Litigation After Biometric Privacy Law Violations: Policyholder Victories and Their Implications

Cort Malone and Abigail Damsky*

Abstract: *States and cities, including New York City, are following Illinois' lead in enacting biometric privacy laws intended to protect employees' and consumers' biometric information. Courts, particularly in Illinois, have cleared up early uncertainty by ruling consistently in favor of policyholders where insurance coverage for violations of the Illinois Biometric Information Privacy Act (BIPA) is at issue. In response, insurance companies are implementing new measures to try to avoid paying for these liabilities. Another emerging area sure to lead to litigation involving privacy and data collection laws is artificial intelligence. As litigation involving privacy laws and artificial intelligence continues to proliferate, will businesses have the same success obtaining insurance coverage for these claims in courts throughout the country as policyholders have in BIPA-related insurance disputes in Illinois? While only time will tell, companies and policyholders should be examining their use of biometrics and artificial intelligence in the present, as well as their current and renewal insurance policies, to ensure adequate protection in the future.*

Introduction to Biometrics

Biometric identifiable information (BII) is an individual's physiological, biological, or behavioral characteristic, including DNA, that can be used to establish individual identity. Biometric information includes imagery of the iris, retina, fingerprint, and face, from which an identifier template, such as a faceprint or voiceprint,

Journal of Emerging Issues in Litigation / Winter 2024, Vol. 4, No. 1, pp. 19–27.

ISSN 2835-5040 (print) /ISSN 2835-5059 (online).

can be extracted. Biometrics are used as a more secure, and convenient, way to confirm identification—as opposed to easily hacked passwords. But there is a risk to using biometric data because such information cannot be replaced or changed if stolen. The frequent use of BII has led states to propose and pass biometric privacy laws to protect consumers and employees. Understanding biometric data and the laws designed to protect it is critical because the use of biometrics will only continue to increase.

Existing and Pending Biometric Privacy Laws

The seminal biometric privacy law in the United States is Illinois' Biometric Information Privacy Act (BIPA), which the Illinois legislature unanimously passed in 2008. BIPA allows individuals to control their own biometric data and prohibits private companies from collecting such data without following certain procedures, such as obtaining written consent. Critically, BIPA creates a private right of action for individuals subject to the law's provisions. It provides statutory damages of up to $1,000 for each negligent violation and up to $5,000 for each intentional or reckless violation. In 2019, the Illinois Supreme Court strengthened BIPA's reach when it held that actual harm is not required to establish standing to sue under BIPA.[1] This means that when an organization violates a procedural or technical aspect of BIPA, even when there is no specific injury or adverse effect, the individual whose biometric data was collected has standing to sue under the law.

At least six other states have followed Illinois' lead and passed biometric privacy laws designed to protect individuals from the collection, use, and sale of their personal biometric data. Eighteen states have pending legislation, some of which is similar to BIPA in that it would include a private right of action.

In 2021, the New York City Council amended New York City's administrative code to implement biometric privacy protections. It required businesses to notify customers of the use of biometric identifier technology and prohibited the sale of biometric identifier information. The city's Biometric Identifier Information Law (BII Law) addresses the collection and use of biometric identifier information by commercial establishments to track consumer activity. The BII Law also provides a private right of action that allows

for judgments of $500 for negligently sharing biometric information or failing to post signage that the commercial establishment is collecting biometric identifier information and $5,000 for the intentional or reckless sale of biometric information. While New York City passed the BII Law, New York State's biometric privacy law is still pending. Even though the City's BII Law is less rigorous than BIPA, the law ultimately may result in extensive litigation seeking massive damages.

When the BII Law was first passed, its impact was unclear because it provides a cure period for certain violations and allows for the collection of biometric data without written consent. In March 2023, however, a lawsuit was brought in federal court in New York against Amazon under the BII Law. The complaint in *Rodriguez Perez v. Amazon.com* alleged that Amazon violated New York City's BII Law because Amazon Go Stores in the city collected, used, retained, converted, and stored consumers' biometric identifying information. The plaintiff further alleged that Amazon tracks customers' behaviors and movements and then charges a customer's Amazon account for what they purchase in the store. The complaint also alleged that despite engaging in these acts and having an obligation to post signs disclosing the use of customer's biometric data, Amazon failed to post the required signs at its Amazon Go stores. Finally, the complaint alleged that after being notified of its violation, Amazon failed to take corrective measures or provide plaintiff with an express written statement that the violation had been cured. While the New York case was dismissed voluntarily in June 2023, plaintiffs re-filed a similar complaint in August 2023 in federal court in Seattle, naming both Amazon and Starbucks as defendants for their use of biometric technology. If plaintiffs survive the motions to dismiss the new lawsuit, the case will provide an example of how the BII Law could have more teeth than initially expected.

Insurance Coverage Litigation Over Biometric Privacy Law Violations Has Favored Policyholders

Liability arising from biometric privacy laws has resulted in significant litigation between policyholders seeking insurance

coverage for alleged violations of these laws and insurance companies arguing that such claims are not covered under the policies or otherwise excluded from coverage. This insurance coverage litigation, particularly regarding BIPA claims, has resulted in important decisions favoring policyholders. One of the first such decisions is *West Bend Mutual Insurance Co. v. Krishna Schaumburg Tan, Inc.*[2] *Krishna* involved an insurance dispute regarding an underlying BIPA lawsuit. The insurance company sought a declaration that it had no duty to defend or indemnify Krishna Schaumburg Tan Inc., arguing that the allegations did not fall within the type of injuries covered in the policy, and that even if the allegations did fall within the policy, a "violation of statutes exclusion" barred coverage. The *Krishna* court disagreed on both counts and found that the insurance company had a duty to defend Krishna against the underlying BIPA complaint.

Two recent decisions have continued the pro-policyholder trend of Illinois rulings, including refuting the exclusion cited by the insurance company in *Krishna* and two other commonly cited exclusions. In June 2023, the Seventh Circuit upheld a federal district court's finding that an insurance company has a duty to defend its policyholder accused of BIPA violations.[3] The case involved two class actions alleging that Wynndalco, an Illinois-based information technology services and consulting firm, violated BIPA.[4] The complaints asserted that Clearview AI allegedly extracted billions of photographs of individuals from online social media, content-sharing, and digital payment platforms to create a database of facial scans.[5] Wynndalco allegedly purchased and subsequently resold access to Clearview AI's database to the Chicago Police Department for a profit, violating BIPA.[6]

In *Wynndalco*, the Seventh Circuit found that catch-all language within an exclusion barring coverage for violations of specific laws concerning the dissemination of certain information was ambiguous and, therefore, injuries alleged in the underlying action potentially fell within the policy's coverage grant.[7] In so finding, the court determined that the "broad language of the catch-all exclusion purports to take away with one hand what the policy purports to give with the other in defining covered personal and advertising injuries."[8] *Wynndalco* has positive implications for policyholders

and its impact can be seen in subsequent case law, such as *Citizens Insurance Co. of Am. v. Mullins Food Products, Inc.*[9]

In *Mullins*, an Illinois federal court again sided with policyholders on an insurance company's effort to apply exclusions to BIPA claims. The insurance company issued an insurance policy to Mullins Food Products and sought a declaration that it had no duty to defend or indemnify Mullins in the underlying lawsuit alleging BIPA violations.[10] Mullins filed a counterclaim seeking a declaration that the insurance company was obligated to defend and indemnify Mullins and breached the insurance policy by failing to do so.[11]

Citing *Wynndalco*, the court determined that the underlying lawsuit fell within, or potentially within, the scope of the insurance policy.[12] Relying on *Wynndalco*, the court held that the exclusion for recording and distribution of information in violation of the law was ambiguous and, therefore, did not bar coverage.[13] Where "the exclusion all but eliminates coverage for certain claims that the policy by its express terms otherwise purports to cover, the exclusion is ambiguous."[14] The court also determined that the insurance company could not avoid coverage via an ambiguous employment practices exclusion, nor could it rely on an exclusion for access or disclosure of confidential information to avoid coverage. These two cases demonstrate the Illinois courts' trend of favoring policyholders in coverage disputes over claims related to the violation of biometrics privacy laws.

Insurance Companies' Response to BIPA Claims Should Serve as a Warning to Policyholders

While Illinois courts have refuted the typical exclusions cited by insurance companies to avoid BIPA claims, at least one court in another jurisdiction has gone the other way. A federal court in North Carolina applied a broader "recording and distribution" exclusion to deny coverage.[15] As a result, insurance companies may try to use forum shopping in states other than Illinois when litigating coverage for biometric privacy law claims. For example, in August 2023 Hartford Fire Insurance Company filed a declaratory

judgment action in the Eastern District of Virginia against the restaurant chain Five Guys after a proposed class accused Five Guys of collecting employees' biometric information without written consent in violation of BIPA.

The underlying class action complaint filed in the Northern District of Illinois in December 2022 alleged that Five Guys violated BIPA because it did not develop and publish written policies regarding the retention and destruction of biometric information and identifiers and failed to destroy biometric identifiers within the required time period. Five Guys tendered the underlying action, which subsequently was dismissed without prejudice, seeking defense and indemnity from the insurance company. Hartford then sought to have the Virginia federal court determine that the insurance company did not need to provide coverage to Five Guys. The *Impact Fulfillment* and *Five Guys* cases indicate that insurance companies may attempt to forum shop to avoid Illinois law and Illinois courts' tendency to side with policyholders.

In a further effort avoid liability for claims regarding alleged violations of biometric privacy laws, insurance companies have begun including specific biometric privacy claim exclusions in their policies. Some insurance companies have gone so far as to exclude claims under BIPA and any similar privacy protection laws under multiple different lines of coverage, while others have limited such exclusions to a single line of coverage such as Employment Practices Liability insurance. Certain insurance companies are attempting to include even broader exclusions regarding any claims for wrongful collection of data of any kind, which also would encompass biometric information. While these exclusions are becoming more common, they are not necessarily prevalent throughout the industry.

Accordingly, policyholders must confer with brokers to review existing policy terms and with experienced coverage counsel to assess whether courts in their jurisdiction have found coverage for claims alleging violations of biometric privacy laws. Policyholders should review their new or renewal policy terms and be aware of any effort by insurance companies to add more specific exclusionary language in an effort to limit coverage for these claims.

Biometric Privacy Laws and Insurance Litigation Can Help Inform the Future of Artificial Intelligence Claims and Coverage

Like biometrics, use of artificial intelligence (AI) is on the rise. A similar risk attaches to both biometrics and AI: the potential misuse of consumer or employee data. This risk already has resulted in hundreds of BIPA lawsuits, which may portend the future of AI-related litigation. While AI-based wrongful collection claims have not yet risen to the level of BIPA claims, at least two cases involving companies using AI technology have resulted in BIPA litigation that is instructive going forward.

In *Gutierrez v. Wemagine.AI LLP*,[16] the plaintiff brought a putative class action against defendant Wemagine alleging BIPA violations. Wemagine develops and owns a mobile application that uses AI to "extract a person's face from a photo and transform it to look like a cartoon."[17] Gutierrez alleged that Wemagine violated BIPA when it collected, captured, used, and stored his biometric data without a written release and through disclosure or dissemination of his biometric information without written consent. Wegamine filed a motion to dismiss for lack of personal jurisdiction. The court found that the "only connection between Wemagine and Illinois is Gutierrez . . . [t]here was no directed marketing specific to Illinois,"[18] and granted the motion to dismiss. This case is important for future claims under BIPA because it holds that a plaintiff's residence in the state alone is not a sufficient connection to Illinois for the purposes of BIPA to establish personal jurisdiction.

Another case where AI and biometrics intersected was the class action brought against the insurance company Lemonade for alleged BIPA violations. On August 20, 2021, Lemonade was sued in the Southern District of New York over its alleged collection and use of biometric data. The suit claimed that Lemonade collected and stored customers' retina scans, voice prints, and face scans without their knowledge or consent when they upload videos during the claim submission process and that, during this process, Lemonade's AI chatbot analyzes the submitted videos for fraud to "pick up non-verbal cues that traditional insurers can't." The complaint further alleged that Lemonade expressly and impliedly

assured its customers that it would not collect, store, analyze, or otherwise use their biometric data, but that it did so anyway. While admitting no wrongdoing, Lemonade ultimately settled the case for $4 million. This case demonstrates the overlap between AI and biometrics and how privacy laws like BIPA already are impacting both fields to the tune of multi-million-dollar settlements. Thus, companies using AI can look to biometric privacy litigation and the subsequent insurance coverage litigation as somewhat of a blueprint for how AI cases, with or without a biometric component, might be litigated. Understanding such risks, and the potential insurance pitfalls, can be critical to any business relying on either biometrics or AI—whether now or in the future.

Conclusion

Understanding biometric data is vital because its use is increasing through all facets of society. The frequent use of BII has led to states proposing and passing biometric privacy laws to protect consumers and employees. As more states pass these laws, it is critical not only to follow court decisions but also to understand how insurance companies are attempting to avoid liability for such claims. Further, policyholders would be wise to review their new or renewal policy terms and be wary of any effort by insurance companies to insert more specific exclusionary language to limit coverage for these claims going forward. As litigation over AI and biometrics continues to grow, smart businesses will need to put themselves in the best position to limit these liabilities and increase insurance recovery.

Notes

* Cort T. Malone (cmalone@andersonkill.com) is a shareholder in the New York and Stamford offices of Anderson Kill. His practice focuses on insurance coverage litigation and dispute resolution, with an emphasis on commercial general liability insurance, cyber insurance, employment practices liability insurance, advertising injury insurance, directors and officers insurance, and property insurance issues. Abigail

Damsky was a Summer Associate with Anderson Kill in the New York office and is currently a JD candidate at Benjamin Cardozo School of Law, set to graduate in 2024.

1. *See Rosenbach v. Six Flags Ent. Corp.*, 129 N.E.3d 1197 (Ill. 2019).
2. 166 N.E.3d 818 (Ill. App. Ct. 2020), *aff'd*, 183 N.E.3d 47 (Ill. 2021).
3. *Citizens Ins. Co. of Am. v. Wynndalco Enters., LLC*, 70 F.4th 987 (7th Cir. 2023).
4. *Id.* at 991.
5. *Id.* at 990.
6. *Id.* at 991.
7. *Id.* at 1004.
8. *Id.* at 998.
9. No. 22-CV-1334, 2023 WL 4865006 (N.D. Ill. July 31, 2023).
10. *Id.* at *1.
11. *Id.*
12. *Id.* at *5.
13. *Id.* at *8.
14. *Id.* at *10 (citing *Wynndalco*).
15. *Massachusetts Bay Ins. Co. v. Impact Fulfillment Servs., LLC*, No. 20-CV-926-WLO, 2021 WL 4392061 (M.D.N.C. Sept. 24, 2021) (holding, under North Carolina law, that the newer wording of the "Recording and Distribution of Material or Information" exclusion was broader than the exclusion in *Krishna* and thus barred coverage).
16. No. 21 C 5702, 2022 WL 252704 (N.D. Ill. Jan. 26, 2022).
17. *Id.* at *1.
18. *Id.* at *2.