Exclusionary Tech at Sports and Entertainment Venues: A Ticket Gets You In, But Your Face Could Get You Thrown Out

By Cort T. Malone, Shareholder, Anderson Kill P.C.

In June 2022, Madison Square Garden, the New York City sports and entertainment venue dubbed "the world's most famous arena," enacted a policy precluding attorneys from firms engaged in litigation against the company from attending events at its venues until the litigation is resolved. However, the company's method of enforcing the ban has become even more controversial.

The policy is enforced with facial recognition technology supported by computer software that can identify hundreds of lawyers through profile pictures on their firm's websites and use an algorithm to sort through images and suggest a match instantaneously. Facial recognition technology is legal in New York State and typically used in retail stores to identify shoplifters, airports to check in travelers, and casinos to identify cheaters. But MSG appeared to be the first venue to utilize the technology to exclude those taking a public stance against a company. In other words, MSG's use of the technology is punitive as opposed to protective, which questions such as who else may be precluded from entry and what, if anything, ticketholders can do in response.

Relevant New York Law, Court Rulings, and Legislative Response

In July 2021, New York City enacted a Biometric Identifier Information law, which makes it illegal to "sell, lease, trade, share in exchange for anything of value or otherwise profit from the transaction of biometric identifier information." The law applies to commercial establishments, and prohibits businesses from collecting biometric identifiable information – facial scans, fingerprints, etc. – without first posting a conspicuous sign at customer entrances. The signs must notify customers in plain and simple language how biometric identifiers are being collected or processed. The law also prohibits covered companies from selling leasing, trading, sharing, or otherwise profiting from that biometric information. Under the law, commercial establishments may face harsh penalties: up to $500 for each signage violation; up to $500 for each negligent sale violation; and up to $5,000 for each intentional or reckless sale violation. While the New York City law provides for a private right of action, it also provides a 30-day notice-and-cure provision.

In March 2023, a federal class-action data privacy lawsuit was brought against MSG and James Dolan (the owner of MSG, the New York Knicks, and New York Rangers) under Biometric Identifier Information law. MSG and Dolan moved to dismiss the case as not falling within the law because MSG does not profit in any way from the biometric information used via the facial recognition software. Although a magistrate judge initially recommended denying MSG's motion to dismiss the class action in January 2024, Judge Lewis Kaplan of the Southern District of New York ultimately agreed with MSG and dismissed the case in May 2024. Judge Kaplan found the plaintiffs' theory unpersuasive because it failed to explain how MSG violated the language of the law. Specifically, the

plaintiffs, who had purchased tickets to attend concerts at MSG, claimed that the venue collected their biometric information and then used it as part of a "litigation deterrent policy" that entailed "banning lawyers and their entire firms." As a private facility, MSG can set the terms of entry as it sees fit so long as those terms comply with the law. Like some other sports and entertainment venues, MSG uses facial recognition technology to enhance arena security measures and facilitate authentication of ticket holders. But the plaintiffs asserted that MSG's policy went too far in that the biometric policy unjustly confers an economic benefit because by deterring litigation against the company, the policy reduces MSG's litigation expenses. Plaintiffs also allege that MSG profited when it shared biometric data with a third-party vendor to assist in the banning.

Judge Kaplan found that this argument was incompatible with both the language of the New York City law and common sense, explaining that the law "does not prohibit companies from receiving any benefit, no matter how attenuated, from the sharing of biometric data." Rather, the law merely forbids profiting from the transaction itself, which the plaintiffs did not allege in their complaint. "To say that a company profits when it purchases a product or service defies common sense." Kaplan further questioned how the plaintiffs interpret the word "profit" given that the code "explicitly permits the collection and sharing of biometric data for commercial purposes provided that the public is warned." Thus, because the court held that MSG does not sell or profit from its customers' biometric data, its facial recognition technology, and use of same to exclude certain customers, is legal under current New York law.

Also in March 2023, a state appellate court upheld MSG's right to ban any attorneys involved in active lawsuits against the company or owners from attending Knicks and Rangers games, concerts, and other events at its venues. In response, New York legislators have proposed a bill to preclude MSG and other sports venues from restricting access to ticketed customers.

In January 2023, several New York state legislators introduced a bill that would severely limit MSG's attorney exclusion policy by including sporting events under a pre-existing state civil rights law that prevents places of public entertainment from wrongfully refusing admission to anyone with a valid ticket. The law currently includes theaters, concert halls, and opera houses, but does not include sporting events. One of the sponsors of the bill even wrote letters to NBA Commissioner Adam Silver and NHL Commissioner Gary Bettman urging them to sanction Dolan for using facial recognition software to exclude his courtroom adversaries. At present, the bill remains in committee in the New York legislature.

Another New York State bill that has remained in legislative limbo since being introduced back in January 2021 is the "Biometric Privacy Act" (the "BPA".) If passed, New York's BPA would require businesses to establish a written policy setting forth a schedule and guidelines for permanently destroying people's biometric identifiers and biometric information – either when the initial purpose for collecting or obtaining such identifiers or information has been satisfied, or within three years of the individual's last interaction with the private entity, whichever occurs first.

Like the NYC Biometric Privacy law, the BPA would include a private right of action, and preclude the sale, lease, trade, or otherwise profiting from the use of biometric information or identifiers. But crucially, unlike the City's law, the NY BPA, as currently drafted, contains no cure provision.

The implications of the BPA could be game changing. Without a cure provision, enterprising plaintiffs would not have to wait for companies to attempt to fix the alleged violation. This could lead to a massive upswing in lawsuits in New York, along with potential multi-million dollar damages awards.

Other states, such as, California, Texas, Virginia, and Washington have passed biometric privacy laws that do not contain a private right of action, but rather are enforced by the state's attorney general. Yet companies in states with biometric privacy laws that do not include a private right of action still should be concerned as state Attorneys General have aggressively pursued violations. Most notably, the Texas Attorney General has pursued claims against Meta, Facebook's parent company, for billions of dollars' worth of damages under the state's Capture or Use of Biometric Identifier Act ("CUBI"). Many other states across the nation are considering bills on biometric privacy protection as well.

Insurance Ramifications

As more state biometric privacy laws are passed, the risks for companies using biometric information continues to grow. These risks go beyond litigation over exclusion of customers from sports and entertainment venues, as class actions under biometric privacy laws have been brought against companies ranging from Amazon to Starbucks for allegedly unlawful collection and use of customers' biometric data. And more liability risk means more insurance coverage disputes are sure to follow.

While insurance companies' attempts to deny coverage for biometric claims on the basis of existing exclusions in liability policies initially mostly failed, these companies are now adding more specific exclusions for biometric privacy claims into their general liability and employment practices liability policies. Accordingly, when purchasing and renewing insurance policies, businesses at risk of liability under biometric privacy laws need to scrutinize their existing liability coverage and be wary of insurance companies adding such exclusions or making other impactful changes to policy language that may endanger coverage for biometric privacy claims.

Conclusion

As facial recognition technology expands, civil rights groups have expressed fear of the technology being used for malevolent purposes. Within the sports world, stadiums and venues have installed facial recognition technology to authenticate ticket holders' identities and get them inside quickly. The advantages of utilizing this technology in gameday operations include shorter wait times to enter venues and reduced ticket scalping. However, while most stadiums implement the technology to benefit spectators, MSG has shown that this technology also can be used to exclude patrons. Without state

laws governing the use of facial recognition technology in these spaces, owners will maintain this power of exclusion.

The proliferation of privacy rights litigation means that biometric damages claims are here to stay. Accordingly, policyholders – including those conducting business in New York – must take stock of both their current and potential future uses of biometric technology, and carefully review their insurance policies to ensure the best protection against biometric privacy law claims and the insurance companies seeking to avoid the resulting potential liability.