Maine State Legislature
OFFICE OF POLICY AND LEGAL ANALYSIS
www.mainelegislature.gov/opla
13 State House Station, Augusta, Maine 04333-0013
(207) 287-1670

MEMORANDUM

TO: Members, Joint Standing Committee on Judiciary

FROM: Janet Stocco, Legislative Analyst

DATE: September 25, 2023

RE: **Overview: carryover bills related to data privacy**

The chart below provides an overview of the bills related to data privacy carried over by the Judiciary Committee to the Second Regular Session.

	Issue addressed	Brief overview
LD 1056, An Act Restricting State Assistance in Federal Collection of Personal Electronic Data and Metadata (Sen. Brakey)	4th Amendment: State and local cooperation with federal agency access to electronic communication info.	Prohibits the State and its political subdivisions from providing resources or support to any federal agency in the collection or use of a person's electronic communication data and metadata about electronic communications unless the collection or use is based on consent, a warrant or an exception to the warrant requirement.
LD 1576, An Act to Update the Laws Governing Electronic Device Information as Evidence (Rep. O'Neil)	4th Amendment: State and local government access to electronic device data	Extends state law to require state and local government entities to obtain a search warrant and provide subsequent notice to the owner of any electronic device—or meet a specific exception to the warrant or notice requirements—to obtain each of the following types of information, whether the information is obtained from a cellular, email, social media or cloud company; from anyone not the owner/user of the device; or by searching or communicating with the device: • Content of electronic communications • Specific info. about electronic communications (recipient, date, etc.) • Current and prior location information • Other info. stored on or transmitted through the electronic device Information obtained in violation of the law is inadmissible at trial and a court may issue an injunction against a government entity that violates the law.

LD 1705, An Act to Give Consumers Control over Sensitive Personal Data by Requiring Consumer Consent Prior to Collection of Data (Rep. O'Neil)	Consumer privacy: Biometric identifiers	Regulates the collection, storage, use and dissemination of biometric identifiers • *Not applicable to:* government entities, medical research; personal health information subject to HIPAA; or personal information collected, processed, sold or disclosed under the federal Gramm-Leach-Bliley Act. • *Requires* private entities (a) to obtain written consent before they collect, store, purchase, use, disclose or disseminate biometric identifiers; (b) to disclose specified information about biometric identifiers associated with a requesting individual on request; (c) to establish publicly available written polices for retention and destruction of biometric identifiers; and (d) to store and transmit biometric identifiers safely in a way that prevents disclosure. • *Prohibits* (a) discrimination against customers who do not consent to collection of biometric identifiers; (b) entities from selling, leasing or trading the biometric identifiers they collect or permitting other entities with whom they share biometric identifiers from doing so. • *Remedies:* Individual or Attorney General may bring an action for damages of ≥$1,000 for negligence or ≥$5,000 for reckless or intentional misconduct, attorney's fees and/or equitable relief under the bill or bring a UTPA action. • **Effective date**: January 1, 2025
LD 1902, An Act to Protect Personal Health Data (Rep. O'Neil) *Short title:* "My Health My Data Act"	Consumer privacy: Health data not held by a HIPAA-regulated entity	Regulates the collection, storage and dissemination of consumer health data (includes biometric identifiers if used for health-care-related purposes) • *Not applicable to*: government entities and information collected, used or disclosed under specific laws related to the confidentiality of health care information (HIPAA, the state analogue to HIPAA and federal substance use disorder patient record regulations). • *Requires* private entities (a) to obtain separate consent for collection and sharing of consumer health data, unless collection or sharing is necessary to provide a product or service the consumer requested; (b) to confirm their collection or sharing of consumer health data on request and to comply with consent withdrawals or data-deletion requests; (c) to establish and display a data privacy policy and (c) to limit access to consumer health data and establish and follow data security and retention and destruction policies. • *Prohibits*: (a) discrimination against consumers who do not consent to their data being collected or shared; (b) the sale of consumer health data; or (c) creating a geofence around a facility to identify, track or target messages to consumers therein. • *Remedies:* Individual or Attorney General may bring an action for damages of ≥$1,000 for negligence or ≥$5,000 for reckless or intentional misconduct, attorney's fees and/or equitable relief under the bill or bring a UTPA action.

LD 1973, An Act to Enact the Maine Consumer Privacy Act (Sen. Keim)	Consumer privacy: Personal data (all types)	**A.** Regulates sale and "processing"—collection, use, storage, disclosure, analysis and modification—of "personal data" (non-public information linkable to an individual) • *Applicability:* Businesses that processes personal data of ≥ 100,000 Maine consumers per year (or ≥ 25,000 Maine consumers per year if that represents > 25% of gross revenue) o Does not apply to the State or political subdivisions, certain tax-exempt organizations, higher education institutions, federally regulated financial institutions and credit reporting agencies, entities governed by HIPAA, human subject research, etc. (long list) • *Requires* consumer or their agent to opt-in/consent to (a) process certain sensitive data for any purpose—includes all personal data of children < 13; (b) process other personal data for purposes of targeted advertising or profiling and (c) sell any personal data. o May only collect personal data reasonably necessary to purpose disclosed to consumer • *Consumer rights*: to confirm whether business has one's personal data and obtain a copy of and request correction or deletion of that data (generally may make one free request/year) • *Other business duties:* (a) may not discriminate against consumers who opt-out, except certain voluntary consumer loyalty programs; (b) must provide privacy notice identifying what personal data is processed and why, business contact info. and info. on how to exercise consumer rights; and (d) must conduct data protection assessments for processing activities presenting a heightened risk to consumers, ex: sale of personal data. (Not a complete list) • *Remedies:* The bill's requirements are enforceable in a civil action by the Attorney General (not an action by a consumer), after notice and 30-day right to cure period **B.** Repeals 35-A M.R.S. §9301, a state law eff. July 1, 2020, generally requiring broadband internet service providers to obtain consent before using, disclosing, or selling personal info.
LD 1977, An Act to Create the Data Privacy and Protection Act (Representative O'Neil)	Consumer privacy: Personal data (all types)	Regulates collection, use, storage, disclosure, analysis and sale of "covered data" (non-public information linkable, alone or in combination with other info., to an identifiable individual) • *Applicability*: Does <u>not</u> apply to government agencies <u>or</u> businesses that have < $20 million per year in revenue, collect/process data of ≤ 75,000 individuals/year, <u>and</u> do not sell data • *Prohibitions:* Covered entities may not: o Collect, process or transfer—any covered data unless reasonably necessary and proportionate or sensitive data unless strictly necessary—to provide or maintain a specific product or service requested by the individual; o Transfer sensitive data to a third party without affirmative consent (unless necessary for a purpose listed in the bill, for example, to prevent imminent injury, etc.); o If the entity is a cable or other video service, share data on content used without consent or as is strictly necessary to provide or maintain the product or service;

		○ Process sensitive data for targeted advertising; ○ Engage in targeted advertising to a minor; ○ Engage in targeted advertising of an adult without affirmative consent; ○ Transfer covered data of a known minor without affirmative consent of the minor or their parent/guardian, except may report child victimization info. to authorities • *Consumer rights*: may, in any language in which service is offered, request access to covered data collected or transferred in past 24 months and request correction or deletion of that covered data. (May make 2 free requests/year) • *Other business duties*: (a) may not retaliate against individual for not consenting to collection or use of covered data, but may offer customer loyalty or rewards programs if certain conditions are met; (b) may not collect or use covered data to discriminate on the basis of race, color, religion, national origin, sex, or disability – unless the business is a private club; (c) must create a publicly available and accessible privacy policy identifying: covered data it collects and uses as well as why and for how long it is kept; the third parties with whom covered data is shared; contact information; and how to exercise consumer rights; (d) notify customers of material changes to its privacy policy. (Not a complete list) • *Additional tasks for specific businesses*: ○ Large data holders must annually: disclose to public specific metrics; review internal controls and reporting structures; and certify compliance to the Attorney General ○ Data brokers: must notify public of status and register annually with Attorney General; ○ If not a "small business": must before use and annually thereafter conduct an impact assessment of certain algorithms to minimize risks of harm and submit audit report to Attorney General; and designate a privacy officer and data security officers; and conduct privacy impact assessments (available to Atty General) every other year. • *Remedies:* Attorney General, district attorney or municipal attorney may bring action for civil penalties, restitution or other compensation for residents of the State, equitable relief and attorney's fees. A private individual may bring action (but not against a small business) for damages (at least $5,000), punitive damages, attorney's fees and equitable relief. Pre-dispute arbitration agreements and waivers of right to class action status are unenforceable. • *Effective date*: most of the bill is effective 180 days after adjournment; certain requirements (ex: periodic algorithm and privacy impact assessments) are effective 1 to 2 years later.