

**2025 – 2026 Legislative Memorandum**

**Subject:** An act to amend the civil rights law, in relation to prohibiting the use of biometric surveillance system or biometric surveillance information in places of public accommodation S.8004 (May) / A.6211 (Simone)

**Position:** SUPPORT

---

New Yorkers should be able to access public accommodations such as stores, restaurants, hotels, and venues without having their most sensitive personal information taken. Biometric surveillance technologies, which include face, voice, and gait recognition, directly threaten these abilities by enabling invasive powers to track who we are, where we go, and who we meet. S.8004 (May) / A.6211 (Simone) would ban the use of biometric surveillance technologies in places of public accommodation to ensure that all New Yorkers can freely move and associate without fearing that unreliable, racially-biased biometric surveillance systems will be used against them.

Biometric surveillance technologies are inaccurate and biased, especially as it pertains to women, children, and people of color.<sup>1</sup> When deployed in places of public accommodation, including as a means of permitting or barring access to a particular location, these inaccuracies can have far reaching consequences for people trying to go about their daily lives. For example, a Black teenager in Detroit was barred from entering a skating rink after the rink's facial recognition system misidentified the teen as a different patron.<sup>2</sup>

---

<sup>1</sup> Mei Wang and Weihong Deng, *Deep Face Recognition: A Survey*, 215 *Neurocomputing* 429 (March 14, 2021), <https://doi.org/10.1016/j.neucom.2020.10.081>; National Institute of Standards and Technology, *NIST Study Evaluates Effects of Race, Age, Sex on Face Recognition Software* (2019), <https://www.nist.gov/news-events/news/2019/12/nist-study-evaluates-effects-race-age-sex-face-recognition-software>; Joy Buolamwini and Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 *Proceedings in Machine Learning Research*, Conference on Fairness, Accountability and Transparency (2018), <https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf>; Joseph Goldstein and Ali Watkins, *She Was Arrested at 14. Then Her Photo Went to a Facial Recognition Database*, N.Y. TIMES, Aug. 1, 2019, <https://www.nytimes.com/2019/08/01/nyregion/nypd-facial-recognition-children-teenagers.html>.

<sup>2</sup> Dave Gershgorin, Black teen barred from skating rink by inaccurate facial recognition, THE VERGE (2021), <https://www.theverge.com/2021/7/15/22578801/black-teen-skating-rink-inaccurate-facial-recognition>.

Similarly in the UK, a woman was misidentified as a shoplifter and subsequently bag searched, asked to leave the store, and banned from all stores using the same technology—until the company acknowledged its mistake.<sup>3</sup> These biases in facial recognition technology risk excluding marginalized communities from everyday life.

The Federal Trade Commission (FTC) has recognized the dangers of facial recognition technology. In December 2023, the FTC banned the grocery chain Rite Aid from using facial recognition surveillance for five years after the company deployed the technology without reasonable safeguards.<sup>4</sup> Rite Aid’s facial recognition technology misidentified thousands of customers, disproportionately people of color and women, as previous shoplifters.<sup>5</sup> Suspected individuals were then followed around stores and searched, ordered to leave, or publicly accused of shoplifting.

Facial recognition technology is also ripe for abuse. Madison Square Garden (“MSG”) owner James Dolan has used facial recognition as a retaliatory tool to bar those against whom he has a personal vendetta from access to his facilities. In 2022, Dolan ejected a mother trying to watch the Rockettes show at Radio City Music Hall with her daughter’s Girl Scouts troop, simply because she was identified as an employee of a law firm engaged in litigation against MSG, even though she never directly worked on the lawsuit.<sup>6</sup> He later ejected someone for creating a t-shirt that made fun of him.<sup>7</sup> This sort of biometric retaliation sets a chilling precedent for how the rich and powerful can silence their opponents, critics, and those helping them fight for their day in court.

Stores are increasingly deploying facial recognition to monitor customers, screen against watch lists, and share information with other businesses, security firms, and law enforcement – without people’s knowledge and often resulting in misidentifications leading to accusations, searches, or access restrictions.<sup>8</sup> Pursuant to New York City’s limited Biometric Disclosure Law, Local Law 3 of 2021, retailers including Macy’s, Fairway, Whole Foods, and Wegmans have disclosed their use of biometric surveillance technology,

---

<sup>3</sup> James Clayton, “I Was Misidentified as Shoplifter by Facial Recognition Tech,” BBC, May 25, 2024, <https://www.bbc.com/news/technology-69055945>.

<sup>4</sup> Press Release, Federal Trade Commission, *Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards*, Dec. 19, 2023, <https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without>.

<sup>5</sup> *Id.*

<sup>6</sup> Sarah Wallace, *Face Recognition Tech Gets Girl Scout Mom Booted From Rockettes Show — Due to Where She Works*, NBC N.Y., Dec. 19, 2022, <https://www.nbcnewyork.com/investigations/face-recognition-tech-gets-girl-scout-mom-booted-from-rockettes-show-due-to-her-employer/4004677>.

<sup>7</sup> Mia Sato, *Madison Square Garden’s surveillance system banned this fan over his T-shirt design*, THE VERGE, Mar. 28, 2025, <https://www.theverge.com/news/637228/madison-square-garden-james-dolan-facial-recognition-fan-ban>.

<sup>8</sup> See Adam Satariano and Kashmir Hill, *Barred from Grocery Stores by Facial Recognition*, N.Y. TIMES, June 28, 2023, <https://www.nytimes.com/2023/06/28/technology/facial-recognition-shoplifters-britain.html>.

generating significant public surprise and disapproval.<sup>9</sup> However, mere notice falls far short of protecting New Yorkers from the civil liberties harms this technology enables. Additionally, some businesses may also use biometric surveillance technology to implement surveillance pricing, identifying individuals to change prices dynamically based on personal data, behavior, perceived willingness to pay, or other inferences.<sup>10</sup> These deployments point to Orwellian use cases where it will be impossible to move, purchase goods, and associate freely. The need for stronger privacy protections has never been clearer. New Yorkers should not be required to have their faces scanned and biometric data collected simply to buy groceries and other necessities of daily life.

With invasive and aggressive overreach from Federal immigration authorities, the collection of biometric data poses an unprecedented threat to New York's immigrant communities, many of whom are already afraid to go about their daily lives.<sup>11</sup> Immigrants should not have to face existential danger simply because they want to buy groceries. Immigration and Customs Enforcement (ICE) already uses facial recognition regularly and has been documented using tactics like accessing utility records to locate individuals for detention and deportation.<sup>12</sup> Stores actively partner with law enforcement to voluntarily share data about customers, and the same customer data can easily then be acquired by ICE if the agency simply submits a subpoena request. For example, ICE accessed millions of financial records from Western Union using administrative subpoenas<sup>13</sup> and purchases data it would normally need a warrant to access.<sup>14</sup> Even in so-called sanctuary jurisdictions, nothing prevents these sorts of private-public partnerships on immigration enforcement, actively putting immigrant neighbors in harm's way.

---

<sup>9</sup> Paige Oamek and Andrew Giambrone, *Not just Wegmans: More NYC retailers using facial recognition as tech outpaces law*, GOTHAMIST, Jan. 12, 2026, <https://gothamist.com/news/not-just-wegmans-more-nyc-retailers-using-facial-recognition-as-tech-outpaces-law>.

<sup>10</sup> See e.g., Alexis Benveniste, *Brooklyn Wegmans Pilots Facial Recognition Amid Fears of Dynamic Pricing*, EATER NY, Oct. 24, 2024, <https://ny.eater.com/2024/10/24/24278212/brooklyn-wegmans-facial-recognition>; Mayu Tobin-Miyaji, *Kroger's Surveillance Pricing Harms Consumers and Raises Prices, With or Without Facial Recognition*, EPIC, Feb. 14, 2025, <https://epic.org/krogers-surveillance-pricing-harms-consumers-and-raises-prices-with-or-without-facial-recognition/>.

<sup>11</sup> Luis Ferré-Sadurní, *An Immigrant Neighborhood Where Trump Made Inroads Now Fears ICE Raids*, N.Y. TIMES, Mar. 2, 2025, <https://www.nytimes.com/2025/03/02/nyregion/ice-raids-fears-corona-nyc-immigrants.html>; Miriam Jordan et. al, *Immigrant Communities in Hiding: 'People Think ICE Is Everywhere'*, N.Y. TIMES, Jan. 30, 2025, <https://www.nytimes.com/2025/01/30/us/immigrant-communities-hiding-ice.html>.

<sup>12</sup> Jude Joffe-Block, *Immigration agents have new technology to identify and track people*, NPR, Nov. 8, 2025, <https://www.npr.org/2025/11/08/nx-s1-5585691/ice-facial-recognition-immigration-tracking-spyware>; Nina Wang, Allison McDonald, Daniel Bateyko & Emily Tucker, *American Dragnet: Data-Driven Deportation in the 21st Century*, CENTER ON PRIVACY & TECHNOLOGY AT GEORGETOWN LAW, May 10, 2022, <https://www.americandragnet.org>.

<sup>13</sup> Matthew Guariglia, *Here's How ICE Illegally Obtained Bulk Financial Records from Western Union*, ELECTRONIC FRONTIER FOUNDATION, March 10, 2022, <https://www.eff.org/deeplinks/2022/03/heres-how-ice-illegally-obtained-bulk-financial-records-western-union>.

<sup>14</sup> Venkatesh, A.; Yu, L. *DHS is Circumventing Constitution by Buying Data It Would Normally Need a Warrant to Access*. ACLU. <https://www.aclu.org/news/privacy-technology/dhs-is-circumventing-constitution-by-buying-data-it-would-normally-need-a-warrant-to-access>.

Additionally, businesses using facial recognition are lucrative targets for identity thieves and hackers.<sup>15</sup> More dangerous than other personal identifiers like a social security number, biometric identifiers are static and are almost impossible to change.<sup>16</sup> When a hacker acquires another person's biometric data, it puts them at risk for identity theft for the rest of their lives.<sup>17</sup> In addition to the discrimination cited in the FTC's ban on Rite Aid's use of facial recognition technology, the Commission found that the company collected tens of thousands of photographs of shoppers without their knowledge or consent—worse still, Rite Aid stored these photos improperly and shared indiscriminately through a nationwide database.<sup>18</sup>

Visiting retail stores, restaurants, museums, entertainment venues, or healthcare sites should not automatically open one up for the collection of sensitive biometric information without prior informed consent and clear rules for access, use, security, retention, and deletion. Banning biometric surveillance in places of public accommodation is necessary to ensure New Yorkers can access these spaces without fear of being tracked or wrongly excluded from daily life. The NYCLU strongly supports passage of A.6211/S.8004.

---

<sup>15</sup> A. Dellinger, *Hackers Defeat Vein Authentication by Making a Fake Hand*, ENGADGET, Dec. 28, 2018, <https://www.engadget.com/2018-12-28-hackers-defeat-vein-authentication-by-making-a-fake-hand.html>.

<sup>16</sup> Anthony Ortega, *Do Biometrics Protect Your Data or Put Your Identity at Risk?*, SPICEWORKS, Oct. 8, 2018, <https://www.spiceworks.com/it-security/data-security/articles/do-biometrics-protect-your-data-or-put-your-identity-at-risk/>.

<sup>17</sup> *Is Your Identity at Risk from Biometric Data Collection?*, BEYONDTRUST (last accessed Oct. 6, 2022), <https://www.beyondtrust.com/blog/entry/is-your-identity-at-risk-from-biometric-data-collection>.

<sup>18</sup> Federal Trade Commission, *supra* note 4.