

2025-2026 Legislative Memorandum

Subject: An act to amend the executive law, in relation to prohibiting the use of biometric surveillance technology by law enforcement; establishing the biometric surveillance regulation task force; and providing for the repeal of certain provisions upon expiration thereof

S.5609 (Salazar) / A.1045 (Glick)

Position: SUPPORT

Biometric surveillance technologies, which include face, voice, and gait recognition, enable the invasive power to track who we are, where we go, and who we meet. But they are also highly flawed and rely on racially-biased systems. The use of these technologies by law enforcement presents a clear danger to all New Yorkers' civil liberties and threatens to erode our fundamental rights to privacy, protest, and equal treatment under the law.

S.5609 (Salazar) / A.1045 (Glick) would prohibit law enforcement agencies from using biometric surveillance technology and would create a task force charged with comprehensively studying the risks and impact of biometric surveillance by law enforcement. The NYCLU strongly supports this legislation and urges its immediate passage.

In the absence of state-mandated guidelines or restrictions on the acquisition and use of surveillance technologies, police departments throughout New York have been left to their own devices. Because departments have been free to set their own rules and because these departments so frequently attempt to evade public demands for greater transparency and oversight, the full reach of the surveillance state is unknown.

What we do know, however, is that the biometric surveillance systems currently being used by law enforcement agencies make countless New Yorkers, particularly people of color, less safe. One particularly concerning form of biometric technology, facial

recognition, is notoriously inaccurate, failing to correctly match faces to a comparison database, especially when it comes to identifying women and people of color.¹

When these systems are used by law enforcement, the real risks of misidentification cannot be overstated, especially considering the potential for lifelong consequences that can result from even a single encounter with law enforcement.² In April 2025, Trevis Williams—a 6’2”, 230-pound Black man—was wrongfully arrested by the New York Police Department (NYPD) for indecent exposure, accused of a crime committed by someone eight inches shorter and 70 pounds lighter. Despite location data showing he was miles away at the time, a faulty facial recognition match landed him behind bars for more than two days.³ Williams’s life and job prospects were put on hold for months due to his false arrest.

Even if the accuracy of the technologies were to improve, biometric surveillance systems would continue to operate with built-in bias. This is because the databases that the technologies rely on for comparators are, themselves, typically generated by law enforcement. For example, facial recognition systems may depend on mugshot databases, which—reflecting the disproportionate rate at which communities of color are policed—have many more faces of people of color in them. The biased policing practices that continue to disproportionately target and criminalize New Yorkers of color⁴ will mean that these technologies will end up being used disproportionately against people of color.⁵

While the risks of misidentification are obvious, the potential for these technologies to produce accurate identifications should also raise serious concerns in the law enforcement context. The widespread deployment of biometric surveillance systems would give law enforcement the ability to easily identify and track New Yorkers’ movements—where they go to school, which doctors they visit, which places of worship they attend, and which protests and demonstrations they decide to attend. The NYPD

¹ See, e.g., Joy Buolamwini & Timnit Gebru, Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 81 PROC. OF MACHINE LEARNING RES. 1, 1 – 15 (2018); see also Jacob Snow, Amazon’s Face Recognition Falsely Matched 28 Members of Congress With Mugshots, ACLU FREE FUTURE, July 26, 2018, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazon-face-recognition-falsely-matched-28>; cf. Paul Berger, MTA’s Initial Foray Into Facial Recognition at High Speed Is a Bust, WALL STREET JOURNAL, Apr. 7, 2019, <https://www.wsj.com/articles/mtas-initial-foray-into-facial-recognition-at-high-speed-is-a-bust11554642000>.

² See, e.g., Kashmir Hill, *Wrongfully Accused by an Algorithm*, THE NEW YORK TIMES, June 24, 2020, <https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html>, Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, The New York Times, December 29, 2020, <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

³ Maria Cramer & Kashmir Hill, *How the N.Y.P.D.’s Facial Recognition Case Fell Apart*, N.Y. TIMES, Aug. 26, 2025, <https://www.nytimes.com/2025/08/26/nyregion/nypd-facial-recognition-dismissed-case.html>.

⁴ See, e.g., Annual Stop-and-Frisk Numbers, NYCLU, <https://www.nyclu.org/en/stop-and-frisk-data> (last visited Dec. 9, 2025) (demonstrating that police stop, detain, frisk, and arrest Black and brown people at disproportionate rates).

⁵ See, e.g., Kashmir Hill, *Another Arrest, and Jail Time, Due to a Bad Facial Recognition Match*, N.Y. TIMES, Dec. 29, 2020, <https://www.nytimes.com/2020/12/29/technology/facial-recognition-misidentify-jail.html>.

already has more than 20,000 cameras integrated into its Domain Awareness System,⁶ and the Department continues to introduce even more cameras in the form of officer body-worn cameras and unmanned drones. It also does not shy away from utilizing social media photographs: In August of 2020, the NYPD used facial recognition software to identify a Black Lives Matter activist during a protest against police brutality through a photo from his Instagram account.⁷

Given the NYPD's long and troubling history of engaging in surveillance tactics that have targeted political dissent, criminalized communities of color, and singled out Muslim New Yorkers for suspicionless surveillance solely on the basis of their religion, New Yorkers should be equally concerned with the dangers that a hypothetically accurate biometric surveillance technologies would pose to our most fundamental rights and liberties.⁸

The mere act of collecting and storing biometric information is also dangerous. It requires the continual monitoring and collection of immutable characteristics, and any database of sensitive information is vulnerable to hacking and misuse. Unlike a password or credit card number, biometric data cannot be changed if there is a security breach. And what we have witnessed so far about police department policies and practices with biometric surveillance technologies should inspire little confidence in their ability to adequately guard against misuse.

Through litigation, the public has learned of the highly flawed, unscientific, and even unlawful practices that pervade the NYPD's facial recognition program since its inception over ten years ago. A 2019 report from the Georgetown Law Center on Privacy and Technology revealed that the NYPD engaged in such dubious tactics as uploading photographs of celebrity lookalikes in lieu of actual suspect photos, editing suspect photographs (including through effects that substantially alter the suspect's actual appearance) in order to generate a potential match, and apprehending suspects "almost entirely on the basis of face recognition 'possible matches'" without taking additional investigative steps to establish probable cause.⁹ Investigative reporters have uncovered even more failures by the NYPD to safeguard sensitive information and ensure officer adherence to even minimal standards on the use of biometric surveillance systems. It was revealed that the NYPD was including mugshots of juveniles and other sealed arrest

⁶ A Conversation with Jessica Tisch '08, HARVARD LAW TODAY (2019), <https://today.law.harvard.edu/a-conversation-with-jessica-tisch-08/>.

⁷ George Joseph & Jake Offenhartz, *NYPD Used Facial Recognition Technology In Siege Of Black Lives Matter Activist's Apartment*, GOTHAMIST (2020), <https://gothamist.com/news/nypd-used-facial-recognition-unit-in-siege-of-black-lives-matter-activists-apartment>.

⁸ A few examples of the many cases the NYCLU has litigated involving NYPD surveillance abuses include *Handschu v. Special Services Division* (challenging surveillance of political activists), *Raza v. City of New York* (challenging the NYPD's Muslim Surveillance Program), and *Millions March NYC v. NYPD* (challenging the NYPD's refusal to respond to a Freedom of Information Law ["FOIL"] request seeking information about whether the NYPD is using invasive technology to infringe on the protest rights of Black Lives Matter advocates).

⁹ Clare Garvie, Georgetown Law Center on Privacy & Technology, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, (2019), <https://www.flawedfacedata.com/>.

records in its facial recognition database.¹⁰ And despite the NYPD's explicit rejection, citing concerns about security and the potential for abuse, of software developed by Clearview AI that scrapes billions of photographs from social media platforms and other public sources, it has been reported that dozens of “rogue” officers have continued to use the software in more than 11,000 searches.¹¹ The reporting noted that “[i]t is not clear if the NYPD officers will face any disciplinary action for using the app,”¹² raising doubts about the willingness of the Department to enforce even its own rules and policies and raising concerns about their ability to safeguard sensitive biometric information going forward. The NYPD has also attempted to circumvent existing restrictions on the use of Clearview AI's facial recognition technology by outsourcing requests to other city agencies, such as the FDNY.¹³

The NYPD is far from the only agency deserving of closer scrutiny; the Staten Island DA purchased the software in 2019¹⁴ and as of 2020, more than 600 law enforcement agencies have secretly used Clearview AI's software, which includes biometric data on virtually everyone who has ever uploaded photos to Facebook, Instagram, Twitter, or Venmo.¹⁵ According to Clearview AI, the number of searches by law enforcement via their software doubled to 2 million in 2023.¹⁶ The widespread affordability and availability of biometric recognition technologies has led to deployments across New York State: by law enforcement agencies, in schools, places of entertainment, housing, airports, toll gantries, and public transport infrastructure. In one particularly alarming example, the MTA and the NYPD partnered with IBM to develop software to search for

¹⁰ Joseph Goldstein & 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-childrenteenagers.html>.

¹¹ See, e.g., Craig McCarthy, *Rogue NYPD Cops are Using Facial Recognition App Clearview*, N.Y. POST, Jan. 23, 2020, <https://nypost.com/2020/01/23/rogue-nypd-cops-are-using-sketchy-facial-recognition-app-clearview/>; Ryan Mac, Caroline Haskins & Logan McDonald, *Clearview's Facial Recognition App Has Been Used By The Justice Department, ICE, Macy's, Walmart, And The NBA*, BUZZFEED NEWS (2020), <https://www.buzzfeednews.com/article/ryanmac/clearview-ai-fbi-ice-global-law-enforcement>.

¹² *Id.*

¹³ See Samantha Maldonado, *NYPD Bypassed Facial Recognition Ban to ID Pro-Palestinian Student Protester*, THE CITY, (Jul. 18, 2025), <https://www.thecity.nyc/2025/07/18/nypd-fdny-clearview-ai-ban-columbia-palestinian-protest/>; *People v. Zuhdi A.*, No. CR-017044-24NY (Crim. Ct. Jun. 17, 2025), available at https://www.nycourts.gov/reporter/3dseries/2025/2025_51047.htm#:~:text=The%20defendant%20was%20identified%20in%20early%20June%202024,to%20dismiss%20the%20felony%20on%20September%2023%2C%202024.

¹⁴ George Joseph, *Staten Island DA Quietly Purchased Controversial Facial Recognition Software*, Gothamist (2021), <https://gothamist.com/news/staten-island-da-quietly-purchased-controversial-facial-recognition-software>.

¹⁵ Kashmir Hill, *The Secretive Company That Might End Privacy as We Know It*, N.Y. TIMES, January 18, 2020, <https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html>.

¹⁶ Suzanne Smalley, *Law enforcement searches of Clearview AI facial recognition doubled in past year*, THE RECORD, June 27, 2024, <https://therecord.media/clearview-ai-police-searches-doubled-2023>.

people by their skin color in the transit system.¹⁷ And Amazon Ring has partnered with hundreds of law enforcement agencies, including in New York City and on Long Island, to facilitate data sharing from privately installed devices to the police.¹⁸ Some of these systems offer or plan to offer other forms of biometric recognition such as affect recognition and aggressive or suspicious behavior detection, whose outcomes are severely inaccurate and plagued by disparate impacts for Black people.¹⁹

New Yorkers need not accept a dystopian future in which our most fundamental rights and liberties are jeopardized so that law enforcement can amass ever more powerful and invasive means of surveillance. S.5609 / A.1045 would prevent this dystopia from becoming reality. By banning the use of biometric surveillance by law enforcement, while providing thoughtfully crafted exceptions for internal department security systems that permit access to DNA and fingerprint comparison databases, this bill will ensure that New Yorkers are not surveilled and criminalized on the basis of flawed and biased technology. It will also ensure that New York does not continue to fall further and further behind, as other states like Maine, Vermont, and New Hampshire have already banned or sharply restricted the use of this technology.²⁰ Over twenty cities or counties have also recognized the severity of the threat the technology poses in the hands of law enforcement, including San Francisco, Boston, Baltimore, and Syracuse, NY.²¹

¹⁷ George Joseph & Kenneth Lipp, *IBM Used NYPD Surveillance Footage to Develop Technology That Lets Police Search by Skin Color*, THE INTERCEPT, Sept. 6, 2018, <https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search/>.

¹⁸ Hurubie Meko, What to Know Now That the N.Y.P.D. Is on Amazon's Neighborhood Watch App, N.Y. TIMES, Dec. 2, 2022, <https://www.nytimes.com/article/nypd-ring-app-surveillance.html>; Drew Harwell, *Doorbell-Camera Firm Ring Has Partnered With 400 Police Forces, Extending Surveillance Concerns*, WASHINGTON POST, Aug. 28, 2019, <https://www.washingtonpost.com/technology/2019/08/28/doorbell-camera-firm-ring-has-partnered-with-police-forces-extending-surveillance-reach>; Catherine Thorbecke, *Long Island Police Partner with Amazon's Ring to Crack Down on Porch Pirates*, ABC NEWS, Dec. 4, 2019, <https://abcnews.go.com/Technology/long-island-police-crack-porch-pirates-amazon-ring/story?id=67489715>.

¹⁹ See Lisa Feldman Barrett et al., *Emotional Expressions Reconsidered: Challenges to Inferring Emotion From Human Facial Movements*, PSYCHOLOGICAL SCIENCE IN THE PUBLIC INTEREST (2019), <https://journals.sagepub.com/eprint/SAUES8UM69EN8TSMUGF9/full> (last visited Feb. 10, 2020); LAUREN RHUE, *Racial Influence on Automated Perceptions of Emotions* (2018), <https://doi.org/10.2139/ssrn.3281765>.

²⁰ ME LD 1585, HP 1174, 130th Legislature, 1st Special Session, https://legislature.maine.gov/legis/bills/display_ps.asp?LD=1585&snum=130; N.H. Rev. Stat. § 105-D:2, <https://gc.nh.gov/rsa/html/vii/105-D/105-D-2.htm>; VT S.124 (2020), <https://legislature.vermont.gov/Documents/2020/Docs/BILLS/S-0124/S-0124%20As%20Passed%20by%20Both%20House%20and%20Senate%20Unofficial.pdf>.

²¹ Doulgas MacMillan, *These cities bar facial recognition tech. Police still found ways to access it.*, Wash. Post, May, 18, 2024, <https://www.washingtonpost.com/business/2024/05/18/facial-recognition-law-enforcement-austin-san-francisco/>; S.F. Admin. Code 19B (2019), <https://sfgov.legistar.com/View.ashx?M=F&ID=7206781&GUID=38D37061-4D87-4A94-9AB3-CB113656159A>; Boston Admin. Code 16-62, https://codelibrary.amlegal.com/codes/boston/latest/boston_ma/0-0-0-18988; Baltimore Council Bill 21-0001 (2021), <https://baltimore.legistar.com/LegislationDetail.aspx?ID=4749282&GUID=3605654F-5629-41A1-BD96-89946A2C32FB&Options=&Search=&FullText=1>; City of Syracuse, Executive Order No. 2, Policy in Regards to the Use of Surveillance Technology,

The unchecked use of biometric surveillance systems by law enforcement magnifies discrimination in areas like immigration, housing, and education. The continued use of these harmful and inaccurate technologies will serve only to further deepen the mistrust between police and communities, while doing nothing to advance public safety. S.5609 / A.1045 will put a stop to the most harmful of these technologies and will serve as a model for efforts across the nation to challenge discriminatory and abusive surveillance practices.

The NYCLU strongly supports S.5609 / A.1045 and calls for its swift passage.