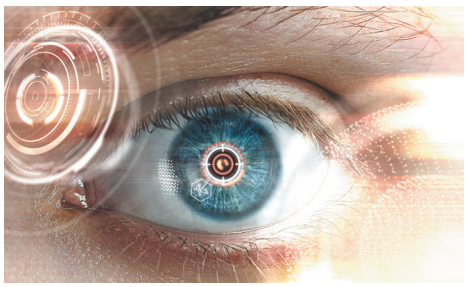
MASSACHUSETTS
LAWYERS WEEKLY

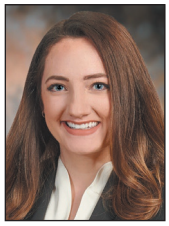
Volume 48
Issue No. 22
June 3, 2019

Consumer data legislation has business lawyers wary

Collection of biometric info regulated in measure

By Pat Murphy
pmurphy@lawyersweekly.com





"As the statute is written, any customer who has suffered a violation may bring a lawsuit. You do not need to show that you have suffered a loss of money or property."

— Melanie A. Conroy, Pierce Atwood LLP

A consumer data privacy bill working its way through the Legislature has defense attorneys on alert over the prospects of an expansive private right of action for violations of what would be the state's first comprehensive regulation on the collection and dissemination of personal information, including an individual's biometric data.

Introduced in January by Sen. Cynthia Stone Creem, D-Newton, S.120 calls for the enactment of the Consumer Data Privacy Act. The measure would require a covered business to provide detailed notice whenever it collects or intends to collect a consumer's personal information. Consumers would have the right to opt out of the collection of their data. Moreover, consumers could demand the "deletion" of any personal information collected by a business.

The bill features a private right of action that affords standing to sue without proof of actual harm. Class action defense attorney Melanie A. Conroy of Boston calls that provision "very broad" and posing a significant liability risk to the business sector.

"As the statute is written, any customer who has suffered a violation may bring a lawsuit," Conroy said. "You do not need to show that you have suffered a loss of money or property."

But Salem class action lawyer Matthew T. LaMothe sees the bill as simply leveling the playing field for consumers.

"The way in which someone's information can be collected and used can be defined by an agreement between a business and a consumer, which is really one-sided," LaMothe said. "This proposed bill gives the consumer the right not only to opt out, but also to be free from any penalty for exercising that right."

Although a defense lawyer himself, Boston data privacy and security attorney William S. Rogers Jr. finds fears that passage of S.120 would "open the floodgates" to class-action litigation to be overblown.

While it is appropriate to be concerned about the breadth of the private right of action and the availability of a class-action remedy under the bill in its current form, Rogers said, the legislative process is far from over.

"Let's not panic," he said. "A lot of things can happen to this piece of legislation between now and it passing both the Senate and the House. [And] would it be signed by the governor?"

Broad scope

After being introduced in January, S.120 was referred to the Joint Committee on Consumer Protection and Professional Licensure where it awaits action. If passed, the measure would add G.L.c. 93L, entitled "Consumer Data Privacy."

While it would be first-of-its-kind legislation for Massachusetts, Conroy said S.120 is modeled after the landmark California Consumer Privacy Act, which was enacted in 2018 and is set to go into effect on Jan. 1.

Because other jurisdictions have either passed or are considering similar data privacy laws, Conroy said in-house counsel are facing the challenge of keeping up with "a very fast-moving" regulatory landscape.

Like the CCPA, the Massachusetts legislation, if enacted, would provide the state with a "comprehensive" data privacy law, Conroy said.

"It really sets out consumer rights with regard to their data that is collected and shared with third parties by businesses that fit within the scope of the statute," she said.

The proposed statute covers businesses with either annual gross revenues in excess of $10 million or businesses that derive 50 percent or more of annual revenues from third-party disclosure of consumers' personal information. The bill provides certain exemptions for the collection of data by not-for-profit entities, as well as for employment, research and law enforcement purposes.

Rogers noted that the California law covers businesses with annual gross revenue in excess of $25 million, meaning the Massachusetts law has broader coverage.

Conroy pointed out that the lower threshold in Massachusetts means that some smaller companies that thought they were off the hook in terms of having to prepare for compliance with the California law may now need to pay close attention to the progress of the legislation.

Reprinted with permission from Lawyers Weekly, 40 Court Street, 5th Floor, Boston, MA 02108, (617) 451-7300 © 2019

"Personal information" is defined in S.120 as "any information relating to an identified or identifiable consumer," as well as 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."

Personal information does not include "publicly available" information. In turn, the proposed statute excludes from the term "publicly available" biometric information collected about a consumer without the consumer's knowledge.

Biometric information is broadly defined as "an individual's physiological, biological or behavioral characteristics, including an individual's DNA, that can be used, singly or in combination with each other or with other identifying data, to establish individual identity."

The bill specifies that biometric information includes "imagery of the iris, retina, fingerprint, face, hand, palm, vein patterns, and voice recordings, from which an identifier template, such as a faceprint, a minutiae template, or a voiceprint, can be extracted, and keystroke patterns or rhythms, gait patterns or rhythms, and sleep, health, or exercise data that contain identifying information."

The breadth of the statute is underscored by the examples of biometric information spelled out in the bill, Conroy said.

Private right of action

Proposed G.L.c. 93L, §2, provides that a business must notify consumers that it collects personal information "at or before the point of collection." Among other things, the statutory notice requires the identification of the categories of information to be collected, the "business purposes" for the data collection, and any third parties to which the data will be disclosed.

Section 3 would require businesses to respond in detail to "verifiable consumer requests" concerning the scope of the collection of their personal information.

Section 5 guarantees the consumer the right to request that a business delete any personal information collected about the consumer, and §6 similarly gives consumers the right to opt out of third-party disclosures of their personal information.

Conroy called the bill "forward-looking" in the sense that it allows the consumer to opt out of future data collection, and "backward-looking" by allowing the deletion of personal information collected in the past.

The bill also includes a non-retaliation provision, barring businesses from discriminating against consumers because they exercised any of their rights under the statute.

As a litigator, Conroy finds striking the broad private right of action guaranteed under the bill. Section 9 of the measure gives any consumer suffering a violation the right to bring a lawsuit against the transgressing business.

Rogers is similarly troubled that the bill in its current form provides that a mere violation of the statute would constitute an "injury in fact," giving a plaintiff standing to sue.

The bill provides that a "violation of this chapter shall constitute an injury in fact to the consumer who has suffered the violation, and 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."

But LaMothe said the proposed statutory language is consistent with the Supreme Judicial Court's recognition in medical monitoring cases that an increased risk of harm can be a harm in itself. LaMothe noted, too, that the bill echoed the recent amendments to the state's data breach law, which impose an obligation on businesses to provide free credit monitoring whenever a data breach includes a Social Security number, regardless of actual harm.

With the passage of S.120, consumers would be entitled to recover either $750 per incident or their actual damages, whichever is greater. In addition, the proposed bill authorizes the recovery of attorneys' fees and costs.

Finally, S.120 explicitly recognizes that the consumer's rights under the statute cannot be waived.

"Any provision of a contract or agreement of any kind that purports to waive or limit in any way a consumer's rights under this chapter, including, but not limited to, any right to a remedy or means of enforcement, shall be considered contrary to public policy and shall be void and unenforceable," the bill states.

No sure thing

In March, Rogers participated in a panel discussion on trends in domestic legislation at the RSA Conference, a data privacy and security industry convention held annually in San Francisco. In handicapping the chances of passage of S.120, Rogers said there are lessons to be learned from the state of Washington's recent failure to enact its own version of the Massachusetts bill, the Washington Privacy Act.

According to Rogers, the Washington bill was broader than the Massachusetts bill now on the table, the one exception being that it did not authorize a private right of action, leaving enforcement to the state's attorney general. On the other hand, the Washington bill was more onerous because it required covered businesses to prepare annual detailed risk assessments concerning the protection of personal data in their possession.

"That's not something that even California requires," Rogers said.

Like the Massachusetts bill, the Washington bill was introduced in January. But it has already been shelved. According to Rogers, the Washington bill "sailed" through the state Senate but died in committee when not enough votes could be mustered in the House.

Rogers said the fate of the Washington measure is typical of many "high-stakes" pieces of legislation and could foreshadow the fate of S.120.

"You had very strong privacy lobby wanting a very restrictive measure, and a very powerful hi-tech business lobby that was intimately involved in crafting the legislation," Rogers said. "When it got down to brass tacks, some of the rifts between those constituencies couldn't be resolved."

The Massachusetts bill in its current form provides that it would take effect Jan. 1, 2023. The bill's sponsor, Sen. Creem, a Boston lawyer, did not respond to a request for an interview.

Reprinted with permission from Lawyers Weekly, 40 Court Street, 5th Floor, Boston, MA 02108, (617) 451-7300 © 2019