New Jersey Law Journal
STATEWIDE LEGAL AUTHORITY SINCE 1878
An ALM Publication
MONDAY, JUNE 27, 2019 NJLJ.COM

New Jersey Eyes Regulation of Biometric Data

By Molly McGinley, Loly Tor and Erinn Rigney

SHUTTERSTOCK

As the use of biometrics becomes more widespread, concerns about privacy have increased alongside the growing trend. Biometric data generally means data generated by analysis of an individual's biological characteristics, such as retina or iris scan, fingerprint, voiceprint, handprint, facial geometry, or other unique biological patterns or characteristics that identify a specific individual. Biometric data can be collected from individuals as they go about their daily lives, from accessing their mobile device, asking Alexa or Siri about the weather, authorizing a withdrawal from an ATM, passing through airport security, and even when attending a concert or sporting event at Madison Square Garden. Since 2008, use of facial recognition and other biometric information collection systems has been common in the public sector. In the private sector, biometric information collection is equally prevalent, including, for example, the use of fingerprint scans to lock and unlock smartphones, facial recognition-based tagging features in digital photo applications, and the collection of such information for employment and security applications.

With daily headlines reporting on, and stoking fear of, large-scale data breaches, increasing public concern about the privacy and security of biometric data is unsurprising. The vast repositories of biometric information collected through these myriad systems may be particularly attractive to hackers because our biometric characteristics are generally immutable. The use of biometric information has grown exponentially in the past 10 years, with more and more businesses, employers, and governmental agencies employing technology to capture and use individuals' biometric information for a wide-range of purposes. Spiceworks, an IT marketplace for the technology industry, reported that nearly 90% of businesses will utilize biometric authentication by 2020, up from 62% in 2018. In 2018, the biometric market revenue sat at $4.9 billion dollars for the United States alone, and the financial services industry had the highest usage, followed closely by the technology

industry, and governmental agencies (Statista.com).

Legal Landscape

At the federal level, bills addressing biometric privacy have been proposed, but not advanced. Recently, in March of 2019, Senators Roy Blunt (R-MO) and Brian Schatz (D-HI) introduced a bill entitled the Commercial Facial Recognition Privacy Act (CFRPA), which would prevent businesses from collecting facial recognition data on consumers or using such data without their authorization. In introducing CFRPA, co-sponsor Schatz stated, "[o]ur faces are our identities. They're personal. So the responsibility is on companies to ask people for their permission before they track and analyze their faces." Senator Blunt further noted that "[c]onsumers are increasingly concerned about how their data is being collected and used, including data collected through facial recognition technology," and "[t]hat's why we need guardrails to ensure that, as this technology continues to develop, it is implemented responsibly." In addition to requiring permission to obtain facial recognition data, CFRPA would require facial recognition providers to meet data security, minimization and retention standards as determined by the Federal Trade Commission and the National Institute of Standards and Technology, which would be promulgated within 180 days of the act's enactment. As the bill is in its early stages, it is unclear if it will be successful. However, given the heightened concerns over data security and the widespread use of biometric information in commercial, employment and government settings, federal regulation may be fast-approaching.

Though no biometric privacy legislation has been passed in New Jersey, the state was poised to be a leader in biometric regulation with a proposed bill (A.B. 2448) back in 2002, six years before biometric privacy legislation was first passed in the United States. A.B. 2448 defined "biometric identifier" as a "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry" and proposed requiring advance authorization from an individual before obtaining biometric identifiers for a commercial advantage. Further, A.B. 2448 addressed concerns related to the sale, lease or other disclosure of biometric identifiers and would have required individual consent to such action outside of a few limited exceptions.

As is common in current biometric legislation, A.B. 2448 required persons who possessed a biometric identifier of an individual to protect and store it with the same reasonable care as taken for confidential information. For violations, the proposed civil penalties were capped at a hefty $25,000 per violation. Finally, A.B. 2448 included provisions addressing governmental entities and imposed similar consent requirements before such entity could sell, lease or otherwise disclose a biometric identifier subject to individual consent, law enforcement or permitted uses under federal or state law. In terms of enforcement, A.B. 2448 included a private right of action for both injunctive relief as well as actual damages incurred including costs and attorney fees. Though A.B. 2448 was reported on favorably by the Assembly Homeland Security and State Preparedness Committee and unanimously passed by the Assembly, it did not gain traction in the New Jersey Senate and failed to move out of the Judiciary Committee.

Fast-forward 16 years, and the New Jersey legislature is considering a similar bill, introduced in both the Assembly (A.B. 4640) and the Senate (Senate Bill No. 3153), which would require certain businesses involved in the collection of personally identifiable information to establish notification protocols and security standards. Additionally, as did A.B. 2448 in 2002, A.B. 4640 provides a private right of action. The bills were introduced in October 2018, and were transferred to the Assembly Homeland Security and State Preparedness Committee and the Senate Commerce Committee in January 2019. If passed, New Jersey would join Illinois and its Biometric Information Privacy Act ("Illinois BIPA"), Texas with its Capture or Use of Biometric Identifier statute, and Washington with its Biometric Identifiers law—the three states that currently have biometric privacy laws in place.

Of the three biometric information laws currently in effect, only Illinois BIPA provides for a private right of action. For context, since June 1, 2017, more than 250 class actions have been filed under Illinois BIPA, and the number is quickly growing. In the past few years, other states have considered (but have not passed) laws governing the collection and use of biometric information, including Alaska (H.B. 72, 30th Leg., Reg. Sess. (Alaska 2017)), New Hampshire (H.B. 523, 2017 N.H. H.R., Reg. Session (N.H. 2017)), and Connecticut (H.B. 5522, 2017 Gen.

Assemb., Reg. Sess. (Conn. 2017)). And in 2018, Arizona, Florida and Massachusetts became the latest states to propose legislation addressing the issue of biometric privacy.

Though A.B. 4640 does not require an individual's consent, it does require notification to consumers when personally identifiable information (PII), which includes biometric data, is collected. The proposed language demonstrates the extent of advancements in the field of biometrics since the prior legislation was introduced. For example, under A.B. 4640, "biometric data" includes an individual's physiological, biological or behavioral characteristics, such as an individual's deoxyribonucleic acid (DNA), fingerprint, voice print, retina or iris image, or other unique physical representation that can be used, singly or in combination with each other or with other identifying data, to establish an individual's identity. A.B. 4640 would cover entities that do business in New Jersey, excluding federal and state agencies and their contractors and subcontractors, and that:

(i) have an annual gross revenue of $5,000,000 or more; (ii) derive 50 percent or more of its annual revenue from selling the personally identifiable information of data subjects; or (iii) alone or in combination, annually buys, receives, sells, or shares for commercial purposes the personally identifiable information of at least 25,000 data subjects.

Entities collecting information covered under A.B. 4640 will be required to provide individuals advance notice about the different categories of PII being collected, the method of collection, the business purpose and legal basis for processing such information, any third parties with which the entity may share the PII and any profits derived from such disclosure, and contact information for an individual at the entity responsible for the data collection. In addition to pre-collection notification, A.B. 4640 also mandates that at the point at which PII is obtained, the covered entity must provide information to the individual regarding the time period for which PII will be stored and the individual's right to request access to his or her PII. A.B. 4640 allows an individual to request a copy of his or her PII that was obtained and processed, as well as the ability to opt out of such collection subject to certain exceptions. A.B. 4640 requires that covered entities maintain an information security program that meets the requirements for any information security program required under federal law, such as for personal health information under the Health Insurance Portability and Accountability Act or, if applicable, industry standards. What is markedly absent is any specific requirement pertaining to the storage of consumer biometric information, given the dearth of such regulation at the federal level.

In terms of violations, A.B. 4640 provides that it will be an unlawful practice if a covered entity fails to comply with any of its provisions and such failure results in the unauthorized access and exfiltration, theft or disclosure of an individual's PII. A.B. 4640 provides for a private right of action, and imposes a civil penalty of "not less than $100 and not more than $750 per data subject per security incident, or actual damages, whichever is greater." Unique to A.B. 4640 is a 30-day cure period that may include a form of alternative dispute resolution.

Conclusion

Though the fate of A.B. 4640 remains unclear, biometric information and the privacy of such information is becoming a focus for regulation within New Jersey and throughout the United States. Given the current legal landscape, businesses that collect or process biometric information should at a minimum evaluate their current practices as they relate to biometric information collection, storage or use. In light of the legislative developments in New Jersey, businesses employing such technology, both those located in the state or simply conducting business there, may also be well served by drafting and implementing policies and procedures to protect biometric information that are compliant with existing and anticipated state statutes, as potentially applicable.

Molly McGinley *is a partner with K&L Gates in Chicago,* ***Loly Tor*** *is a partner in the firm's Newark office, and* ***Erinn Rigney*** *is an associate in the Chicago office.*