Mass. Data Privacy Bill Poses Potential Class Action Risks

By **Peter Guffin, Donald Frederico and Melanie Conroy**

Peter Guffin

Donald Frederico

Melanie Conroy

Earlier this year, Massachusetts state senators introduced a consumer data privacy bill with a private right of action that could become the broadest in the country. The proposed law, An Act Relative to Consumer Data Privacy (S.120) would create a new category of litigation in local state and federal courts against businesses that collect personal information from Massachusetts consumers.[1]

S.120 was most recently referred to the Joint Committee on Consumer Protection and Professional Licensure. If enacted, S.120 would follow in the wake of a series of data privacy laws in Europe, California and Illinois that have dramatically increased data privacy litigation risks for companies that collect consumer data, bringing a potential surge of data privacy class actions to Massachusetts courthouses.

A Recent Wave of Consumer Data Privacy Legislation

In recent years, legislation aimed at protecting consumer data privacy has developed at an unprecedented pace. In 2016 the European Parliament and Council adopted the General Data Protection Regulation (EU Regulation 2016/679), which applies to all companies processing personal data of individuals in the European Union.[2] The GDPR created a private right of action for affected individuals to seek judicial remedy against infringing companies, including through collective action in member states.[3]

Shortly after the GDPR went into effect in May 2018, the California state legislature enacted the California Consumer Privacy Act (A.B. 375), which becomes effective on Jan. 1, 2020.[4] Under the CCPA, California consumers have a private right of action for data breaches resulting from a failure to implement and maintain reasonable safeguards if the business does not cure the breach after receiving presuit notice.[5]

The Illinois Biometric Information Privacy Act (740 ILCS/14), enacted in 2008, is an older statute that has had a recent resurgence.[6] The BIPA regulates the collection and storage of consumer and employee biometric information by companies doing business in Illinois. The BIPA provides a private right of action for any violation of the statute, with statutory damages available to plaintiffs even if no actual harm was suffered.[7]

Consumer data privacy proposals modeled on the GDPR, CCPA and BIPA have cropped up across the country at all levels of government, including in the U.S. Senate,[8] and state legislatures across the country,[9] including Massachusetts.

Key Features of the Massachusetts Consumer Data Privacy Bill

As proposed, S.120 would apply to for-profit businesses that collect personal information from Massachusetts consumers if they either have annual gross revenues over $10 million or derive more than 50% of annual revenues from third-party disclosures of consumer

information.[10] Notably, S.120 would apply to companies that do not meet the CCPA's higher revenue threshold of $25 million.[11] The bill adopts many key features from the CCPA and BIPA, with important distinctions.

Expansive Definition of Personal Information

S.120 broadly defines personal information as "any information relating to an identified or identifiable consumer."[12] Covered personal information includes "an individual's physiological, biological or behavioral characteristics" and any other information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or the consumer's device."[13]

Like the BIPA, S.120 specifies retina or iris scans, fingerprints, face and hand patterns, and voiceprints as biometric personal information.[14] However, S.120 expands on the categories in the BIPA, adding DNA, palm and vein patterns, voice recordings, keystroke rhythms, gait patterns, and sleep, health or exercise data that contains identifying information.[15] These additional categories have the potential to make Massachusetts' proposal significantly broader than BIPA in terms of the products and business activities within its reach, particularly in the health care, security, technology, energy and consumer electronics industries.

Consumer Rights to Notice, Disclosure, Deletion and Opt Out

S.120 would establish consumer rights similar to those created by the CCPA and BIPA. These rights include advance notice about the occurrence and business purpose of data collection and disclosure.[16]

The law would also create a consumer right to request copies of collected personal information, and details about collection sources and third-party disclosures.[17] Consumers could also direct the deletion of all such information[18] and opt out of third-party disclosures.[19] The proposed law would require companies to display "clear and conspicuous" links to opt-out forms on the homepage of their websites[20] and prohibit discrimination against consumers who exercise their rights under the law.[21]

Exceptions for Aggregate Data, Employee Information and Scientific Research

S.120 contains exceptions for activities that are especially relevant to the business and scientific communities in Massachusetts. These exceptions include:

- Clinical trials under the human subject protection requirements of the FDA.
- News gathering protected by the First Amendment.
- Aggregated consumer information from which individual consumer identities have been removed that cannot be re-identified and linked to an individual consumer.
- Compliance with legal obligations and proceedings, and cooperation with law enforcement.
- Collection or disclosure of employee information if "within the scope of its role as an employer," an important distinction between S.120 and BIPA, which applies equally to employees and consumers.[22]

Separately, S.120 exempts certain scientific research activities from the obligation to delete consumer information upon receipt of a verified request, but only if the consumer has provided informed consent and the research is in the public interest, is public or peer-reviewed, would be impaired by the deletion, and adheres to all other applicable ethics and privacy laws.[23] In this exempted research context, collected consumer information can be used only for research purposes consistent with the collection context and not for a commercial purpose, must be aggregated with a prohibition on re-identification, and must be protected by controls and processes that prevent inadvertent release and unnecessary access.[24]

Nonwaivable Private Right of Action for Statutory Damages Without Actual Harm

S.120 creates a private right of action with significant statutory damages that might be recoverable in class actions without a requirement that a plaintiff demonstrate actual injury to establish standing. Under the proposed statutory language, any "consumer who has suffered a violation of this chapter may bring a lawsuit against the business or service provider that violated this chapter."[25]

Critically, the statute directs: "the consumer need not suffer a loss of money or property as a result of the violation in order to bring an action for a violation of this chapter," and any "violation of this chapter shall constitute an injury in fact to the consumer."[26] This provision could remove what has been a critical hurdle for consumers attempting to recover damages in data privacy class actions to date, particularly in federal court following the U.S. Supreme Court's ruling in Spokeo Inc. v. Robins.[27]

A consumer who successfully brings a class action for violation of S.120 could recover up to $750 per consumer per incident (or actual damages, if greater), plus reasonable attorney fees and costs.[28] These statutory damages would be available regardless of the degree of alleged knowledge or intent on the part of the defendant.

Although the proposed law directs courts to consider "the nature and seriousness" and "willfulness of the defendant's misconduct," the bill does not specify that proving the defendant's culpable mental state is a requirement for recovery.[29] This could have dramatic ramifications for class action litigation risk and may exceed the scope of potential liability under the CCPA and BIPA. The CCPA consumer recovery is currently limited to certain data breaches and is capped at $750 per consumer per incident.[30]

The BIPA provides for consumer recovery for any violation of the statute, but specifies that a plaintiff must demonstrate the violation was negligent (with recovery capped at $1,000 per incident) or reckless or intentional (with recovery capped at $5,000 per incident).[31] S.120 contains neither of these limitations, and could therefore create broader categories of litigation risk.

To quantify the potential for enormous damages awards based on data breaches and other technical violations of the proposed law, consider that 391,532 Massachusetts residents were affected by data breaches in 2017(excluding the 2.9 million residents affected by the Equifax breach in 2017).[32] Based on these statistics, for data breaches alone (assuming those breaches indicate noncompliance with the proposed law's requirements), S.120 could expose businesses to more than $293 million in annual potential statutory damages in class actions filed in Massachusetts state and federal courts. The extent of the total class action liability risk posed by S.120, including damages for technical violations, is more difficult to quantify, but could eclipse these numbers.

A final and important aspect of S.120 affecting class action exposure is its apparent prohibition of liability waivers, arbitration provisions, class action waivers, limitation of liability clauses, jury trial waivers, and other contractual provisions that could limit a company's litigation risk. The proposed law expressly renders unenforceable "any provision of a contract or agreement of any kind that purports to waive or limit in anyway a consumer's right under this chapter," including any limitation on "any right to a remedy or means of enforcement."[33]

However, under recent Supreme Court precedent holding that state laws may not discriminate against arbitration, this provision's application to arbitration provisions is likely preempted by the Federal Arbitration Act.[34] Apart from this narrow federal preemption, other contractual provisions that limit litigation risk may be unavailable to companies defending against class actions under S.120, reducing the number of defense strategies available.

Conclusion

As a result of these key provisions in S.120, it is difficult to overstate the magnitude of class action litigation risk the proposed law may create for businesses collecting data from Massachusetts consumers. These businesses and their advisers should follow the progress of S.120 closely, and be prepared to creatively formulate litigation risk strategies to confront a potential new tidal wave of consumer class actions in Massachusetts. If the bill, or one like it, is enacted, business litigators will need to evaluate potential defenses to classwide liability under existing precedent and constitutional limitations.

Peter J. Guffin is a partner and chair of the privacy and data security practice, Donald R. Frederico is a partner and leads the class action defense practice, and Melanie A. Conroy is counsel at Pierce Atwood LLP.

[1] https://malegislature.gov/Bills/191/SD341.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A32016R0679.

[3] See GDPR at Articles 79-84; https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens/redress/can-i-claim-compensation_en.

[4] https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375.

[5] See CCPA at 1798.150.

[6] http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57.

[7] See BIPA at Section 20; Rosenbach v. Six Flags Entertainment Corp., 2019 WL 323902, 2019 IL 123186 (Ill. Jan. 25, 2019).

[8] https://www.congress.gov/bill/116th-congress/senate-bill/847/text.

[9] See https://iapp.org/news/a/us-state-comprehensive-privacy-law-comparison/.

[10] S.120 at Section 1(c).

[11] See CCPA at 1798.140(c)(1)(A).

[12] S.120 at Section 1(m).

[13] Id.

[14] S.120 at Section 1(b); BIPA at Section 10.

[15] Id.

[16] S.120 at Section 2.

[17] S.120 at Section 3.

[18] S.120 at Section 5.

[19] S.120 at Section 6.

[20] S.120 at Section 6.

[21] S.120 at Section 7.

[22] See S.120 at Sections 1(a), 1(m)(3), and 8.

[23] S.120 at Section 5(d).

[24] S.120 at Section 1(q).

[25] S.120 at Section 9.

[26] Id.

[27] 136 S. Ct. 1540 (2016).

[28] S.120 at Section 9.

[29] Id.

[30] See CCPA at 1798.150.

[31] See BIPA at Section 20.

[32] See https://www.bizjournals.com/boston/news/2018/03/30/mass-data-breaches-hit-record-high-last-year.html.

[33] S.120 at Section 14.

[34] See Kindred Nursing Ctrs. L.P. v. Clark, 137 S.Ct. 1421 (2017); AT&T Mobility LLC v. Concepcion, 563 U. S. 333 (2011).