BRENNAN
CENTER
FOR JUSTICE
at New York University School of Law

120 Broadway
Suite 1750
New York, New York 10271
646.292.8310 Fax 212.463.7308
www.brennancenter.org

Written Testimony of Laura Hecht-Felella
Legal Fellow, Liberty & National Security Program
Brennan Center for Justice at NYU School of Law
Before the
Committee on Housing and Buildings, Committee on Technology, and the Committee on Consumer Affairs and Business Licensing
October 7, 2019

Good afternoon members of the Committee on Housing and Buildings, Committee on Technology, and the Committee on Consumer Affairs and Business Licensing.

My name is Laura Hecht-Felella. I am a Legal Fellow with the Liberty and National Security Program at the Brennan Center for Justice.

Thank you Chairman Cornegy, Chairman Holden, and Chairman Espinal for holding this hearing and inviting the Brennan Center to testify.

The Brennan Center is a nonpartisan law and policy institute that seeks to improve our systems of democracy and justice. The Liberty and National Security Program in particular focuses on ensuring that government use of new technologies does not violate fundamental rights.

The Brennan Center commends the City Council on its commitment to addressing the growing prevalence of biometric identification technology in New York City. However, we must also express our disappointment that this commitment has not resulted in oversight of the New York City Police Department ("NYPD").

Meaningful efforts by the City Council to increase transparency of biometric identification technology in New York City must include the NYPD. The NYPD's expansive arsenal of surveillance technology includes several biometric tools like facial recognition, video analytics, and DNA databases. Attached to my testimony is a chart that the Brennan Center published this morning. It outlines the scope of the NYPD's surveillance capabilities, referencing documents obtained in Freedom of Information Law litigation and other publicly available information. Our chart identifies several technologies for which the NYPD has failed to provide even basic information about its policies. For many of its biometric tools, like facial recognition, the NYPD has failed to identify whether it has effective safeguards in place to protect New Yorkers' civil rights and privacy.

Biometric identification technology works by using algorithms to try and identify a person based on distinctive physical or behavioral characteristics.[1] Examples of these characteristics include someone's fingerprints, DNA, face, gait, or voice.[2]

For all of the possibilities that biometric identification technology poses, the truth is that many of these tools are error-prone and cannot reliably identify large swaths of New Yorkers.[3] In particular, facial recognition technology, which attempts to identify a person based on certain facial characteristics, is currently the focus of nationwide concern.[4] This is because facial recognition threatens to place people at unprecedented levels of surveillance as they move about their daily lives, but studies repeatedly find that the technology cannot reliably identify faces that are not white and male.[5] In particular, facial recognition software has been shown to have large error rates in identifying women, people of color, children, the elderly, and people with disabilities.[6]

In response to these concerns, several cities, including San Francisco, Oakland, and Somerville, have banned facial recognition by city agencies.[7] Other state-wide initiatives proposing partial bans or moratoriums are actively moving forward, including in New York and Michigan.[8] Within this regulatory environment, it is disappointing that the legislation proposed by the City Council does not address the unique concerns raised by the deployment of facial recognition by city agencies such as the NYPD.

It is especially concerning because there is a high risk of abuse. Biometric identification technologies make it possible to covertly monitor multitudes of people in public and private spaces at a low cost. This poses serious implications for our basic liberties, including the right to be free from unreasonable search and seizure, as well as freedom of speech, association, and expression.

---

[1] *Community Control Over Police Surveillance: Technology 101*, AMERICAN CIVIL LIBERTIES UNION, www.aclu.org/report/community-control-over-police-surveillance-technology-101.
[2] *Id.*
[3] Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, 81 PROCEEDINGS OF MACHINE LEARNING RESEARCH 1(2018), *available at* http://gendershades.org/overview.html; *see also* Salem Hamed Abdurrahim, *Review On The Effects Of Age, Gender, And Race Demographics On Automatic Face Recognition*, 34 THE VISUAL COMPUTER 1617 (2018), *available at* https://doi.org/10.1007/s00371-017-1428-z*;* Jacob Snow, *Amazon's Face Recognition False Matched 28 Members of Congress with Mugshots*, AMERICAN CIVIL LIBERTIES UNION (July 26, 2018), www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.
[4] *See* Coalition Letter to Elijah Cummings, Chairman, & Jim Jordan, Ranking Member, of the U.S. House Oversight and Reform Committee (June 3, 2019), *available at* https://tinyurl.com/y673fsbv (urging a federal moratorium on face recognition for law enforcement and immigration enforcement purposes); Nicole Martin, *The Major Concerns Around Facial Recognition Technology*, FORBES (Sept. 25, 2019), www.forbes.com/sites/nicolemartin1/2019/09/25/the-major-concerns-around-facial-recognition-technology/#2f3d39534fe3.
[5] Steve Lohr, *Facial Recognition Is Accurate, if You're a White Guy*, N.Y. TIMES (Feb. 2018), https://nyti.ms/2BNurVq.
[6] Buolamwini, *supra* Note 3.
[7] Rachel Metz, *Beyond San Francisco, More Cities Are Saying No To Facial Recognition*, CNN (July 17, 2019), www.cnn.com/2019/07/17/tech/cities-ban-facial-recognition/index.html.
[8] Elizabeth Kim, *Albany Lawmakers Introduce Bill Banning Landlords From Using Facial Recognition Technology*, THE GOTHAMIST (May 15, 2019), https://gothamist.com/news/albany-lawmakers-introduce-bill-banning-landlords-from-using-facial-recognition-technology; Steve Neavling, *House Bill Would Ban Facial Recognition Technology In Michigan*, METRO TIMES (July 11, 2019), www.metrotimes.com/news-hits/archives/2019/07/11/house-bill-would-ban-facial-recognition-technology-in-michigan.

Moreover, biometric identification technology is frequently being utilized in low income communities and communities of color, which are already subject to over surveillance.[9]

The NYPD is one of the largest and most technologically advanced police forces in the United States.[10] Unfortunately, it is not one of the most transparent. The NYPD has historically revealed details about its surveillance technologies only after costly Freedom of Information Law (FOIL) litigation, investigative reporting, or being court ordered.[11] This erodes public trust and can lead to abuses of constitutional rights.

For instance, the Brenan Center was party to a multi-year legal dispute with the NYPD to obtain information about the Department's use of predictive policing technologies beginning in June 2016.[12] The NYPD denied our initial FOIL request and subsequent appeal, forcing the Brennan Center to file a lawsuit.[13] In 2017, a judge finally ordered the NYPD to produce records about its testing, development, and use of predictive policing tools.[14] However, it took a full year for the NYPD to comply. Concerningly, the records we eventually obtained indicated that the NYPD had no policy in place to explicitly govern the use of predictive policing, or the sharing and retention of the data produced.[15]

In another example, after extensive FOIL litigation, Georgetown Law's Center on Privacy and Technology obtained records from the NYPD detailing worrying abuse of their facial recognition software. In one striking case, after the technology failed to produce a match for a suspected low-level shop lifter, detectives uploaded an image of similar looking celebrity instead. They sent the resulting matches from a compromised facial recognition analysis to investigating officers, who then used this faulty data to make an arrest.[16]

Similarly, this summer the New York Times reported that the NYPD has been uploading photos of children as young as eleven into its facial-recognition systems.[17] When questioned by reporters, several members of the City Council said they were unaware of the policy.[18] This is because the NYPD does not transparently report on what surveillance technology it is using, its efficacy, or how it stores, analyzes, or shares the information it collects.

---

[9] *Community Control Over Police Surveillance: Technology 101*, *supra* Note 1.
[10] *About NYPD*, NYC.gov, www1.nyc.gov/site/nypd/about/about-nypd/about-nypd (last accessed Oct. 3, 2019).
[11] Dustin Volz, *Privacy Group Sues NYPD For Release Of Facial-Recognition Documents*, REUTERS (May 2, 2017), www.reuters.com/article/us-usa-cyber-face-recognition-idUSKBN17Y1Z1.
[12] Rachel Levinson-Waldman & Erica Posey, *Court: Public Deserves to Know How NYPD Uses Predictive Policing Software*, THE BRENNAN CENTER FOR JUSTICE (Jan. 28, 2018), https://www.brennancenter.org/our-work/analysis-opinion/court-public-deserves-know-how-nypd-uses-predictive-policing-software.
[13] Rachel Levinson-Waldman & Erica Posey, *Predictive Policing Goes to Court*, THE BRENNAN CENTER FOR JUSTICE (Sept. 5, 2017), http://www.brennancenter.org/blog/predictive-policing-goes-court.
[14] *Supra*, Note 13.
[15] *Supra*, Note 12.
[16] *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEORGETOWN LAW'S CENTER ON PRIVACY AND TECHNOLOGY (May 16, 2019), https://www.flawedfacedata.com.
[17] Joseph Goldstein & Ali Watkins, *She Was Arrested At 14. Then Her Photo Went To A Facial Recognition Databa*se, N.Y. TIMES (Aug. 1, 2019), https://nyti.ms/2GEzuZ8.
[18] *Id.*

A strong local democracy like New York City requires at least a basic level of information about what its local police are doing and how they are doing it, particularly given New York City's history of discriminatory stop-and-frisk policies[19] and because reports show NYPD policing continues to target communities of color.[20]

The Public Oversight of Surveillance Technology (POST) Act, introduced by Council Member Vanessa Gibson, would require the NYPD to disclose basic information about the surveillance tools it uses and the existing safeguards to protect the privacy and civil liberties of New Yorkers.[21] The bill is supported by over half the City Council, with twenty-eight co-sponsors and endorsements from the Black, Latino/a, and Asian Caucus and the Progressive Caucus.

The POST Act is carefully drafted to ensure that the NYPD can continue to keep the city safe, while providing policymakers with the information necessary for effective oversight.[22] It requires the NYPD to issue privacy impact reports, like the reports already published by many federal agencies including Department of Homeland Security (DHS) and the Federal Bureau of Investigations (FBI).[23]

Several municipalities, including San Francisco, Oakland, Berkley, and Seattle have passed more stringent bills, including legislation that bars law enforcement from utilizing new surveillance technologies without City Council approval.[24]

Transparency and oversight are essential features of a strong democracy, and the Brennan Center commends the Council for addressing these critical and timely issues. However, is vital that any legislation requiring transparency on biometric identification technologies also applies to law enforcement.

Thank you again for the opportunity to testify today. I am happy to answer any questions.

---

[19] *See, e.g.*, *Floyd v. City of New York*, 959 F. Supp. 2d 540 (S.D.N.Y. 2013).
[20] *See, e.g.*, *Stop-and-Frisk in the de Blasio Era*, NEW YORK CIVIL LIBERTIES UNION (Mar. 2019), www.nyclu.org/en/stop-and-frisk-data (finding Black and Latino people were more likely to be frisked and, among those frisked, were less likely to be found with a weapon).
[21] New York City Council Int. 0487-2018, *available at* https://legistar.council.nyc.gov/LegislationDetail.aspx?ID=3343878&GUID=996ABB2A-9F4C-4A32-B081-D6F24AB954A0.
[22] For more on Public Oversight of Surveillance Technology Act see "The Public Oversight of Surveillance Technology (POST) Act: A Resource Page, available at www.brennancenter.org/analysis/public-oversight-surveillance-technology-post-act-resource-page.
[23] *Department of Justice/FBI Privacy Impact Assessments*, U.S. FEDERAL BUREAU OF INVESTIGATIONS, *available at* https://www.fbi.gov/services/information-management/foipa/privacy-impact-assessments; *Privacy Impact Assessments*, U.S. DEPARTMENT OF HOMELAND SECURITY, *available at* https://www.dhs.gov/privacy-impact-assessments.
[24] The Editorial Board, *San Francisco Banned Facial Recognition. New York Isn't Even Close.*, N.Y. TIMES (May 18, 2019), https://nyti.ms/2LTq80Q.