To: New Jersey Law Revision Commission
From: Samuel M. Silver, Dep. Director
Re: Biometric Data Collection
Date: October 10, 2022

M E M O R A N D U M

Project Summary

As a routine part of daily life, biometric data is being collected by mobile devices, internet searches, security screenings, employee attendance devices, video doorbells, and home security systems. Biometric information consists of "data generated [through the] analysis of an individual's biological characteristics."[1] These biological characteristics may include "retina and iris scans, fingerprints, voiceprints," a record of a person's hand or face geometry, or other unique biological patterns or characteristics that identify a specific individual.[2] The rate at which this data is collected and the possibility of it being stolen and used for nefarious purposes led many states to consider its regulation.

Attempts to legislate in this area are not without their difficulties. In the wake of a global pandemic many businesses have developed contactless interactions as a primary means of interacting with employees and customers.[3] The methods of data collection, storage, and dissemination are changing at a rapid pace.[4] In the limited number of states that have enacted biometric privacy laws, legal questions involving standing, labor, preemption, and claim accrual are in the process of being decided by the federal courts.[5]

In *McDonald v. Symphony Bronzeville Park, LLC*, the plaintiff filed a putative class action lawsuit against the defendant and alleged that the collection biometric data - as part of a fingerprint timekeeping system - violated Illinois' Privacy Act.[6] The defendant filed a motion to dismiss and maintained that the Compensation Act was the exclusive remedy for "accidental injuries transpiring in the workplace and that an employee has no common law or statutory right to recover civil damages from an employer for injuries that occurred in the course of her employment.[7] Ultimately the Illinois Supreme Court considered the language of the State's Compensation Act and the Privacy Act to "determine whether the Compensation Act's exclusivity provisions bar an employee's claim filed in circuit court for statutory damages under the Privacy Act."[8]

---

[1] Molly McGinley, Loly Tor and Erinn Rigney, *New Jersey Eyes Regulation of Biometric Data*, NEW JERSEY LAW JOURNAL, June 27, 2019.
[2] A.B. 2448, 210th Leg., Sec. Annual Sess. (N.J. 2002).
[3] Zach Capers, Sr. Specialist Analyst, *How the Pandemic Changed Consumer Attitudes Toward Biometric Technology*, GETAPP, Feb. 21, 2022.
[4] Cynthia Lambert, *Data Security, Privacy, and the Law*, New Jersey State Library (Mar. 06, 2020).
[5] THE NATIONAL LAW REVIEW, Jackson Lewis Class Action Trends Report 2022: Biometric Privacy (Feb. 18, 2022).
[6] *McDonald v. Symphony Bronzeville Park, LLC*, No. 126511 slip op. at 2 (Ill. Feb. 3, 2022).
[7] *Id.* at 3.
[8] *Id.* at 6.

The issue presented in *McDonald* raised the question of "whether a similar issue exists at the intersection of New Jersey's privacy law and New Jersey's Workers' Compensation statutory exclusivity provisions."[9] As a preliminary matter, it should be noted that "New Jersey has no comprehensive data privacy laws."[10] Although an "Invasion of Privacy" statute may be found in the New Jersey Criminal Code, this statute does not address data privacy.[11] The statutes that mandate the reporting of data breaches[12] and the security of social security numbers[13] do not address the collection of personal identifiers.[14]

In the absence of a data privacy statute, Staff examined the New Jersey's Legislature's work involving biometric data; Illinois' Biometric Information Privacy Act (BIPA); the rise of class actions suits involving biometric data; the Illinois Supreme Court's decision in *McDonald*; an examination of those states with biometric data statutes; and New Jersey's latest legislation in this area of law to determine whether a *McDonald*-type issue exists in New Jersey.

Historical Background

• *New Jersey's Proposed Biometric Identifier Privacy Act of 2002*

For almost two decades, the New Jersey Legislature has been concerned with the methods by which biometric data is collected, and the protection of such data.[15] On June 13, 2002, A2448, entitled the "Biometric Identifier Privacy Act," was introduced in the New Jersey Assembly and referred to the Assembly Homeland Security and State Preparedness Committee.[16,17]

The introduction of this bill pre-dated the passage of the country's first biometric privacy legislation, in Illinois, by approximately six years.[18] The New Jersey bill that sought to define the term "biometric identifier,"[19] would have required advanced authorization from the individual before obtaining such identifiers for commercial advantage and would have addressed concerns about the sale of such data without consent.[20] In addition, the bill would have required those who collected biometric data to protect it and store it with the same care utilized for confidential information.[21]

---

[9] E-mail from Comm'r Bernard W. Bell to Laura C. Tharney, Exec. Dir., N.J. Law Revision Comm'n (Mar. 09, 2022) (on file with the NJLRC).
[10] *See* source cited *supra* n. 4. As of the date of this Memorandum, New Jersey has not enacted a comprehensive statute regarding data privacy protection.
[11] *Id.; see also* N.J. STAT. ANN. 2C:14-9 (West 2022) (making it a crime to surreptitiously observing, filming, photographing, or disclosing the intimate acts of another without consent).
[12] N.J. STAT. ANN. 58:8-163 (West 2022).
[13] N.J. STAT. ANN. 58:8-164 (West 2022).
[14] *See* source cited *supra* n. 4.
[15] *Id.*
[16] https://www.njleg.state.nj.us/bill-search/2002/A2448 (last visited Sept. 26, 2022).
[17] A.B. 2448, 210th Leg., Sec. Annual Sess. (N.J. 2002).
[18] *See* discussion *infra* p. 3 regarding the *Illinois' Biometric Information Privacy Act of 2008*. 740 ILCS 14/1 (West 2022).
[19] *Id.* (defining biometric identifier to include "retina or iris scan, fingerprint, voiceprint, or record of hand or face geometry.").
[20] *Id.*
[21] *Id.*

A violation of the proposed statute carried with it a civil penalty of not more than $25,000 for each violation.[22] In addition, the bill contained provisions to limit the possession, sale, lease, or disclosure of biometric information without the individual's consent.[23] If enacted, New Jersey would have been the first state to permit a right of private action that would have allowed the aggrieved individual to pursue both injunctive relief and actual damages – including attorney fees.[24] On September 12, 2002, the bill reported out of the Assembly Committee, with amendments.[25]

On September 23, 2002, A2448 passed the Assembly with a vote of 77-0-0.[26] The bill was received in the New Jersey Senate on September 26, 2002. Thereafter, it was referred to the Judiciary Committee where it failed to move out of committee.[27] Over the next five years, the Biometric Identifier Privacy Act would be introduced in the Legislature.[28] There is no indication that the Legislature sought to introduce the Biometric Privacy Act after 2007.

• *Illinois' Biometric Information Privacy Act of 2008*

Six years after New Jersey began efforts to enact legislation to protect biometric identifiers, Illinois became the first state to enact a Biometric Information Privacy Act (BIPA or the Act).[29] The BIPA, much like the cutting-edge bills that had been introduced in New Jersey, sought to regulate "the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information."[30]

The BIPA restricts the manner in which private entities may collect, retain, use, disclose, and destroy "biometric identifiers" and "biometric information."[31] The Act also requires that the entity collecting the information inform the individual, in writing, that their data is being collected or stored; the purpose of the data collection or use; and how long the data will be collected, stored, and used.[32] Pursuant to the Act, the data collector must also obtain a written release before collecting the data.[33] In addition, the BIPA requires consent before the collected data is disclosed and a retention schedule and guidelines must be publicly available in written form.[34] Finally, like the 2002 New Jersey statute, a violation is enforceable through a private right of action.[35] These

[22] *Id.*
[23] *Id.*
[24] *Id.*
[25] https://www.njleg.state.nj.us/bill-search/2002/A2448 (last visited Sept. 26, 2022).
[26] *Id.*
[27] https://www.njleg.state.nj.us/bill-search/2002/A2448 (last visited Sept. 26, 2022).
[28] A.B. 1194, 211th Leg., First Annual Sess. (N.J. 2004); A.B. 1373, 212th Leg., First Annual Session (N.J. 2006).
[29] 740 ILCS 14/1 (West 2022).
[30] 740 ILCS 14/5(g) (West 2022).
[31] 740 ILCS 14/1 et. seq.
[32] 740 ILCS 15(b).
[33] 740 ILCS 15(b)(3).
[34] 740 ILCS 15(d), (a).
[35] 740 ILCS 14/20 (West 2016).

actions include injunctive relief, and monetary damages for negligent and reckless violations of the act.[36]

• *The Rise in Biometric Litigation – Class Actions*

The private right of action provided for in the BIPA brought with it a wave of litigation. From 2008 until 2018, there were 163 BIPA class action lawsuits filed in Illinois.[37] In 2019, the number of BIPA suits rose to over 300. In 2021, "plaintiff's attorneys expanded the types of BIPA cases they [were] bringing beyond just claims involving the use of alleged biometric time clocks."[38] The cases involving biometric technology have expanded to include consumers, rather than being limited to employees.[39] Given the relatively recent development of this area of law, the question of what constitutes a "violation" of the BIPA has yet to be settled by the courts.[40]

Although BIPA statutes are in their infancy, large settlements have resulted from the enactment of these laws. In 2021, multi-million-dollar settlements were reached even in cases in which there was no allegation that the biometric data was compromised or accessed by an unauthorized third party.[41] A California federal court authorized a $65 million BIPA class action settlement "against a social medial company that allegedly collected users' facial geometry without following the requirements of BIPA."[42] In Illinois, a federal judge granted preliminary approval of a $92 million dollar BIPA settlement against another social media company that was alleged to have "surreptitiously harvest[ed] and profit[ed] from private information, including their biometric data, geolocation information, personally identifiable information and unpublished digital recordings."[43] These settlements "reflect the magnitude of possible liability under BIPA and the reach of the statute" in a legal landscape that is far from settled and frequently changing.

Recent Developments

• *McDonald v. Symphony Bronzeville Park, LLC*

In *McDonald*, the plaintiff alleged that the defendant (Symphony) had collected biometric data through the use of its timeclock system: without properly obtaining written releases from them before collecting, using and storing their biometric identifiers and the information; and had failed to inform them in writing that these identifiers were being collected and stored; failed to inform them in writing of the purpose and length of time for which their identifiers was collected, stored and used; and did not publicly provide a retentions schedule or guideline for destroying this information.[44] In this context, and in the absence of case law on the subject, of the Court was asked

[36] 740 ILCS 15(b) (allowing, liquidated damages of $1,000 or actual damages, whichever is greater, in instances of negligent violations; and liquidated damages of $5,000 or actual damages, whichever is greater, in instances of reckless violations).
[37] Joseph Stafford, Michael Duffy, and Ashley Conaghan, Bloomberg Law, *Illinois Supreme Court Finds Insurer Has Duty to Defend BIPA Suit* (June 18, 2021).
[38] THE NATIONAL LAW REVIEW, Jackson Lewis Class Action Trends Report 2022: Biometric Privacy (Feb. 18, 2022).
[39] *Id.*
[40] *Id.*
[41] *Id.*
[42] *Id.*
[43] *Id.*
[44] *McDonald*, slip op. at 3.

to consider whether the Illinois Workers' Compensation Act preempts a claim under the Privacy Act.[45]

The Court examined the law in two contexts and reasoned that, "the personal and societal injuries caused by violating the Privacy Act's prophylactic requirements are different in nature and scope from the physical and psychological work injuries that are compensable under the Compensation Act. The Privacy Act involves prophylactic measures to prevent compromise of an individual's biometrics."[46] As such, the plaintiff's "loss of the ability to maintain her privacy rights was not a psychological or physical injury that is compensable under the Compensation Act. . . [and] a Privacy Act violation is not the type of injury that categorically fits within the purview of the Compensation Act and is thus not compensable under the Compensation Act."[47]

Ultimately, the Illinois Supreme Court determined that the Compensation Act does not preempt the state's Biometric Information Privacy Act of 2008 and the matter was remanded to for further proceedings.[48]

50 State Survey

To this time, only three states have enacted biometric privacy laws - Illinois, Texas, and Washington.[49] In the first four months of 2022, seven states – California, Kentucky, Maine, Maryland, Massachusetts, Missouri, and New York - introduced biometric privacy laws.[50] These bills are generally based on Illinois's BIPA.[51]

Of those states with biometric laws, only Illinois provides individuals with a private right of action.[52] Although California has a Consumer Privacy Act (CCPA) that covers the protection of biometric data, that "act only provides a private right of action where the information was involved in an unauthorized exposure as a result of the business' failure to implement and maintain reasonable security procedures and the business' failure to take certain steps after receiving a consumer request."[53]

The American Law Institute

The American Law Institute (ALI) began its work on the *Principles of Law, Data Privacy* (*Principles*) in 2012.[54] The ALI's work is considered a "Principles" project because "area of law

---

[45] *Id.* at 5.
[46] *Id.* at 16.
[47] *Id.*
[48] *Id.* at 18.
[49] Molly S. DiRago, Kim Phan, Ronald I Raether, Jr., Robyn W. Lin, Troutman Pepper - Insights, *A Fresh "Face" of Privacy: 2022 Biometric Laws*,https://www.troutman.com/insights/a-fresh-face-of-privacy-2022-biometric-laws.html#:~:text=Introduction%3A%20Biometric%20Laws%20in%202022,Information%20Privacy%20Act%20(BIPA).
[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.*
[54] Solove, Daniel J. and Schwartz, Paul M., ALI Data Privacy: Overview and Black Letter Text (February 23, 2022). 68 UCLA Law Review 1252, 1261 (2022), Available at SSRN: https://ssrn.com/abstract=3457563 or http://dx.doi.org/10.2139/ssrn.3457563.

is so new that there is little established law" and the work can be used to "provide guidance for the evolution of the… law toward a more comprehensive and coherent approach."[55] The focus of the *Principles* is on "the sale and provision of goods or services and the functioning of institutions and organizations[,] including the employment of persons."[56]

The ALI's work commenced because "[c]ourts, legislatures, and policymakers were struggling to understand concepts such as personal identifiable information, the nature of privacy harms, the elements of meaningful consent for data collection, and the duties that should be owed a person whose personal information is processed."[57] The aim of the *Principles* is to bring consistency and depth to this burgeoning area of law characterized as "a bewildering assortment of numerous federal and state laws that differ significantly from each other"[58]

After seven years, the ALI approved the *Principles* to address the collection, use, and disclosure of personal data.[59]

The Uniform Law Commission

Staff also conducted a cursory examination of the work of the Uniform Law Commission's (ULI) work in this area. In 2021, the ULI promulgated the Uniform Personal Data Protection Act (UPDA).[60] The UPDA "applies fair information practices to the collection and use of personal data from *consumers* by business enterprises."[61]

The UPDA does not, however, address the collection of biometric data from employees as discussed in *McDonald.*

Pending Bills

• *Federal*

The subject of biometric data collection is being considered by the United States Congress. To this time, numerous bills have been introduced to Congress that reference the term "biometric."[62] Among these bills is one that seeks to protect personal data, including biometric information.

The "Data Protection Act of 2021" would "create in the Executive branch an independent agency to be known as the "Data Protection Agency," which shall regulate high-risk data practices and the collection, processing, and sharing of personal data."[63] The Data Protection Agency would,

---

[55] *Id.* at 1257-58.
[56] *Id.* at 1265.
[57] *Id.* at 1261.
[58] *Id.* at 1254.
[59] *Id.* at 1258, 1262.
[60] UNIF. PERSONAL DATA PROTECTION ACT (UNIF. L. COMM'N 2021).
[61] UNIF. PERSONAL DATA PROTECTION ACT, Accompanying summary (UNIF. L. COMM'N 2021), available at https://www.uniformlaws.org/HigherLogic/System/DownloadDocumentFile.ashx?DocumentFileKey=49202c5e-4ff6-8410-102b-2158d4937cd0&forceDialog=0.
[62] A search of the website Congress.gov using the term "biometric" in the search field, and limiters of Congressional years 1973-2022, a then the 2021-2022 session yielded twenty-seven results.
[63] S. 2134, 117th Congress (2022).

among other functions, "oversee the use of high-risk data practices, which include (1) using automated decision systems, such as machine learning; (2) profiling individuals on a large scale; (3) and processing personally identifying biometric information, such as genetic data."[64] The Agency is tasked with preventing and remediating specified privacy harms such as commercial practices that may lead to an adverse outcomes resulting from the collection, processing, or sharing of personal data.[65]

On June 17, 2021, this bill was referred to the Senate Commerce, Science, and Transportation Committee.[66] No legislative action has been reported regarding this bill since its introduction.[67]

• *New Jersey*

Since 2002, the New Jersey Legislature has consistently been working in the area of biometric privacy. A bill involving biometric data has been introduced in the Legislature virtually every year, with the exception of 2016-2017 legislative session.[68]

---

[64] *Id.*
[65] *Id.*
[66] https://www.congress.gov/bill/117th-congress/senate-bill/2134/committees?r=20&s=4 (last visited Sept. 28. 2022).
[67] *Id.*
[68] A.B. 2448, 210th Leg., Sec. Annual Sess. (N.J. 2002) (Biometric Identifier Privacy Act); A.B. 1194, 211th Leg., First Annual Sess. (N.J. 2004) (Biometric Identifier Privacy Act); A.B. 1373, 212th Leg., First Annual Session (N.J. 2006) (Biometric Identifier Privacy Act); A.B. 1447, 213th Leg., First Annual Session (N.J. 2008) (requiring local officer or employee employed by more than one local unit to submit timesheet to discourage double billing; establishes biometric fingerprint scanner grant program); S.B. 1326, 213th Leg., First Annual Session (N.J. 2008) (identical to A.B. 1447); A.B. 3440, 214th Leg., First Annual Session (N.J. 2010) (requiring use of biometric technology to verify coverage under Medicaid program); A.B. 1823, 215th Leg., First Annual Session (N.J. 2012) (requiring use of biometric technology to verify coverage under Medicaid program); A.B. 4306, 215th Leg., Sec. Annual Session (N.J. 2013) (prohibits the governmental collection of biometric identifiers without consent); A.B. 191, 216th Leg., First Annual Session (N.J. 2014) (prohibits the governmental collection of biometric identifiers without consent); A.B. 5969, 218th Leg., Sec. Annual Session (N.J. 2018) (restricts use of facial recognition technology and other biometric recognition by governmental entities); S.B. 4216, 218th Leg., Sec. Annual Session (N.J. 2018) (identical to A.B. 1447); A.B. 3283, 219th Leg., First Annual Session (N.J. 2020) ("New Jersey Disclosure and Accountability Transparency Act (NJ DaTA)"; establishes certain requirements for disclosure and processing of personally identifiable information; establishes Office of Data Protection and Responsible Use in Division of Consumer Affairs); A.B. 3625, 219th Leg., First Annual Session (N.J. 2020) (imposes moratorium on collection of biometric identifiers by public entities and requires the Attorney General to recommend appropriate uses; restricts private use of biometric information); A.B. 5211, 219th Leg., First Annual Session (N.J. 2020) (imposes moratorium on use of biometric surveillance systems technology by law enforcement agencies; establishes commission to recommend appropriate law enforcement uses for biometric surveillance systems technology); S.B. 116, 219th Leg., First Annual Session (N.J. 2020) (restricts use of facial recognition technology and other biometric recognition by governmental entities); S.B. 1917, 219th Leg., First Annual Session (N.J. 2020) (prohibits use of facial recognition or biometric surveillance systems on police body-worn cameras); A.B. 505, 220th Leg., First Annual Session (N.J. 2022) ("New Jersey Disclosure and Accountability Transparency Act (NJ DaTA)"; establishes certain requirements for disclosure and processing of personally identifiable information; establishes Office of Data Protection and Responsible Use in Division of Consumer Affairs); S.B. 365, 220th Leg., First Annual Session (N.J. 2022) (prohibits use of facial recognition or biometric surveillances systems on police body-worn cameras); S.B. 1715, 220th Leg., First Annual Session (N.J. 2022) (restricts use of facial recognition technology and other biometric recognition by governmental entities).

In 2018, sixteen years after introducing the "Biometric Identifier Privacy Act," Assembly Bill 4640, was introduced in the New Jersey Assembly and Senate.[69] If enacted, this bill would have required certain business to notify data subjects of the collection of personally identifiable information and would have established certain security standards for safeguarding the collected data.[70] After the Assembly bill was introduced, it was transferred to the Assembly Homeland Security and State Preparedness Committee.[71] No action or referral was made by the Senate regarding the bill introduced in that chamber.[72]

In 2022, the "New Jersey Disclosure and Accountability Transparency Act (NJ DaTA)" was introduced in the New Jersey Assembly.[73] If enacted, this bill will "establish certain requirements for disclosure and processing of personally identifiable information."[74] In addition, it will establish the Office of Data Protection and Responsible Use within the Division of Consumer Affairs.[75] As of January 11, 2022, this bill was referred to the Assembly Science, Innovation and Technology Committee for further consideration.[76] No further information about the status of this bill is available.

Conclusion

Over the past two decades, the New Jersey Legislature has become familiar with the issue involved in the collection of biometric data. The State is not alone in treading cautiously into this area of the law. To this time, the magnitude of possible liability and the reach of such statutes are amplified by the uncertain and undefined legal landscape.

Given the pace at which this legal landscape is changing, the Legislature's awareness of the subject matter, and the possible policy and fiscal ramifications of working in this field, Staff seeks the direction of the Commission regarding the need for additional research and outreach given the ongoing work of the Legislature in this area.

---

[69] A.B. 4640, 218th Leg., First Annual Sess. (N.J. 2018); S.B. 3153, 218th Leg., First Annual Session (N.J. 2018).
[70] *Id.*
[71] https://www.njleg.state.nj.us/bill-search/2018/A4640, (last visited Sept. 26, 2022).
[72] https://www.njleg.state.nj.us/bill-search/2018/S3153, (last visited Sept. 26, 2022).
[73] A.B. A505, 220th Leg., First Annual Sess. (N.J. 2022). The identical legislation was introduced as A.B. 3283 during the 2020-2021 legislative session with no further action after being referred to the Assembly Science, Innovation and Technology Committee.
[74] https://www.njleg.state.nj.us/bill-search/2018/A4640, (last visited Sept. 26, 2022).
[75] https://www.njleg.state.nj.us/bill-search/2018/A4640, (last visited Sept. 26, 2022).
[76] https://www.njleg.state.nj.us/bill-search/2022/A505 (last visited Sept. 26, 2022).