordinates, that directly identifies the specific location of an individual with precision and accuracy within a radius of 1,750 feet. "Precise geolocation data" does not include:

- A. The content of communications; or
- B. Data generated by or connected to advanced utility metering infrastructure systems or equipment for use by a utility.

18. Process. "Process" means an operation or set of operations performed on personal data, including the collection, use, storage, disclosure, analysis, deletion or modification of personal data.

19. Processor. "Processor" means a person that processes personal data on behalf of a controller.

20. Profiling. "Profiling" means any form of solely automated process performed on personal data to evaluate, analyze or predict personal aspects related to an identified or identifiable individual's economic situation, health, personal preferences, interests, reliability, behavior, location or movements.

21. Protected health information. "Protected health information" has the same meaning as in the regulations, rules, guidance and exemptions adopted pursuant to the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C.

22. Pseudonymous data. "Pseudonymous data" means personal data that cannot be attributed to a specific individual without the use of additional information, as long as the additional information is kept separately from the personal data and is subject to appropriate technical and organizational measures to ensure that the personal data is not attributed to an identified or identifiable individual.

23. Publicly available information. "Publicly available information" means information that:

- A. Is lawfully made available to the general public through federal, state or local government records; or
- B. Is lawfully made available to the general public through widely distributed media.

24. Sale of personal data. "Sale of personal data" means the exchange of personal data for monetary or other valuable consideration by the controller to a 3rd party. "Sale of personal data" does not include:

- A. The disclosure of personal data to a processor that processes the personal data on behalf of the controller;
- B. The disclosure of personal data to a 3rd party for purposes of providing a product or service requested by the consumer;
- C. The disclosure or transfer of personal data to an affiliate of the controller;
- D. The disclosure of personal data when the consumer directs the controller to disclose the personal data or intentionally uses the controller to interact with a 3rd party;
- E. The disclosure of personal data that the consumer:
 - (1) Intentionally made available to the general public via a channel of mass media; and
 - (2) Did not restrict to a specific audience; or

F. The disclosure or transfer of personal data to a 3rd party as an asset that is part of a merger, acquisition, bankruptcy or other transaction, or a proposed merger, acquisition, bankruptcy or other transaction, in which the 3rd party assumes control of all or part of the controller's assets.

25. Sensitive data. "Sensitive data" means personal data that includes:

- A. Data revealing racial or ethnic origins, religious beliefs, medical history, mental or physical health conditions, or diagnoses made by a medical professional, sexual orientation or citizenship or immigration status;
- B. The processing of genetic Genetic or biometric data for purposes of uniquely identifying an individual;

C. Personal data collected from a consumer known to be a child;

D. Precise geolocation data; ~~or~~

E. A social security number, driver's license number or nondriver identification card number, except that "sensitive data" does not include the last 4 digits of a social security number, driver's license number or nondriver identification card number;

F. A consumer's account number, log-in information, financial account number or credit or debit card number that, in combination with any required security code, access code or password, permits access to a consumer's financial account; or

~~G~~ E. Data concerning an individual's status as a victim of a crime. For the purposes of this paragraph, "victim" has the same meaning as in Title 17-A, section 2101, subsection 2.

26. Targeted advertising. "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.

27. Trade secret. "Trade secret" has the same meaning as in section 1542, subsection 4.

§9603. Scope

1. Applicability; July 1, 2026 to December 31, 2027. From July 1, 2026 to December 31, 2027, the provisions of this chapter apply to persons that conduct business in this State or persons that produce products or services that are targeted to residents of this State and that during the preceding calendar year:

A. Controlled or processed the personal data of not less than 100,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

B. Controlled or processed the personal data of not less than 25,000 consumers and derived more than 25% of gross revenue from the sale of personal data.

2. Applicability; beginning January 1, 2028. Beginning January 1, 2028, the provisions of this chapter apply to persons that conduct business in this State or persons that produce products or services that are targeted to residents of this State and that during the preceding calendar year:

A. Controlled or processed the personal data of not less than 50,000 consumers, excluding personal data controlled or processed solely for the purpose of completing a payment transaction; or

B. Controlled or processed the personal data of not less than 25,000 consumers and derived more than 25% of gross revenue from the sale of personal data.

3. Exempt entities. The provisions of this chapter do not apply to:

A. A body, authority, board, bureau, commission, district or agency of this State, a political subdivision of this State or a federally recognized Indian tribe in this State;

B. A national securities association that is registered under the federal Securities Exchange Act of 1934, 15 United States Code, Section 78a et seq.;

C. A financial institution or affiliate of a financial institution, including a service corporation, that is subject to Title V of the federal Gramm-Leach-Bliley Act, 15 United States Code, Section 6801 et seq. (1999), as amended;

D. A person or entity that qualifies as a licensee under Title 24-A, section 2263, subsection 8, to the extent the person or entity is in compliance with any applicable data security and data privacy requirements of Title 24-A; or

E. A nonprofit organization ~~that: that is established to detect and prevent fraudulent acts in connection with insurance;~~

(1) Does not receive any revenue from the sale of personal data; or

(2) A nonprofit organization that is established to detect and prevent fraudulent actions in connection with insurance; or

F. A person or entity that is a motor vehicle dealer franchisee under Title 10, section 1171, subsection 7.

4. Exempt data. The provisions of this chapter do not apply to:

A. Nonpublic personal information regulated under and collected, processed, sold or disclosed in accordance with the requirements of the federal Gramm-Leach-Bliley Act, 15 United States Code, Section 6801 et seq. (1999), as amended;

B. Health care information as defined in Title 22, section 1711-C, subsection 1, paragraph E;

C. Protected health information under the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

D. Patient-identifying information as described in 42 United States Code, Section 290dd-2;

E. Identifiable private information for the protection of human subjects in research under 45 Code of Federal Regulations, Part 46;

F. Identifiable private information that is otherwise information collected as part of human subjects in research pursuant to the good clinical practice guidelines issued by the International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use or successor organization;

G. The protection of human subjects in research under 21 Code of Federal Regulations, Parts 50 and 56, or personal data used or shared in research, as defined in 45 Code of Federal Regulations, Section 164.501, that is conducted in accordance with the standards set forth in paragraphs E and F, or other research conducted in accordance with applicable law;

H. Information and documents created for purposes of the federal Health Care Quality Improvement Act of 1986, 42 United States Code, Section 11101 et seq;

I. Information derived from health care-related information listed in this subsection that is de-identified in accordance with the requirements for de-identification pursuant to the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

J. Information that originates from information described in paragraphs C to I, or information that is intermingled so as to be indistinguishable from information described in paragraphs C to I, that a covered entity, business associate or program or activity relating to substance use disorder as described in 42 United States Code, Section 290dd-2, creates, processes or maintains in the same manner as is required under the applicable laws and regulations cited in paragraphs C to I;

K. Information used for public health activities and purposes as authorized by the federal Health Insurance Portability and Accountability Act of 1996, 42 United States Code, Chapter 7, Subchapter XI, Part C, and the regulations, rules, guidance and exemptions adopted pursuant to that Act;

L. The collection, maintenance, disclosure, sale, communication or use of personal information bearing on a consumer's creditworthiness, credit standing, credit capacity, character, general reputation, personal characteristics or mode of living by a consumer reporting agency, furnisher or user that provides information for use in a consumer report, and by a user of a consumer report, but only to the extent that such activity is regulated by and authorized under the federal Fair Credit Reporting Act, 15 United States Code, Section 1681 et seq.;

M. Personal data collected, processed, sold or disclosed in compliance with the federal Driver's Privacy Protection Act of 1994, 18 United States Code, Section 2721 et seq.;

N. Personal data regulated by the federal Family Educational Rights and Privacy Act of 1974, 20 United States Code, Section 1232g;

O. Personal data collected, processed, sold or disclosed in compliance with the federal Farm Credit Act of 1971, 12 United States Code, Section 2001 et seq.;

P. Data processed or maintained:

(1) In the course of an individual applying to, employed by or acting as an agent or independent contractor of a controller, processor or 3rd party, to the extent that the data is collected and used within the context of that role;

(2) As the emergency contact information of an individual under this chapter used for emergency contact purposes; or

(3) That is necessary to retain to administer benefits for another individual relating to the individual who is the subject of the information under subparagraph (1) and used for the purposes of administering those benefits; or

Q. Personal data collected, processed, sold or disclosed in relation to price, route or service, as such terms are used in the federal Airline Deregulation Act of 1978, 49 United States Code, Section 40101 et seq., by an air carrier subject to that Act, to the extent this chapter is preempted by the federal Airline Deregulation Act of 1978, 49 United States Code, Section 41713.

5. Compliance with COPPA. Controllers and processors that comply with the verifiable parental consent requirements of COPPA are deemed to be compliant with an obligation to obtain parental consent pursuant to this chapter.

§9604. Consumer rights

1. Consumer rights. A consumer has a right to:

A. Confirm whether or not a controller is processing the consumer's personal data and to access that personal data, unless such confirmation or access would require the controller to reveal a trade secret;

B. Correct inaccuracies in the consumer's personal data, taking into account the nature of the personal data and the purposes of the processing of the consumer's personal data;

C. Delete personal data provided by, or obtained about, the consumer;

D. Obtain a copy of the consumer's personal data processed by the controller, in a portable and, to the extent technically feasible, readily usable format that allows the consumer to transmit the data to another controller without hindrance, when the processing is carried out by automated means, as long as the controller is not required to reveal a trade secret; and

E. Opt out of the processing of the consumer's personal data for purposes of:

(1) Targeted advertising;

(2) The sale of personal data; or

(3) Profiling in furtherance of solely automated decisions that produce legal or similarly significant effects concerning the consumer.

2. Exercise of consumer rights. A consumer may communicate and access the information necessary to exercise rights under this section by a secure and reliable means established by the controller and described to the consumer in the controller's privacy notice. A consumer may designate an authorized agent in accordance with section 9605 to exercise the rights of the consumer to opt out of the processing of the consumer's personal data as specified in subsection 1, paragraph E, subparagraphs (1) and (2). In the case of processing personal data of a consumer known to be a child, the parent or legal guardian may exercise consumer rights on the child's behalf. In the case of processing personal data concerning a consumer subject to a guardianship, conservatorship or other protective arrangement, the guardian or the conservator of the consumer may exercise rights on the consumer's behalf.

3. Responding to exercise of consumer rights. Except as otherwise provided in this chapter, a controller shall comply with a request by a consumer to exercise the consumer's rights authorized pursuant to this chapter as follows.

A. A controller shall respond to the consumer without undue delay, but not later than the 45th day after receipt of the request. The controller may extend the response period by 45 days when reasonably necessary considering the complexity and number of the consumer's requests, as long as the controller informs the consumer of the extension within the initial 45-day response period.

B. If a controller declines to take action regarding the consumer's request, the controller shall inform the consumer without undue delay, but not later than the 45th day after receipt of the request, of the justification for declining to take action and instructions for how to appeal the decision.

C. The controller shall provide information in response to a consumer's request, free of charge, once during any 12-month period. If requests from a consumer are manifestly unfounded, excessive or repetitive, the controller may charge the consumer a reasonable fee to cover the administrative costs of complying with the request or decline to act on the request. The controller bears the burden of demonstrating the manifestly unfounded, excessive or repetitive nature of the request.

D. If a controller is unable to authenticate a request to exercise a right afforded under subsection 1, using commercially reasonable efforts, the controller is not required to comply with a request to initiate an action pursuant to this section and shall provide notice to the consumer that the controller is unable to authenticate the request to exercise the right until the consumer provides additional information reasonably necessary to authenticate the consumer and the consumer's request to exercise the right.

E. A controller that has obtained personal data about a consumer from a source other than the consumer is in compliance with a consumer's request to delete that data pursuant to subsection 1, paragraph C by:

(1) Retaining a record of the deletion request and the minimum data necessary for the purpose of ensuring that the consumer's personal data remains deleted from the controller's records and not using the retained data for any other purpose pursuant to the provisions of this chapter; or

(2) Opting the consumer out of the processing of the personal data for any purpose other than the purposes exempted from the provisions of this chapter.

4. Appeals. A controller shall establish a process for a consumer to appeal the controller's inaction on a request within a reasonable period of time after the consumer's receipt of the decision. The appeal process must be conspicuously available and similar to the process for submitting requests to initiate action pursuant to this section. Not later than the 60th day after receipt of an appeal, a controller shall inform the consumer in writing of action taken or not taken in response to the appeal, including a written explanation of the reasons for the decisions. If the appeal is denied, the controller shall also provide the consumer with an online mechanism, if available, or other method through which the consumer may contact the Attorney General to submit a complaint.

§9605. Authorized agent

A consumer may designate another person to serve as the consumer's authorized agent, and act on the consumer's behalf, to opt out of the processing of the consumer's personal data for the purposes specified in section 9604, subsection 1, paragraph E, subparagraphs (1) and (2). The consumer may designate an authorized agent by way of, among other methods, technology, including, but not limited to, an Internet link or a browser setting, browser extension or global device setting, indicating the consumer's intent to opt out of such processing. A controller shall comply with an opt-out request received from an authorized agent if the controller is able to verify, using commercially reasonable efforts, the identity of the consumer and the authorized agent's authority to act on the consumer's behalf.

§9606. Actions of controllers

1. Data minimization. A controller must comply with the requirements of this subsection.

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.

B. Except as otherwise provided in this chapter, a controller may not process personal data for purposes that are neither reasonably necessary for, nor compatible with, the disclosed purposes for which the data is processed, as disclosed to the consumer, unless the controller obtains the consumer's consent.

C. A controller shall process the minimum amount of personal data that is reasonably necessary, adequate or relevant for each purpose for which data is processed, as disclosed to the consumer

2. Duties. A controller shall:

A. Establish, implement and maintain reasonable administrative, technical and physical data security practices to protect the confidentiality, integrity and accessibility of personal data appropriate to the volume and nature of the personal data;

B. In the case of the processing of sensitive data concerning a consumer known to be a child, process the data in accordance with the federal Children's Online Privacy Protection Act of 1998, 15 United States Code, Section 6501 et seq., and the regulations, rules, guidance and exemptions adopted pursuant to that Act; and

C. 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 and, upon revocation of the consent, cease to process the data as soon as practicable, but not later than 15 days after the receipt of the request.

3. Prohibitions. A controller may not:

A. Process sensitive data concerning a consumer unless the controller obtains the consumer's consent;

B. Process personal data in violation of the laws of this State and federal laws that prohibit unlawful discrimination against consumers;

C. When the controller, under the circumstances, has actual knowledge or willfully disregards that the consumer is at least 13 years of age but has not attained 16 years of age:

(1) Process the personal data of the consumer for purposes of targeted advertising; or

(2) Sell the consumer's personal data without the consumer's consent; or

D. Retaliate against a consumer for exercising a consumer right in this chapter or for not agreeing to the collection or processing of personal data for a separate product or service, including by denying goods or services, charging different prices or rates for goods or services or providing a different level of quality of goods or services to the consumer.

4. Loyalty and rewards programs. Subsection 3 may not be construed to require a controller to provide a product or service that requires the personal data of a consumer that the controller does not collect or maintain or prohibit a controller from offering a different rate, level, quality or selection of goods or services to a consumer;

~~including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program.~~

4. Exceptions; loyalty programs. Subsection 3 may not be construed to:

A. Require a controller to provide a product or service that requires the processing of personal data of a consumer that the controller does not collect or maintain; or

B. Prohibit a controller from offering a different price, rate, level, quality or selection of goods or services to a consumer, including offering goods or services for no fee, if the offering is in connection with a consumer's voluntary participation in a bona fide loyalty, rewards, premium features, discounts or club card program, as long as the sale of personal data is not a condition of participation in the program.

5. Privacy notice. A controller shall provide consumers with an accessible, clear and meaningful privacy notice in plain language that is understandable by a reasonable consumer that includes:

A. The categories of personal data processed by the controller;

B. The purpose for processing personal data;

C. How consumers may exercise their consumer rights, including how a consumer may appeal a controller's decision with regard to the consumer's request;

D. The categories of personal data that the controller shares with 3rd parties, if any;

E. The categories of 3rd parties, if any, with which the controller shares personal data; and

F. An active e-mail address or other mechanism that the consumer may use to contact the controller.

6. Consumer rights request mechanism. A controller shall establish, and shall describe in a privacy notice, one or more secure and reliable means for consumers to submit a request to exercise a consumer right pursuant to this chapter. The design of the secure and reliable means must take into account the ways in which consumers normally interact with the controller, the need for secure and reliable communication of requests and the ability of the controller to verify the identity of the consumer making the request. A controller may not require a consumer to create a new account in order to exercise a consumer right, but may require a consumer to use an existing account.

~~**7. Notice of sale and targeted advertising.** If a controller sells personal data to a 3rd party or processes personal data for 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.~~

~~**7. Notice of sale and targeted advertising; opt-out mechanism.** If a controller sells personal data to a 3rd party or processes personal data for 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. The disclosure required under this section must include:~~

~~A. A clear and conspicuous link titled "Do Not Sell My Personal Data" or bearing a substantially similar title on the controller's publicly accessible website that directs the consumer, or an agent of the consumer, to a publicly accessible website that enables the consumer, or an agent of the consumer, to opt out of the sale of the consumer's personal data; and~~

~~B. A clear and conspicuous link titled "Opt Me Out of Targeted Advertising" or bearing a substantially similar title on the controller's publicly accessible website that directs the consumer, or an agent of the consumer, to a publicly accessible website that enables the consumer, or an agent of the consumer, to opt out of processing of the consumer's personal data for targeted advertising.~~

~~*In lieu of providing the 2 links described in paragraphs A and B, a controller may satisfy the requirements of this subsection by providing a single conspicuous and clearly labeled link on the controller's publicly accessible website that allows a consumer, or an agent of the consumer, both to opt out of the sale of the consumer's personal data and to opt out of the processing of the consumer's personal data for targeted advertising. If the*~~

controller maintains a specific section or page of its publicly accessible website that allows a consumer, or an agent of the consumer, to opt out of the sale of the consumer's data or the processing of the consumer's data for targeted advertising and to select additional privacy controls, the controller may satisfy the requirements of this subsection by providing a single conspicuous and clearly labeled link on the controller's publicly accessible website titled "Your Privacy Choices" or bearing a substantially similar title that directs the consumer, or an agent of the consumer, to that specific section or page of its publicly accessible website.

8. Universal opt-out mechanism. No later than December 1, 2027, a controller shall allow a consumer to opt out of any processing of the consumer's personal data for the purposes of targeted advertising or any sale of personal data through an opt-out preference signal sent, with the consumer's consent, by a platform, technology or mechanism to the controller indicating the consumer's intent to opt out of any such processing or sale. The platform, technology or mechanism:

- A. Must be consumer-friendly and easy to use by the average consumer;
- B. May not unfairly disadvantage another controller;
- C. May not make use of a default setting but must require the consumer to make an affirmative, freely given and unambiguous choice to opt out of any such processing or sale of the consumer's personal data;
- D. Must be as consistent as possible with another similar platform, technology or mechanism required by federal or state law; and
- E. Must enable the controller to reasonably determine whether the consumer is a resident of this State and whether the consumer has made a legitimate request to opt out of to the sale of the consumer's personal data or targeted advertising.

A controller that recognizes an opt-out preference signal that has been approved by the laws or regulations of another state is in compliance with this subsection.

§9607. Responsibilities of processors and controllers

1. Processor responsibilities. A processor shall adhere to the instructions of a controller and shall assist the controller in meeting the controller's obligations under this chapter. Assistance provided under this section must include:

- A. Taking into account the nature of processing and the information available to the processor, by appropriate technical and organizational measures, so far as is reasonably practicable, to fulfill the controller's obligation to respond to a consumer rights request;
- B. Taking into account the nature of processing and the information available to the processor, by assisting the controller in meeting the controller's obligations in relation to the security of processing the personal data and in relation to the notification of a breach of security, as required by chapter 210-B, of the system of the processor, in order to meet the controller's obligations; and
- C. Providing necessary information to enable the controller to conduct and document data protection assessments.

2. Contractual requirements. A contract between a controller and a processor must govern the processor's data processing procedures with respect to processing performed on behalf of the controller. The contract must clearly set forth instructions for processing data, the nature and purpose of processing, the type of data subject to processing, the duration of processing and the rights and obligations of both parties. The contract must require that the processor:

- A. Ensure that each person processing personal data is subject to a duty of confidentiality with respect to the data;
- B. At the controller's direction, delete or return all personal data to the controller as requested at the end of the provision of services, unless retention of the personal data is required by law;

C. On the reasonable request of the controller, make available to the controller all information in the processor's possession necessary to demonstrate the processor's compliance with the obligations in this chapter;

D. Allow and cooperate with reasonable assessments by the controller or the controller's designated assessor or arrange for a qualified and independent assessor to conduct an assessment of the processor's policies and technical and organizational measures in support of the obligations in this chapter, using an appropriate and accepted control standard or framework and assessment procedure for the assessment. The processor shall provide a report of the assessment to the controller upon request; and

E. Engage a subcontractor pursuant to a written contract that requires the subcontractor to meet the obligations of the processor with respect to the personal data.

3. Processing relationship liability. This section may not be construed to relieve a controller or processor from the liabilities imposed on the controller or processor by virtue of the controller's or processor's role in the processing relationship as described in this chapter.

4. Fact-based determination. Determining whether a person is acting as a controller or processor with respect to a specific processing of data is a fact-based determination that depends upon the context in which personal data is to be processed. A person who is not limited in the person's processing of personal data pursuant to a controller's instructions, or who fails to adhere to the instructions, is a controller and not a processor with respect to a specific processing of data. A processor that continues to adhere to a controller's instructions with respect to a specific processing of personal data remains a processor. If a processor begins, alone or jointly with other persons, determining the purposes and means of the processing of personal data, the processor acts as a controller with respect to the processing and may be subject to an enforcement action under section 9611.

§9608. Data protection assessments

1. Documentation. A controller shall conduct and document a data protection assessment for each of the controller's processing activities that presents a heightened risk of harm to a consumer. For the purposes of this section, "processing that presents a heightened risk of harm to a consumer" includes:

A. The processing of personal data for the purposes of targeted advertising;

B. The sale of personal data;

C. The processing of personal data for the purposes of profiling, when profiling presents a reasonably foreseeable risk of:

(1) Unfair or deceptive treatment of, or unlawful disparate impact on, consumers;

(2) Financial, physical or reputational injury to consumers;

(3) A physical or other intrusion upon the solitude or seclusion, or the private affairs or concerns, of consumers, when the intrusion would be offensive to a reasonable person; or

(4) Other substantial injury to consumers; and

D. The processing of sensitive data.

2. Required elements. Data protection assessments conducted pursuant to subsection 1 must identify and weigh the benefits that may flow, directly and indirectly, from the processing to the controller, the consumer, other stakeholders and the public against the potential risks to the rights of the consumer associated with the processing, as mitigated by safeguards that can be employed by the controller to reduce the risks. The controller shall factor into the data protection assessment the use of de-identified data and the reasonable expectations of consumers, as well as the context of the processing and the relationship between the controller and the consumer whose personal data will be processed.

3. Attorney General disclosure; exemption from public records. The Attorney General may require that a controller disclose a data protection assessment that is relevant to an investigation conducted by the Attorney

General, and the controller shall make the data protection assessment available to the Attorney General. The Attorney General may evaluate the data protection assessment for compliance with the responsibilities set forth in this chapter. A data protection assessment is confidential and exempt from disclosure under Title 1, chapter 13. To the extent information contained in a data protection assessment disclosed to the Attorney General includes information subject to attorney-client privilege or work product protection, the disclosure does not constitute a waiver of that privilege or protection.

4. Processing activity. A single data protection assessment may address a comparable set of processing operations that include similar activities.

5. Reciprocity. If a controller conducts a data protection assessment for the purpose of complying with another applicable law or regulation, the data protection assessment satisfies the requirements established in this section if the data protection assessment is reasonably similar in scope and effect to the data protection assessment that would otherwise be conducted pursuant to this section.

6. Application. A controller is not required to conduct a data protection assessment under this section for any processing activity created or initiated before July 1, 2026.

§9609. De-identified and pseudonymous data

1. De-identified data requirements. A controller in possession of de-identified data shall:

- A. Take reasonable measures to ensure that the data cannot be associated with an individual;
- B. Publicly commit to maintaining and using de-identified data without attempting to re-identify the data; and
- C. Contractually obligate recipients of the de-identified data to comply with all provisions of this chapter.

2. De-identified data and pseudonymous re-identification of data. This chapter may not be construed to require a controller or processor to:

- A. Re-identify de-identified data or pseudonymous data; or
- B. Maintain data in identifiable form, or collect, obtain, retain or access data or technology, in order to be capable of associating an authenticated consumer request with personal data.

3. Consumer requests. This chapter may not be construed to require a controller or processor to comply with an authenticated consumer rights request if the controller:

- A. Is not reasonably capable of associating the request with the personal data, or it would be unreasonably burdensome for the controller to associate the request with the personal data;
- B. Does not use the personal data to recognize or respond to the consumer who is the subject of the personal data, or associate the personal data with other personal data about the same consumer; and
- C. Does not sell the personal data to a 3rd party or otherwise voluntarily disclose the personal data to a 3rd party other than a processor, except as otherwise permitted in this section.

4. Pseudonymous data requirements. The rights afforded under section 9604, subsection 1 do not apply to pseudonymous data in cases when the controller is able to demonstrate that information necessary to identify the consumer is kept separately and is subject to effective technical and organizational controls that prevent the controller from accessing the information.

5. Contractual oversight. A controller that discloses pseudonymous data or de-identified data shall exercise reasonable oversight to monitor compliance with contractual commitments to which the pseudonymous data or de-identified data is subject and shall take appropriate steps to address breaches of those contractual commitments.

§9610. Controller and processor; duties and obligations

1. Exempt controller and processor activities. This chapter may not be construed to restrict a controller's or processor's ability to:

- A. Comply with federal laws or regulations or the laws or rules of a state;
- B. Comply with a civil, criminal or regulatory inquiry, investigation, subpoena or summons by federal or state governmental authorities or governmental authorities of a federally recognized Indian tribe in this State;
- C. Cooperate with federal, tribal or state law enforcement agencies concerning conduct or activity that the controller or processor reasonably and in good faith believes may violate federal laws or regulations or the laws and rules of a state;
- D. Investigate, establish, exercise, prepare for or defend legal claims;
- E. Provide a product or service specifically requested by a consumer;
- F. Perform under a contract to which a consumer is a party, including fulfilling the terms of a written warranty;
- G. Take steps at the request of a consumer prior to entering into a contract;
- H. Take immediate steps to protect an interest that is essential for the life or physical safety of the consumer or another individual and when the processing cannot be manifestly based on another legal basis;
- I. Prevent, detect, protect against or respond to security incidents, identity theft, fraud, harassment, malicious or deceptive activities or illegal activity or preserve the integrity or security of systems or investigate, report or prosecute those responsible for an action described in this paragraph;
- J. Engage in public or peer-reviewed scientific or statistical research in the public interest that adheres to all other applicable ethics and privacy laws and is approved, monitored and governed by an institutional review board that determines, or similar independent oversight entities that determine:
 - (1) Whether the deletion of the information is likely to provide substantial benefits that do not exclusively accrue to the controller;
 - (2) Whether the expected benefits of the research outweigh the privacy risks; and
 - (3) Whether the controller has implemented reasonable safeguards to mitigate privacy risks associated with research, including risks associated with re-identification;
- K. Assist another controller, processor or 3rd party with obligations under this chapter; or
- L. Process personal data for reasons of public interest in the area of public health, but solely to the extent that the processing is:
 - (1) Subject to suitable and specific measures to safeguard the rights of the consumer whose personal data is being processed; and
 - (2) Under the responsibility of a professional subject to confidentiality obligations under federal or state laws or local ordinances.

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

- A. Conduct internal research to develop, improve or repair products, services or technology;
- B. Effectuate a product recall;
- C. Identify and repair technical errors that impair existing or intended functionality; or
- D. Perform internal operations that are reasonably aligned with the expectations of the consumer or reasonably anticipated based on the consumer's existing relationship with the controller, or are otherwise compatible with processing data in furtherance of the provision of a product or service specifically requested by a consumer or the performance of a contract to which the consumer is a party.

3. Evidentiary privilege. The obligations imposed on controllers or processors under this chapter do not apply when compliance with this chapter by the controller or processor would violate an evidentiary privilege under the laws of this State. This chapter may not be construed to prevent a controller or processor from providing personal data concerning a consumer to a person covered by an evidentiary privilege under the laws of this State as part of a privileged communication.

4. Liability. A controller or processor that discloses personal data to a 3rd-party processor or 3rd-party controller in accordance with this chapter has not violated this chapter if the 3rd-party processor or 3rd-party controller that receives and processes the personal data violates this chapter, as long as, at the time the disclosing controller or processor disclosed the personal data, the disclosing controller or processor did not have actual knowledge that the receiving 3rd-party processor or 3rd-party controller would violate this chapter. A 3rd-party controller or 3rd-party processor receiving personal data from a controller or processor in compliance with this chapter is likewise not in violation of this chapter for the transgressions of the controller or processor from which the 3rd-party controller or 3rd-party processor receives the personal data.

5. Exemptions. This chapter may not be construed to:

A. Impose an obligation on a controller or processor that adversely affects the rights or freedoms of a person, including, but not limited to, the rights of a person:

- (1) To freedom of speech or freedom of the press guaranteed in the United States Constitution, Amendment I; or
- (2) Under Title 16, section 61; or

B. Apply to a person's processing of personal data in the course of the person's purely personal or household activities.

6. Limitations. Personal data processed by a controller or processor pursuant to this section may be processed only to the extent that the processing is:

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

B. Adequate, relevant and limited to what is reasonably necessary in relation to the specific purposes listed in this section. Personal data collected, used or retained pursuant to subsection 2 must, when applicable, take into account the nature and purpose of the collection, use or retention. The data must be subject to reasonable administrative, technical and physical measures to protect the confidentiality, integrity and accessibility of the personal data and to reduce reasonably foreseeable risks of harm to consumers relating to the collection, use or retention of personal data.

7. Controller burden. If a controller processes personal data pursuant to an exemption in this section, the controller bears the burden of demonstrating that the processing qualifies for the exemption and complies with the limitations in subsection 6.

8. Clarification of roles. Processing personal data for the purposes expressly identified in this section does not solely make a legal entity a controller with respect to the processing.

§9611. Enforcement

1. Violation as unfair trade practice; exclusive Attorney General enforcement. A violation of this chapter constitutes an unfair trade practice under the Maine Unfair Trade Practices Act, except that the provisions of Title 5, section 207, subsection 2 do not apply to this chapter and except as provided in subsections 2 and 3. The Attorney General has the exclusive authority to enforce violations of this chapter under the Maine Unfair Trade Practices Act.

2. Notice. Notwithstanding any provision of Title 5, section 209 to the contrary, at least 30 days prior to commencement of any action under the Maine Unfair Trade Practices Act to enforce this chapter, the Attorney General shall notify the person against whom an action may be brought of the intended action and give the person an opportunity to cure the alleged violation or violations. The Attorney General may bring an action pursuant to

this section only if the controller fails to cure one or more of the alleged violations described in the notice within 30 days of receiving the notice.

3. No private right of action. Notwithstanding Title 5, section 213, this chapter may not be construed as creating a private right of action under this chapter or any other provision of law against any person based on a violation of any provision of this chapter or any other law.

4. Preemption. This chapter supersedes and preempts any ordinance, resolution, rule or other regulation adopted by a political subdivision of the State regarding the processing of personal data by a controller or processor.

§9612. Maine Privacy Fund established

1. Establishment; purpose. The Maine Privacy Fund, referred to in this section as the "fund," is established within the Department of the Attorney General as a nonlapsing fund to providing funding for the staff and activities of the department necessary to enforce the provisions of this chapter.

2. Administration. The Department of the Attorney General shall administer the fund. The fund must be established and held separate and apart from any other funds or money of the State or the department and must be used and administered exclusively for purposes authorized in this section. The fund consists of:

A. Any civil penalties, attorney's fees or costs awarded to the State in an action brought by the Attorney General to enforce a violation of this chapter;

B. Sums that may be appropriated by the Legislature to the fund or transferred by the Treasurer of State to the fund;

C. Interest earned on fund balances; and

D. Other funds received from any public or private source, including grants, gifts, bequests and donations.

Sec. 2. 35-A MRSA c. 94, as amended, is repealed.

Sec. 32. Report. By February 1, 2027, the Attorney General shall submit a report to the joint standing committee of the Legislature having jurisdiction over judiciary matters regarding the operation and implementation of the Maine Revised Statutes, Title 10, chapter 1057. The report must include, at a minimum, the following information:

1. The number of notices the Attorney General has issued under Title 10, section 9611, subsection 2 and the nature of the violations alleged in the notices;

2. The number of persons sent a notice described in subsection 1 that conferred with the Attorney General during the notice period described in Title 10, section 9611, subsection 2 in a manner that alleviated the need for a civil action under the Maine Unfair Trade Practices Act;

3. The number of civil actions brought by the Attorney General under the Maine Unfair Trade Practices Act to enforce violations of Title 10, chapter 1057; and

4. Any recommendations the Attorney General has for improving the operation of Title 10, chapter 1057.

The joint standing committee of the Legislature having jurisdiction over judiciary matters may report out legislation related to the report to the 133rd Legislature in 2027.

Sec. 43. Effective date. This Act takes effect July 1, 2026.

SUMMARY

This amendment ... [amendment summary not yet drafted]