Biometric Information Privacy Protection Act

Description

By Colin Coleman, John Ottaviani, and Brian Reilly

Privacy protection continues to be a theme at the Rhode Island General Assembly. As we reported in our April 1, 2019 Client Alert, which can be read here, the "Consumer Privacy Protection Act" was introduced on March 29, 2019 proposing more stringent requirements on businesses that collect and retain consumers' personal information.

More recently, on April 3, 2019, state representatives introduced 2019 — H 5945, the "Biometric Information Privacy Protection Act" (the "Act"), which, if enacted, would regulate the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and biometric information.

Biometric information is a personal identifier that is unique to an individual. Examples include a retina or iris scan, fingerprint, voiceprint, or a face scan. The Act would seek to protect individuals from breaches of biometric data by mandating certain procedures governing disclosure, retention, and destruction.

In essence, the Act would require any "private entity" to: (1) inform individuals before collecting their biometric information that their biometric information is being collected and to inform them in writing of the specific purpose and length of time for which their biometric information is being collected, stored, and used; (2) obtain an individual's written consent before collecting his or her biometric information; and (3) adopt a written retention policy specific to biometric information that establishes a retention schedule and guidelines for permanently destroying biometric information when the initial purpose for collecting the biometric information has been satisfied or within three (3) years of the individual's last interaction with the private entity, whichever occurs first. The Act would define a "private entity" as any individual, partnership, corporation, limited liability company, association, or other group, however organized; but it does not include any state or local government agency.

The Act would provide individuals with a private right of action against any private entity that does not comply with the Act's provisions. A determination that a private entity is in violation of the Act would result in the aggrieved individual recovering up to $5,000 and reasonable attorneys' fees and costs from the private entity.

If the new law passes, employers would be required to provide notice to employees and obtain consent before collecting and using biometric information. For example, in the workplace employers are increasingly requiring employees to use biometrics such as fingerprints or retina scans to log into computer systems and to access data stored on those systems and in the cloud.

This Client Alert is intended to provide a high-level overview of the proposed Act. Should the Act be enacted, the Act's final version may contain different and/or additional provisions than those contained within its present form. We will provide updates if and when any new developments arise.

Thank you to our Associate Joshua D. Xavier and our Law Clerk Krystal Medeiros for their assistance in preparing this article. If you would like to discuss your company's data privacy or cybersecurity compliance, please contact Colin A. Coleman, John E. Ottaviani, or Brian Reilly at Partridge Snow & Hahn LLP.

Date Created
April 8, 2019