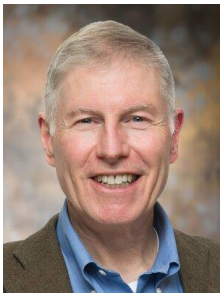
As Mass. Punts On Privacy Law, Cos. Can't Be Complacent

By **Peter Guffin and Melanie Conroy** (October 11, 2022)



Peter Guffin

Melanie Conroy

With another legislative session set to close, the Massachusetts Legislature has yet again punted the issue of comprehensive consumer data privacy to a future term.

This development may come as a disappointment or relief, depending on an observer's view on proposed legislation to date. Nonetheless, businesses should continue to evaluate their existing operations and obligations to ensure they remain well prepared for recent changes and future developments.

While Massachusetts lawmakers are at a standstill, companies doing business in the commonwealth should not become complacent and need to look beyond Massachusetts.

Operations in Massachusetts can easily intersect with other states' recently enacted data privacy legislation, and companies should anticipate the prospect of new Federal Trade Commission consumer privacy rules that, although not imminent, appear to be on the horizon.

In this article, we recap recent legislative activity in Massachusetts, recent developments in other states, and the FTC's recent announcement that it is exploring privacy rulemaking.

Massachusetts Consumer Data Privacy Introduced and Debated in 2019 and 2021

In 2019, Massachusetts state senators introduced a consumer data privacy bill with a broad private right of action.[1]

The proposed law, An Act Relative to Consumer Data Privacy or S.B. 120, would have permitted any consumer to bring a lawsuit against any violating business or service provider, regardless of actual losses.[2] S.B. 120 was referred to the Joint Committee on Consumer Protection and Professional Licensure,[3] which held a hearing in October 2019.[4]

Following a public hearing Feb. 5, 2020, the Joint Committee issued a Study Order on S.B. 120.[5][6]

During the next legislative session in 2021, a successor bill, the Massachusetts Information Privacy and Security Act or H.B. 142, was introduced.[7]

The proposed law would have reshaped how businesses interact with Massachusetts consumers, increased the cost and complexity of privacy design and compliance, expanded the Massachusetts attorney general's enforcement powers, and exposed companies to new and significant litigation risks.[8]

The newly created Joint Committee on Advanced Information Technology held a virtual hearing on the legislation October 2021,[9] and in March reported a new draft of the bill, titled the Massachusetts Information Privacy and Security Act or H.B. 4514,[10]

recommending its passage and forwarding it on to review by the Joint Committee on Health Care Financing.[11]

The reporting date for the bill was extended to June 1, pending concurrence by the Senate, and the Senate ultimately concurred on May 26. However, on Sept. 15, the bill met a final roadblock in this legislative session when, like its predecessor, it was sent to a study order.

A study order authorizes the joint committee to sit during recess to study the bill and, if appropriate, to file a report of findings.

However, for the vast majority of bills sent to a study order, no further committee activity takes place. For this reason, many observers view a study order as a procedural mechanism to table a bill until a future legislative session.

The Future of Comprehensive Consumer Data Privacy in Massachusetts

Many believed the latest draft of comprehensive consumer data privacy legislation had favorable odds of passage and could have made Massachusetts an early mover in creating a comprehensive regulatory scheme for consumer data privacy.

Now, the future of consumer data privacy law in Massachusetts is more uncertain.

However, the legislative focus on data privacy is unlikely to abate. Absent federal legislation or regulation that would preempt state-level action, we are likely to see a comprehensive consumer data privacy law introduced in the next legislative term.

The current legislative term comes to an end at the close of this year, and sponsors may introduce new legislation at the start of the new term in January.[12]

Looking Beyond Massachusetts to a Growing Consensus of State Privacy Laws

In the meantime, of course, Massachusetts businesses should not assume they are off the hook for consumer privacy compliance.

In other recent developments, five comprehensive state consumer privacy laws take effect in 2023:

- The California Privacy Rights Act, or CPRA;[13]
- The Virginia Consumer Data Protection Act, or CDPA;[14]
- The Connecticut Act Concerning Personal Data Privacy and Online Monitoring, or CTDPA;[15]
- The Colorado Privacy Act, or CPA;[16] and
- The Utah Consumer Privacy Act, or UCPA.[17]

These new laws may apply to Massachusetts companies doing business in those five states. Two of those laws — the CPRA and the CDPA — take effect as early as Jan. 1.

Although there are some significant differences among each of these new consumer privacy

laws, especially concerning applicability triggers, there are several key, substantive similarities.

These harmonies represent an increasing awareness of the fast-evolving privacy threat landscape in today's digital economy as well as a growing coalescence around what constitutes reasonable consumer rights and protections for personal data and the privacy measures organizations must put in place.

For example, all of these new laws establish a separate category of sensitive data that includes, among other things, personal data revealing precise geolocation, biometric information, race, ethnicity, religious affiliation, mental or physical health condition, and sexual orientation.

Consumers under all of these laws now have the right to limit a company's use and disclosure of sensitive data, and a company holding such information is prohibited from using or disclosing it without the consumer's consent. The CPA, CDPA and CTDPA specifically require opt-in consent.

In addition to granting rights to consumers for accessing, correcting, and deleting their personal data, all of these new laws also specifically grant consumers the right to opt out of the sale of their personal data.

The definition of "sale" is similar under all of these laws. It generally means the exchange to a third party for monetary consideration, subject to certain exceptions, e.g., transfers to processors and affiliates.

Consumers under the CPA, CDPA, UCPA and CTDPA have the right to opt out of targeted advertising.

The definition of "targeted advertising" is essentially the same under all four laws. It means displaying advertisements to a consumer based on personal information obtained from that consumer's activities over time and across nonaffiliated websites, or online applications to predict preferences or interests.

Consumers under the CPA, CDPA and CTDPA have the right to opt out of profiling.

The definition of "profiling" is essentially the same under all three of these laws. It means automated processing to evaluate, analyze, or predict personal aspects related to a person's economic situation, health, personal preferences, interests, reliability, behavior, location, or movement.

With the exception of the UCPA, all of these new laws require companies to conduct data protection impact assessments in circumstances where there is a heightened risk of harm to consumers, including any sale of personal data, any processing of sensitive data, and any risky targeted advertising or profiling.

All of these new laws also impose obligations for companies to include certain stringent contractual limitations in their contracts with any third-party recipients of personal data, such as service providers.

Each of these new laws charges the attorneys general in the state with responsibility for enforcement. There is no private right of action under any of these laws, except for the CPRA in very limited circumstances.

Except for the CPRA, all of these new laws have exemptions for employee or applicant personal data within the employment context, and commercial and B2B personal data within the business context. Except for the CPA, all of these new laws exempt non-profits.

During public hearings on proposed data privacy legislation in Massachusetts, commenters urged lawmakers to adopt laws that would be in harmony with other jurisdictions and thus reduce the burden of compliance on Massachusetts businesses.

Future Prospects for Harmonization?

Although the prospects are now looking pretty dim for federal privacy legislation, at least in the foreseeable future, the current, nascent harmonization of state consumer privacy laws is likely to get a strong boost from the Federal Trade Commission's recent announcement that it is exploring privacy rulemaking under its Section 18 authority to crack down on harmful commercial surveillance and lax data security.[18]

According to the FTC, the massive scale at which companies collect personal data on individuals, and the vast array of collection contexts, have heightened the risks and stakes of data breaches, deception, manipulation, and other abuses. If privacy rules are established by the FTC, they would be binding on all of the industries under its jurisdiction.

Not surprisingly, the topics of particular concern expressed by the FTC in its advance notice of proposed rulemaking align closely with many of the same, heightened-risk areas that have been the focus of new comprehensive state privacy laws, including sensitive personal data, targeted advertising and profiling.

For example, the FTC has stated it is concerned about the protective efficacy of the notice and consent framework for certain categories of data, and is considering whether certain types of data collection and processing should be permitted in the first place.

Biometric information is a priority area for the FTC, suggesting that the FTC is considering rules that impose substantive limits on the use of facial recognition, fingerprinting and other biometric technologies.

Personalized advertising, algorithms, and algorithmic discrimination also appear to be key areas of focus for the FTC, in addition to data security, data minimization, and retention. More specificity and detail about these topics will become evident in any subsequent notice of proposed rulemaking where the FTC must publish the text of any proposed rules.

Although it is much too early to tell, the FTC's regulatory requirements could include:

- Measures on transparency;
- User rights to data access, correction, deletion and portability;
- A ban on algorithmic discrimination;
- Disparate impact assessments for algorithmic applications; an opt-out of targeted ads;
- A ban on targeted ads to minors; and
- Mandates for privacy impact assessments.

The rules also could include a mandate that companies implement specific security measures, such as encryption, or require that all industry sectors subject to its jurisdiction

comply with the data security requirements under the FTC Safeguards Rule, which was recently updated by the FTC.[19]

The FTC Safeguards Rule currently applies only to certain financial institutions by virtue of the Gramm-Leach-Bliley Act.

Taking the long view, all of this recent state legislative and FTC rulemaking activity signals that we are now at a critical inflection point for consumer privacy rights and protection in the U.S.

Together, the results of these separate initiatives move the U.S. closer, albeit slowly, toward a comprehensive privacy protection framework that harmonizes a set of new governing, fundamental principles for today's digital world.

Peter J. Guffin is of counsel and chair of the privacy and data security practice at Pierce Atwood LLP.

Melanie A. Conroy is a partner at the firm.

[1] "Massachusetts Consumer Data Privacy Bill Could Dramatically Expand Class Action Litigation Risk," 05/21/2019, available at: https://www.pierceatwood.com/alerts/massachusetts-consumer-data-privacy-bill-could-dramatically-expand-class-action-litigation.

[2] An Act Relative to Consumer Data Privacy, Bill S.120, 191st (2019 - 2020), available at: https://malegislature.gov/Bills/191/SD341.

[3] Joint Committee on Consumer Protection and Professional Licensure, available at: https://malegislature.gov/Committees/Detail/J17/191.

[4] "State Legislature Hears Concerns About Proposed Massachusetts Consumer Data Privacy Bill," 10/11/2019, available at: https://www.pierceatwood.com/alerts/state-legislature-hears-concerns-about-proposed-massachusetts-consumer-data-privacy-bill.

[5] Joint Committee on Consumer Protection and Professional Licensure, available at: https://malegislature.gov/Committees/Detail/J17/191/Bills/asc/EntityNumber/?current=False&pageNumber=2.

[6] For an in-depth description of the 2019 bill and its fate, see our earlier alert on that topic. "The Massachusetts Legislature Hits the Pause Button on Comprehensive Consumer Data Privacy," 02/07/2020, available at: https://www.pierceatwood.com/alerts/massachusetts-legislature-hits-pause-button-comprehensive-consumer-data-privacy.

[7] An Act establishing the Massachusetts information privacy act, Bill H.142, 192nd (Current), available at: https://malegislature.gov/Bills/192/H142.

[8] Our prior alert provides a more in-depth analysis of the proposed law and its potential effects. "Massachusetts Data Privacy Bill Advances in Legislature," 02/14/2022, available at: https://www.pierceatwood.com/alerts/massachusetts-data-privacy-bill-advances-legislature.

[9] Joint Committee on Advanced Information Technology, the Internet and Cybersecurity, available at: https://malegislature.gov/Committees/Detail/J33/192.

[10] An Act establishing the Massachusetts Information Privacy and Security Act, Bill H.4514, 192nd (Current), available at: https://malegislature.gov/Bills/192/H4514.

[11] Joint Committee on Health Care Financing, available at: https://malegislature.gov/Committees/Detail/J24/192.

[12] 2021-2022 Session Legislative Deadlines & Significant Dates, available at: https://malegislature.gov/ClerksOffice/Senate/Deadlines.

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

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

[15] Connecticut Senate Bill No. 6, available at: https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF.

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

[17] Utah Senate Bill No. 227, available at: https://le.utah.gov/~2022/bills/static/SB0227.html.

[18] "FTC Explores Rules Cracking Down on Commercial Surveillance and Lax Data Security Practices," 08/11/2022, available at: https://www.ftc.gov/news-events/news/press-releases/2022/08/ftc-explores-rules-cracking-down-commercial-surveillance-lax-data-security-practices.

[19] Safeguards Rule, 16 CFR Part 314, available at: https://www.ftc.gov/legal-library/browse/rules/safeguards-rule.