NYCLU
ACLU of New York

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

Testimony of Daniel Schwarz

On Behalf of the New York Civil Liberties Union

Before the New York City Department of Consumer and Worker Protection

Regarding the new rules to implement Local Law 3 of 2021

August 30, 2021

The New York Civil Liberties Union ("NYCLU") respectfully submits the following testimony regarding the new rules to implement Local Law 3 of 2021. The NYCLU, the New York affiliate of the American Civil Liberties Union, is a not-for-profit, non-partisan organization with eight offices throughout the state and more than 180,000 members and supporters. The NYCLU's mission is to defend and promote the fundamental principles, rights, and values embodied in the Bill of Rights, the U.S. Constitution, and the Constitution of the State of New York. The NYCLU works to expand the right to privacy, increase the control individuals have over their personal information, and ensure civil liberties are enhanced rather than compromised by technological innovation.

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 widespread use of these technologies 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.

In recognition of these harms, the New York City Council enacted Local Law 3 of 2021 ("LL 3") as a first step to diagnose the spread and use of these surveillance technologies in businesses. The law, which came into effect on July 9, 2021, takes a rudimentary approach to biometric surveillance technology, requiring certain "commercial establishments" that collect, use, or retain "biometric identifier information" from their customers to post notices at all customer entrances in a form prescribed by the New York City Department of Consumer and Worker Protection ("DCWP" or "Department"). In order for this law to not just be a mere rubber stamp on the use of biometric surveillance, it is incumbent on the Department to promulgate rules that, at the very least, give the public basic information about the technologies in use and any privacy policies that govern them.

Unfortunately, the proposed rules by the DCWP fall far short of that goal. The rules as drafted would not disclose any meaningful information and fail to notify customers in plain and simple language about the use and implications of biometric surveillance technologies.

The DCWP published a Biometric Identifier Information Disclosure sign template[1] on its website, which businesses simply have to add their names to and post at every entrance to fulfill the notice requirement. The 35-word notice is so ambiguous that it actively obscures any information value whatsoever from the disclosure. It lacks any specificity about the type of biometric data collection occurring, and does not include privacy policies covering the use, access, retention, deletion, sharing, and security measures governing that data – or where to find them. Further, the sign template lists only two examples of biometric identifier information: eye scans and voiceprints. Notably absent is any mention of facial recognition, which is the most prominent and newsworthy type of biometric data collection – and was the primary target of the Council in passing the underlying legislation. This focus on facial recognition can be seen in the legislative history, including in LL3/Intro. 1170-2018's summary, Committee reports, and minutes of the Council's Stated Meeting. Deliberately excluding the most widely known type of biometric identifier thwarts transparency and weakens the notice's potential impact.

It's also critical that businesses clearly disclose the specific types of biometric data collection they deploy, particularly as these technologies are notoriously inaccurate and racially biased. Numerous studies have shown that face surveillance technologies are particularly inaccurate for women and people of color.[2] And misidentifications have led to harassments, removals from establishments, arrests, and jail time.[3]

It has been practically impossible to find out whether businesses deploy biometric recognition technologies. In 2018, the ACLU asked some of the biggest retailers whether they

[1] Sign template, Biometric Identifier Information Disclosure, https://www1.nyc.gov/assets/dca/downloads/pdf/businesses/Biometric-Identifier-Information-Disclosure-Sign.pdf.

[2] See e.g., Cynthia M. Cook et al., *Demographic Effects in Facial Recognition and their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems*, 1 IEEE TRANSACTIONS ON BIOMETRICS, BEHAVIOR, AND IDENTITY SCIENCE 32–41 (2019); Joy Buolamwini & Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, PROCEEDINGS OF MACHINE LEARNING RESEARCH (2018), http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[3] See e.g., Dave Gershgorn, *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 (last visited Aug 20, 2021); 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 (last visited Aug 20, 2021); The Computer Got it Wrong: Why We're Taking the Detroit Police to Court Over a Faulty Face Recognition "Match," AMERICAN CIVIL LIBERTIES UNION, https://www.aclu.org/news/privacy-technology/the-computer-got-it-wrong-why-were-taking-the-detroit-police-to-court-over-a-faulty-face-recognition-match/ (last visited May 20, 2021).

use facial recognition: of nineteen retailers, only two answered.[4] In contrast to this, people clearly want transparency and control over their data: a recent survey shows that 69% of Americans believe that stores should inform customers about the use of facial recognition and 65% would want to have the choice to opt-out.[5] This becomes ever-more important as corporate and retail surveillance expand and allow for further data collection, correlation, and analysis, e.g. by combining someone's biometric data with other information such as their credit card, smartphone (through WiFi, Bluetooth, or other identifiers), customer loyalty card, other NFC-enabled devices, or even online activities.

The mere collection and storage of biometric information can also be harmful and lead to unforeseen consequences. 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 should inspire little confidence in many companies' ability to adequately guard against misuse.[6] Disclosing data policies and creating appropriate security mechanisms should be the baseline for anyone handling biometric data.

The DCWP proposed rules also give more leeway to businesses for the place of posting the sign than, for example, restaurants have for the posting of letter grade cards. Restaurants are required to post letter grade cards in a "conspicuous place where it is <u>visible to passersby</u> […] on the front window, door or exterior wall […] <u>within five feet</u> of the front door or other opening to the establishment where customers enter from the street, at a vertical <u>height no less than four feet and no more than six feet</u> from the ground or floor."[7] Additionally, letter grade cards have a much higher visibility and recognizability, given their colorful, conspicuous, large design elements; all qualities lacking in the Biometric Identifier Disclosure template sign, which is likely to not attract much attention and is designed to blend in.

Let's be clear; a sign is not a sufficient tool to reign in on facial recognition and other biometric surveillance tools by businesses. There's no substitute for individual, informed opt-in consent. But in the absence of other protections at the local, state, and federal level, the rules

[4] Jenna Bitar & Jay Stanley, *Are Stores You Shop at Secretly Using Face Recognition on You?*, AMERICAN CIVIL LIBERTIES UNION (2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face (last visited Aug 20, 2021).

[5] Face-recognition tech in retail Are Americans prepared for it?, PIPLSAY (2021), https://piplsay.com/face-recognition-tech-in-retail-are-americans-prepared-for-it/ (last visited Aug 16, 2021).

[6] See, e.g.: Patrick Howell O'Neill, *Data leak exposes unchangeable biometric data of over 1 million people*, MIT TECHNOLOGY REVIEW (2019), https://www.technologyreview.com/2019/08/14/133723/data-leak-exposes-unchangeable-biometric-data-of-over-1-million-people/ (last visited Aug 20, 2021), Josh Taylor, *Major breach found in biometrics system used by banks, UK police and defence firms*, THE GUARDIAN (2019), http://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms (last visited Aug 20, 2021).

[7] Rules of NYC, Title 24, § 23-07 Posting letter grades. (7) f.

for the implementation of LL3 need to be tailored towards giving people the information they need to make an informed choice about the stores they frequent.

In conclusion, the NYCLU thanks the Department of Consumer and Worker Protection for the opportunity to provide testimony. The Department's rulemaking is instrumental in ensuring a productive implementation of Local Law 3. We urge the Department to amend and strengthen the proposed rules to require businesses to disclose the types of biometric recognition technologies and their privacy policies – and do so in a way that will be clearly noticeable and recognizable by passersby. Without meaningful levels of detail and specificity, the rules risk to desensitize people to the sign and normalize pernicious data collection in the everyday lives of New Yorkers.