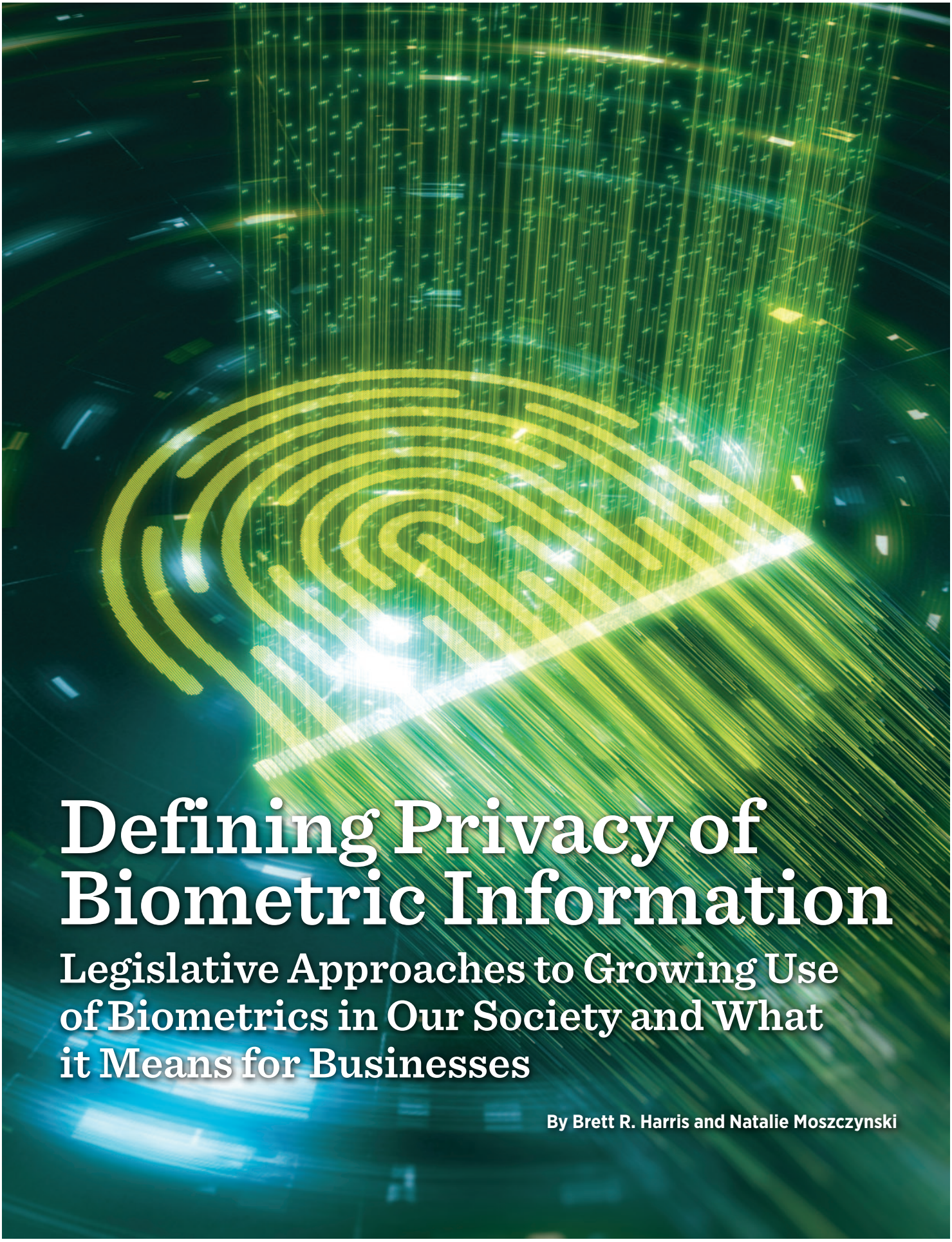

Defining Privacy of Biometric Information

Legislative Approaches to Growing Use of Biometrics in Our Society and What it Means for Businesses

By Brett R. Harris and Natalie Moszczynski

The use of biometric identifiers is not a new concept. The sci-fi and action-thriller media of the late 20th century touted retinal scans as a means to access bank vaults and facial recognition to track the location of villains as spy gadgets, which didn't truly exist in day-to-day life. Nowadays, these concepts are no longer futuristic and unrealistic, and instead are entirely believable and in use. Biometric information use ranges from medical practices to security and police agencies, from employment agencies to social media companies, and is even collected at amusement parks.

Following this uptick in biometric data collection, there also has been an increase in biometric data privacy laws both enacted and proposed, along with an increase in legislation to ensure adherence and protect consumers. Currently a dichotomy exists where some states have created their own tailored legislative mechanisms to protect consumers specifically with respect to biometric information, whereas other states incorporate biometric information as part of their definitions of what consumers are protected from in already existing privacy laws. Since New Jersey clients may be affected by this patchwork of nationwide laws, this article addresses this issue and sets forth an overview of the intersection of privacy and biometric data laws.

What is Biometric Information

The legal definition of biometric information or identifiers varies by state. As of now, no overarching federal regulation of biometric information exists. The only federal privacy mechanism that the government may apply is Section 5 of the Federal Trade Commission Act which applies to unfair or deceptive acts or practices in commerce.[1]

States have taken it upon themselves to pass legislation defining biometric data, whether including it as a lone definition or expanding existing definitions of personal information to include biometric identifiers. Biometric information can be generally described as metrics of physical personal characteristics that belong to each individual such as, but not limited to, the sound of one's voice, a fingerprint, or a photo of a face or retina. A sample of how biometric information and biometric identifiers are defined in the first biometric legislation, Illinois' Biometric Information Privacy Act (BIPA), is as follows:

> 'Biometric Identifier' means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry. Biometric identifiers do not include writing samples, written signatures, photographs, human biological samples used for valid scientific testing or screening, demographic data, tattoo descriptions, or physical descriptions such as height, weight, hair color, or eye color.... 'Biometric Information' means any information, regardless of how it is captured, converted, stored, or shared, based on an individual's biometric identifier used to identify an individual. Biometric information does not include information derived from items or procedures excluded under the definition of biometric identifiers.[2]

Each state appears to define biometric data differently. While BIPA has a very extensive definition of biometric information in its legislation, states that have included biometric information in existing laws have a tendency to more generally explain biometrics. This is not always the case, but is more likely when no current biometric specific legislation is in place. For example:

Vermont

As part of its consumer protection privacy laws, Vermont refers to biometric information within the definition of "brokered personal information," which is a computerized data element about a consumer meant for the dissemination to third parties. Biometric data falls under a subset of brokered personal information defined as "unique biometric data generated from measurements or technical analysis of human body characteristics used by the owner or licensee of the data to identify or authenticate the consumer, such as a fingerprint, retina or iris image, or other unique physical representation or digital representation of biometric data."[3]

BRETT R. HARRIS, *is a shareholder on the Business Law team at Wilentz, Goldman & Spitzer, P.A. Known as a Business, Nonprofit and Technology Attorney, she is admitted in New Jersey and New York with a broad-based general corporate practice consisting of both transactional matters and client counseling on everyday business matters with a focus on technology and IP issues. She also has a particular focus of representing nonprofit organizations, foundations and tax-exempt entities.*

NATALIE MOSZCZYNSKI *is an associate on the Business Law Team with Wilentz, Goldman & Spitzer, P.A., where she focuses her legal practice in health law, corporate law and cannabis law.*

California

California is the most inclusive. It deems biometric information to be a varietal of personal information.[4] However, the California legislature took the additional step of stating that while personal information is typically information that is not publicly available, biometric information is an exception, and it cannot be derived off of publicly available information even if such public access exists. The definition of biometric information in the California Consumer Privacy Act is as follows:

> ...an individual's physiological, biological or behavioral characteristics, including an individual's deoxyribonucleic acid (DNA), that can be used, singly or in combination with each other or with other identifying data, to establish individual identity. Biometric information includes, but is not limited to, 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.[5]

Virginia

The Virginia Consumer Data Privacy Act (VCDPA) will come into effect on January 1, 2023, and defines biometric data as "data generated by automatic measurements of an individual's biological characteristics, such as a fingerprint, voiceprint, eye retinas, irises, or other unique biological patterns or characteristics that is used to identify a specific individual. 'Biometric data' does not include a physical or digital photograph, a video or audio recording or data generated therefrom, or information collected, used, or stored for health care treatment, payment, or operations under HIPAA."[6]

Due to the prevalence with which such information is being obtained and stored, states have been passing legislation toward protecting their consumers by providing them with privacy rights over whether such information can be stored at all, what information may be collected, whether it may be provided to outside third parties, and what a company must do in the case of a security breach. The main difference between biometrics and certain other personal data currently protected in consumer privacy laws is that biometric information is specific to each person. For instance, while a password can be changed routinely and periodically, an individual's retina is much less likely to be altered. Biometric information is extremely individualized and thus can provide heightened security. But, it obviously comes with a heightened risk of vulnerability.

Current State of Biometric Information in Legislation

Only a few states have enacted legislation specific to biometric data collection, the consents required to collect such information, and penalties applicable if the laws are disregarded. These states include Illinois, Texas, and Washington. As mentioned earlier, some states have simply chosen to include biometric data restrictions into existing consumer privacy legislation, such as California, Virginia, Vermont, Maryland, Arkansas and Colorado. The benefit of having a biometric specific law is that it allows states to specify interaction with such data – especially since it is not always exclusively collected for security purposes. The biometric privacy laws institute regimes that require consent and notice be provided to consumers in a more stringent manner than those in existing consumer privacy legislation. States that have adopted biometric information as part of their definitions for personal identifying information tend to lack the specificity that biometric privacy laws maintain. For instance, Colorado states that "A covered entity that maintains, owns, or licenses personal identifying information (including biometric information) must develop a written policy for the destruction and disposal of all paper and electronic documents containing personal identifying information for the disposal of such information such as by shredding, erasing, or otherwise modifying the personal identifying information in the paper or electronic documents to be unreadable or indecipherable and must implement and maintain reasonable security procedures and practices."[7] Its consumer protection act does not require consent, nor does it require that the consumers potentially implicated must be notified of the written plan.

Biometric specific laws are being proposed throughout the country, including in states that have altered the definition of personal identifying information (also known as PII) in existing privacy legislation, because they recognize the sensitivity inherent to biometric identifiers and therefore provide greater restrictions for the security of the consumer. These restrictions tend to provide that consumers have a right to request disclosure of any and all personally identifying information, including biometric identifiers collected about the individual consumer, providing them with the ability to request deletion of such information, allowing them to opt out of provision of such information or its further sale to third parties, and giving consumers notice of the length of time for which such data will be maintained by a business.

Biometric Specific Legislation

Illinois was the first state to regulate how biometric data is used, collected, and disclosed by enacting BIPA in 2008.[8] A major stand out between the Illinois

law and other state laws is that the main method of enforcement of BIPA is through private right of action.

> BIPA requires any private entity that possesses biometric information or identifiers to develop and make publicly available a written policy that includes a retention schedule and guidelines for permanently destroying the biometric identifiers and biometric information when the initial purpose for collecting or obtaining it has been satisfied or within 3 years of the individual's last interaction with the entity, whichever occurs first. Furthermore, a private entity may not collect, capture, purchase, receive through trade, or otherwise obtain a person's or a customer's biometric identifier or information unless it first provides the individual with (1) a written statement that the data will be collected or stored and (2) detailing the specific purpose and retention period for the collected biometric data and (3) obtains a written release from the individual, and BIPA sets forth similar restrictions on a private entity's ability to disclose such information to outside parties.[9] It is important to note that BIPA grants aggrieved individuals a private right of action to sue for a mere violation of the law's requirements even if the individual does not suffer actual injury.[10]

Alongside BIPA, Texas has enacted the Texas Statute on the Capture or Use of Biometric Identifier[s][11] and Washington passed H.B. 1493 in 2017,[12] as the second and third states to enact such legislation, respectfully. The similarities among the three legislations are quite distinct. Biometric data may not be stored longer than is necessary after its initial purpose has been completed. Consent is another highly important condition, and although the process in which consent and notice are given vary by state, the fact that a consumer must agree to their biometric information being collected is an unchanging standard. The bills have several differences. The most noticeable is that BIPA offers private citizens a right to bring suit against companies that do not properly follow the provisions, whereas Texas and Washington have not included such language in their legislation, instead allowing only government actors to bring suit against companies.

New Jersey Proposals for Biometric Privacy Laws

So how do these laws affect New Jersey? The implementation of these regulations throughout certain states, along with the consistent proposals for similar New Jersey legislation, requires businesses to plan ahead to shield themselves from liability, whether it be from consumers across the country or even those in New Jersey. Over the past few years, New Jersey has proposed legislation to regulate collection, usage, and storage of biometric data.

One of the features of the most recently proposed New Jersey legislation has been that whenever biometric data is to be used, a written consent must be obtained from the individual providing data.[13] The New Jersey proposal follows similar requirements to those imposed by BIPA; however New Jersey has included that the written release provided by the individual must also be executed[14]—a feat that may not always be possible, especially in the context of who collects biometric data. For instance, biometric data often is collected through a smartphone via a fingerprint or facial recognition software or by a website. While it is in essence possible for that entity to send consent to be electronically signed by their consumer, it may make data collection an onerous process. Drawing out the process that people are currently used to, such as checking a box to agree to the terms and conditions of a website, may lessen a consumer's desire to read the terms to which they are consenting. But more difficult is the potential of biometric information being collected from the general public when, for example, they enter a store using biometric data collection as a form of security. It is highly unlikely that every passerby would execute a formal consent in such a scenario, making it difficult to implement use of such biometric data as a security method. Legislation could facilitate such usage by lowering the means of consent, such as by simplifying the standard to informed consent or reasonable notification so that any potential individual whose biometric information is being collected is aware of such. At the commencement of New Jersey's 220th Legislative Session in early 2022, proposed legislation regarding biometrics had yet to be sponsored.

Concerns For Businesses

Businesses have different concerns depending upon their intended use of biometric data. Many businesses have collected biometric information across state lines via the internet. Because of the expansiveness of today's internet age, should private actors abide by the strictest applications of BIPA to shield themselves from potential litigation risk? And how would they take steps to protect themselves from such liability? The first step a business should take is to investigate the extent of their insurance coverage to ascertain if it applies in the case of a security breach involving biometric information. Cybersecurity policies do not always assume the collection and maintenance of biometric information and the business should conduct a risk assessment with knowledge of any limits of coverage. Additionally, many states, albeit not all, extend their biometric privacy and consumer privacy legislations to all consumers, irrespective of where their biometric data is being processed,

collected, or maintained; therefore, if a business were to use the biometric information of an Illinois resident, they would find themselves subject to BIPA even without any presence of the business in Illinois.

Businesses have the option to act in the most conservative manner and abide entirely by the requirements of BIPA for private entities who are involved in processing biometric information. This would require stringent compliance, because "no private entity in possession of a biometric identifier or biometric information may disclose, redisclose, or otherwise disseminate a person's or a customer's biometric identifier or biometric information unless: 1) the subject of the biometric identifier or biometric information or the subject's legally authorized representative consents to the disclosure or redisclosure; 2) the disclosure or redisclosure completes a financial transaction requested or authorized by the subject of the biometric identifier or the biometric information or the subject's legally authorized representative; 3) the disclosure or redisclosure is required by State or federal law or municipal ordinance; or 4) the disclosure is required pursuant to a valid warrant or subpoena issued by a court of competent jurisdiction."[15]

Providing notice regarding the collection and maintenance of such information, ensuring reasonable security and maintenance of such information, and requiring consent from consumers are positive initial steps to take to encourage legal compliance as more states consider passing legislation regarding biometric information. ■

Endnotes

1. 15 U.S.C.A. § 45 (5).
2. 740 Ill. Comp. Stat. Ann. 14/10.
3. Vt. Stat. Ann. tit. 9, § 2430 (1)(A)(vi).
4. Cal. Civ. Code § 1798.140 (o)(1)(E).
5. Cal. Civ. Code § 1798.140 (b).
6. Va. Code Ann. § 59.1-571.
7. Colo. Rev. Stat. Ann. § 6-1-713; *See also* Colo. Rev. Stat. Ann. § 6-1-713.5.
8. 740 Ill. Comp. Stat. Ann. 14.
9. *Id*. at 14/15.
10. *Id*. at 14/20.
11. Tex. Bus. & Com. Code Ann. § 503.001.
12. Wash. Rev. Code Ann. § 40.26.
13. 2020 New Jersey Assembly Bill No. 3625, New Jersey 219th Legislature - Second Annual Session.
14. *Id*. at Section 4(b).
15. 740 Ill. Comp. Stat. Ann. 14/15.