Legislative Affairs
One Whitehall Street
New York, NY 10004
212-607-3300
www.nyclu.org

2019-2020 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.7572 (Hoylman) / A.9767 (Glick)

Position: SUPPORT

Biometric surveillance technologies, which include face, voice, and gait recognition, rely on flawed and 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.7572 (Hoylman) / A. 9767 (Glick) would prohibit law enforcement agencies from using biometric surveillance technology and would mandate a comprehensive study of 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]

---

[1] See 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/surveillancetechnologies/amazons-

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.

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 color[2] will mean that these technologies will end up being used disproportionately against people of color.

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' every 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 New York Police Department (NYPD) already has more than 20,000 cameras integrated into its Domain Awareness System,[3] and the Department continues to introduce even more cameras in the form of officer body-worn cameras and unmanned drones.

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.[4]

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

---

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.*, Annual Stop-and-Frisk Numbers, NYCLU, https://www.nyclu.org/en/stop-and-frisk-data (last visited Feb. 7, 2020) (demonstrating that police stop, detain, frisk, and arrest Black and brown people at disproportionate rates).

[3] A Conversation with Jessica Tisch '08, HARVARD LAW TODAY (2019), https://today.law.harvard.edu/a-conversation-with-jessica-tisch-08/ (last visited Feb. 7, 2020).

[4] 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).

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.[5]

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 records in its facial recognition database.[6] 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.[7] The reporting noted that "[i]t is not clear if the NYPD officers will face any disciplinary action for using the app,"[8] 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 is far from the only agency deserving of closer scrutiny; 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.[9]

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 people by their skin color in the transit

---

[5] Clare Garvie, Georgetown Law Center on Privacy & Technology, Garbage In, Garbage Out: Face Recognition on Flawed Data, (2019), https://www.flawedfacedata.com/ (last visited Feb. 7, 2020).
[6] 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.
[7] 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/.
[8] *Id.*
[9] 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.

system.[10] And Amazon Ring has partnered with hundreds of law enforcement agencies, including on Long Island, to facilitate data sharing from privately installed devices to the police.[11] 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.[12]

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.7572/A.9767 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 and 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.

S.7572/A.9767 would also establish a task force to further study the issue, with an explicit mandate to consider the impact of biometric surveillance on communities of color, LGBTQ and gender-nonconforming people, and people with disabilities, and whose appointed membership is to include experts in the fields of data privacy and security, civil rights and liberties, legal representation of low-income individuals and/or tenants, and criminal defense. These perspectives are essential voices in an arena that has largely been dominated by law enforcement and private industry.

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.7572/A.9767 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.7572/A.9767 and calls for its swift passage.

---

[10] 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/.

[11] 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.

[12] *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 (last visited Feb. 10, 2020).