Mass. Data Privacy Bill Would Increase Litigation Risks

By **Melanie Conroy and Peter Guffin** (November 19, 2021)

Melanie Conroy

Peter Guffin

On Oct. 13, the Joint Committee on Advanced Information Technology, the Internet and Cybersecurity — newly created by the commonwealth of Massachusetts — held a public hearing on pending legislation, including a comprehensive data privacy bill.

While the hearing's agenda covered a range of topics including net neutrality, equitable broadband access and technology in education, comprehensive data privacy was a central focus of public comment.[1]

The bill in question, An Act establishing the Massachusetts Information Privacy Act, was introduced as S.46 by Sen. Cynthia Stone Creem and as H.142 by Rep. Juan Vargas.[2] If enacted, the proposed law could reshape how businesses interact with Massachusetts consumers and employees, increase the cost and complexity of privacy design and compliance, and expose companies to new and significant enforcement and litigation risks.

A Recent History of Data Privacy Legislation

In early 2019, the Massachusetts Legislature introduced a predecessor bill that would have reshaped the privacy landscape in the commonwealth. We published a summary of that predecessor legislation in May 2019, and chronicled its public debate before the Committee on Consumer Protection and Professional Licensure before it ultimately stalled at the end of the prior legislative session.[3]

This prior proposal was introduced against a backdrop of landmark data privacy legislation in Europe, California and Illinois: the General Data Protection Regulation, or GDPR, which went into effect in May 2018;[4] the California Consumer Privacy Act, or CCPA, which became effective on Jan. 1, 2020;[5] and the Illinois Biometric Information Privacy Act, or BIPA, which was enacted in 2008.[6]

In the intervening years since data privacy was last under consideration by the Massachusetts Legislature, state privacy laws have proliferated, providing additional benchmarks for the commonwealth to consider.

Proposition 24, which was approved by California voters in November 2020, amended the CCPA with enhanced privacy protections for sensitive personal information through the California Privacy Rights Act, or CPRA, which becomes effective Jan. 1, 2023.[7]

Although Washington state appeared poised to follow California, for a second year in a row, the legislation foundered in 2020 over the issue of a private right of action.[8] Instead, in March 2021, Virginia became the second state to pass a comprehensive data privacy law, the Consumer Data Protection Act, which becomes effective Jan. 1, 2023.[9]

Colorado quickly followed, enacting the Colorado Privacy Act in July 2021, which will become effective on July 1, 2023.[10] Despite a growing patchwork of state laws that would benefit from a uniform federal statute, federal privacy legislation has thus far stalled, and privacy bills are currently pending in Maine, Minnesota, New York, North Carolina, Ohio and

Pennsylvania.

Key Features of Massachusetts' Privacy Bill

The proposed Massachusetts Information Privacy Act, or MIPA, draws on GDPR, CCPA/CPRA, and BIPA. MIPA would take effect 12 months after enacted and some have described it as the most sweeping privacy legislation proposed to date. Its notable features include:

- Broad application to businesses operating in Massachusetts that earn $10,000 or more annual revenue through 300 or more transactions or that process or maintain the personal information of 10,000 or more individuals annually.

- Creation of a new state agency, the Massachusetts Information Privacy Commission, with enforcement, investigation, rulemaking and regulatory authority, including to hear civil administrative complaints by individuals.

  The five commissioners would be required to have expertise in the relevant subject matter and would be appointed to a five-year term by the governor, attorney general and secretary of the commonwealth.

  Both the commission and the Massachusetts Attorney General would be empowered to seek civil penalties between $15,000 (or 0.15% of the annual global revenue of the covered entity, if greater) and $20,000,000 (or 4.00% of the annual global revenue of the covered entity, if greater) — depending on enumerated factors, including the number of individuals affected, the conduct of the entity. and the risks created by noncompliance.

  In addition, MIPA would empower the Massachusetts Attorney General to bring a civil action against a covered entity to recover the same range of civil penalties based on the same factors.

- Rights beyond a notice-and-consent framework — including rights of access, correction, portability, disclosure and deletion through a notice and consent process.

  Consent must be renewed annually and before processing is changed, or otherwise is deemed to have been withdrawn. The bill would also create duties of care, confidentiality and loyalty that covered entities owe to Massachusetts residents, including for data minimization, breach disclosure and information security.

- Strict regulation of biometric and sensitive location information, forbidding the collection of this information absent express, handwritten consent, barring the use of devices to record such data without notice and consent that can remain effective for only 180 days, and prohibiting the monetization of such information.

  The only exception to the bar on monetization is the recommendation of goods or services subject to enhanced notice and consent provisions.

- Limiting employee surveillance by restricting an employer's ability to monitor employees — including through devices, with narrow exceptions only for quality, safety or essential job function purposes that must be conducted by the least invasive means possible and limited to the smallest number of employees necessary.

  Covered entities may not require employees to install applications or wear data-collecting devices unless necessary to accomplish essential job functions, narrowly limited to the activities and times necessary to accomplish essential job functions.

- Prohibiting discrimination by forbidding the processing of personal information that results in unlawful discriminatory actions or discrimination in the provision of information or services based on the provision of consent. The bill would also proscribe unfair and deceptive trade practices that interfere with the ability of individuals to understand the use of their data or take advantage of individuals' reliance on covered entities to act in their interests.

- Creating a private right of action for individuals ages 13 and older to bring a civil action for any violation of MIPA or a regulation promulgated thereunder regarding that individual's personal information. MIPA would create a rebuttable presumption of harm and prohibit any requirement for an individual to file an administrative complaint before filing suit.

  Individuals could recover (1) minimum damages of 0.15% of the annual global revenue of the covered entity or $15,000 per violation, whichever is greater, (2) punitive damages, (3) reasonable attorney's fees and costs, (4) injunctive and other appropriate relief.

  Covered entities may not require individuals, as a condition of service or otherwise, to accept mandatory arbitration. MIPA states that it would invalidate any waiver of a remedy or means of enforcement in any contract as contrary to public policy.

- Very limited exceptions distinguish MIPA from other state privacy legislation.

  MIPA exempts only (1) health information collected by providers, to diagnose or treat an illness, for medical education or public health purposes, or subject to the federal Health Insurance Portability and Accountability Act of 1996, and (2) contact and networking information shared by individuals or employers.

  MIPA would not exempt institutions of higher education or non-profit entities, and does not exempt data or entities subject to the Gramm Leach Bliley Act, the Family Educational Rights and Privacy Act or the Fair Credit Reporting Act.

Public Comments on MIPA

At the Oct. 13, public hearing, a majority of commenters spoke in favor of MIPA. A broad range of supporting organizations and speakers urged legislators to position Massachusetts as a leader in data privacy, going beyond even the most expansive laws enacted in other jurisdictions, including Europe, California and Illinois.

Those testifying against the passage of MIPA as currently drafted cautioned that vague or overbroad definitions and the expansive private right of action could create a feeding frenzy of class action activity in the commonwealth, making Massachusetts a hotbed of litigation that may benefit few outside the plaintiffs bar.

Commenters also warned that overbroad nondiscrimination provisions could harm consumers, barring customer loyalty benefits, discount programs and fraud prevention benefits. Speakers warned that repetitive and extensive notice and consent requirements would burden consumers with little proven benefit.

These presenters urged legislators to look to Virginia and other jurisdictions, aiming for uniformity with other states rather than blazing a new path that adds to a multistate compliance maelstrom.

The committee indicated it would carefully consider public testimony from the hearing as well as submitted written statements.

What Businesses Should Know About the Legislative Timeline

Under current legislative deadlines, the committee is required to report out on MIPA by Feb. 2, 2022.[11] In a favorable report, the committee can recommend that MIPA pass in its original form or with amendments. An unfavorable report or study order would effectively derail MIPA, like its predecessor, for the remainder of the current session.

However, even with an unfavorable report or study order, proponents could introduce a new version of the bill during the next legislative session in 2023.

How Businesses Can Prepare for MIPA's Potential Passage

Although businesses would have 12 months from the date enacted to prepare for MIPA compliance, there are steps to prepare that make sense regardless of the legislative outcome.

- Consider the likelihood that MIPA might apply to your business based on its current language.

  MIPA has a significantly lower threshold for application than laws in California, Virginia and Colorado, and so businesses that are not yet subject to comprehensive privacy laws may find themselves under tight time pressure to get up to speed. Companies can avoid an unnecessary scramble by making an early assessment of whether they would be subject to a new law.

- Embrace best practices that mitigate risk because, regardless of whether such obligations are enacted through MIPA, they could prevent avoidable liabilities.

The CPRA memorializes the right to data minimization, and so businesses that are already preparing for compliance will be well positioned in the event MIPA is enacted. Even if a business would not be subject to CPRA, minimization is a prudent principle to embrace.

In addition, while MIPA would create information security duties, it is advisable amid growing cybersecurity risks for all companies to assess and enhance their data security.

- Do not rely on compliance with other state privacy laws, because MIPA contains new and expanded features that build on prior legislation.

  While a robust compliance program designed to meet the standards of predecessor statutes is a strong head start, businesses cannot be complacent in the event that MIPA is passed and would need to separately examine any potential compliance hurdles specific to a new Massachusetts law.

- Evaluate the extent to which highly sensitive biometric and location information is collected — including from employees through applications or devices — and assess whether these practices are already subject to notice and consent procedures and are minimized and tailored to necessary functions to the greatest extent possible.

- Invest in privacy expertise and compliance today, because an increasingly complex and inconsistent patchwork of different state standards appears to be an ongoing reality that is not going away. With federal privacy legislation stalling and state proposals proliferating, compliance challenges are likely to increase rather than abate.

- Prepare for increased consumer and employee scrutiny, regardless of whether or when comprehensive data privacy passes in Massachusetts.

  As news headlines over the past year have shown, consumers and employers alike are becoming ever more concerned with how their information is collected and used and the security of their personal data. In this environment, a robust privacy policy can be a competitive advantage for businesses with potential employees and consumers.

- Assess arbitration provisions and prepare for legal battles ahead concerning MIPA's private right of action.

Like its California and Illinois predecessors — but unlike the laws recently enacted in Virginia and Colorado — MIPA contains a private right of action that is unprecedented and would be the broadest in the country. The available damages under MIPA dramatically exceed the maximum offered in California at $750 per violation and Illinois at $5,000 per violation.

And, unlike California's private right of action, MIPA does not restrict the private right of action to certain types of violations. Critics' warnings that MIPA could open Massachusetts to a tidal wave of litigation are grounded in experience and are not hollow claims.

MIPA's prohibition on mandatory arbitration would most certainly meet a challenge under the Federal Arbitration Act, with litigants likely looking to the Sept. 15, U.S. Court of Appeals for the Ninth Circuit decision in Chamber of Commerce of the United States v. Bonta, which upheld California's mandatory arbitration ban enacted in AB51.

Businesses would be well advised to consider current arbitration provisions and confer with counsel concerning whether updates to arbitration terms or procedures are appropriate in the current climate.

Conclusion

It is difficult to overstate the magnitude of compliance and litigation risks MIPA may create for businesses collecting data from Massachusetts consumers and employees.

These businesses and their advisers should follow the progress of MIPA closely, and be prepared to creatively formulate compliance and risk mitigation strategies to confront a potential tidal wave of enforcement activity and class action litigation in Massachusetts.

Melanie A. Conroy is counsel and Peter J. Guffin is a partner at Pierce Atwood LLP.

[1] 10/13/2021 Agenda, Committee Hearing on Bills Related to Data Use, Data Privacy, the Internet, and Broadband Access, Joint Committee on Advanced Technology, the Internet and Cyber Security https://malegislature.gov/Events/Hearings/Detail/4007.

[2] S.46, https://malegislature.gov/Bills/192/S46;
H.142, https://malegislature.gov/Bills/192/H142.

[3] For our coverage of those developments, please see: https://www.pierceatwood.com/alerts/massachusetts-consumer-data-privacy-bill-could-dramatically-expand-class-action-litigation, https://www.pierceatwood.com/alerts/state-legislature-hears-concerns-about-proposed-massachusetts-consumer-data-privacy-bill, https://www.pierceatwood.com/alerts/massachusetts-legislature-hits-pause-button-

comprehensive-consumer-data-privacy.

[4] EU Regulation 2016/679, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679.

[5] Cal. Civ. Code § 1798.100 (as amended by California Consumer Privacy Rights and Enforcement Act on November 3, 2020), https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[6] 740 ILCS/14, https://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[7] California Assembly Bill No. 1490, https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=202120220AB1490.

[8] Concerning the management and oversight of personal data, Washington Senate Bill No. 6281 https://app.leg.wa.gov/billsummary?BillNumber=6281&Initiative=false&Year=2019.

[9] Virginia Senate Bill No. 1392, https://lis.virginia.gov/cgi-bin/legp604.exe?ses=212&typ=bil&val=sb1392.

[10] Colorado Senate Bill No. 190, https://leg.colorado.gov/sites/default/files/2021a_190_signed.pdf.

[11] 2021-2022 Session Legislative Deadlines & Significant Dates, https://malegislature.gov/ClerksOffice/Senate/Deadlines.