NYCLU
NEW YORK CIVIL LIBERTIES UNION

125 Broad Street
New York, NY 10004
212.607.3300
212.607.3318
www.nyclu.org

May 1, 2019

New York State Homes and Community Renewal (HCR)
Office of Rent Administration/MCI Unit
Gertz Plaza
92-31 Union Hall Street
Jamaica, New York 11433

Letter in Support of Brooklyn Legal Services' Opposition

Re: Docket Nos. GS210005OD and GS210008OD – Owner's Application for Modification of Services to Install a Facial Recognition Entry System

Dear NYS Homes and Community Renewal Administrator:

The New York Civil Liberties Union ("NYCLU") respectfully submits the following letter in support of Brooklyn Legal Services' opposition to the application for the installation of a Facial Recognition Entry System (Docket Nos: GS210005OD and GS210008OD) in the rent-stabilized buildings of Atlantic Plaza Towers, located at 249 Thomas S. Boyland Street, Brooklyn, NY, 11233 and 216 Rockaway Avenue, Brooklyn, NY, 11233 owned by Atlantic Towers Associates, L.P. ("Owner").

The NYCLU, the New York state affiliate of the American Civil Liberties Union ("ACLU"), is a not-for-profit, non-partisan organization with eight offices across the state, and approximately 150,000 members and supporters statewide. The NYCLU's mission is to defend and promote the fundamental principles, rights and values embodied in the Bill of Rights of 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.

The proposed Facial Recognition Entry System represents a major shift in tenant rights and in the policies that govern the residents of over 700 households in the Atlantic Plaza Towers, predominantly women and people of color. The imposition of a biometric identification access system for entrance into one's own home raises constitutional concerns and intrudes on tenants' rights of self-determination and privacy. It conditions entry into one's home – the place where our constitutional rights are at their most robust – on the provision of one's most sensitive biological data. Residents should not have to live in fear that landlords are tracking their comings and goings and amassing sensitive data on tenants and their guests. And those tenants and guests who are women, children, and people of color have particular reason to fear such a change in their housing rights, as facial recognition systems are notoriously inaccurate when it comes to these groups.

Thus, not only would installation of this system cause harm to tenants' privacy rights, but also their civil rights to access housing on equal and nondiscriminatory terms.

A mandatory facial recognition access system will have detrimental effects on the civil liberties and rights of residents and guests. Any such technology should only be used with the affirmative, informed consent and explicit opt-in of any tenant, and never as a blanket requirement imposed on tenants as a condition of housing.

Privacy and Consent

The proposed Facial Recognition Entry System represents a significant departure from other modes of entry, because such a system enables landlords to gather real-time, personally identifiable data on every movement of every tenant and each of her guests.

In contrast to a regular key, the proposed biometric identification method is uniquely tied to the immutable features of an individual's face. Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. Unlike many other biometric systems, facial recognition can be used for general surveillance in combination with public video cameras, and it can be used in a passive way that doesn't require the knowledge, consent, or participation of the subject.

At a minimum, in order to function as a "key," a residential facial recognition system would require a face scan from *at least* one entrant to any apartment and deem the person admissible. It would therefore create a detailed data trail with the precise timestamps of every entrance and exit. Such intricate details about tenants' private lives and social interactions should not be collected in the first place. Once collected, these data combine to produce a detailed picture of an individual's geographic location, schedule, and associations. Landlords already hold a position of great power over their tenants – the ability to control the availability and conditions of their housing – and should not have access to the granular details of their tenant's movements and associations. The Office of Rent Administration should recognize the installation of facial recognition technology for what it is: a dramatic shift in the distribution of rights between landlord and tenant.

Furthermore, this kind of system requires a database to function – with massive amounts of sensitive tenant data flowing in and out of that database, which is held and queried by a private third-party company. A Facial Recognition Entry System raises serious questions about the how such mountains of data would be governed – and it would be flatly inappropriate for the Office of Rent Administration to bless the use of such a system in the absence of clear rules about whether and how tenant data is captured, stored, shared, and sold. The technology also raises questions about how tenants' freedom of association may be affected; for example, if a positive "face match" is required for entry, a tenant could not have a friend or babysitter visit the apartment in her absence, with serious ramifications for tenants' ability to receive visitors.

Requiring tenants (and potentially their guests) to provide sensitive personal data not only to landlords, but also to corporate entities unrelated to housing management, is a separate and distinct change in tenant's conditions of living. This harm is far greater in the absence of rules that would provide clarity to tenants about how any of their data would be treated and shared.

The sharing of granular location and biometric data without a tenant's explicit and informed consent also raises serious legal and constitutional concerns. Although the company selected for the Atlantic Towers' proposed Facial Recognition Entry System, StoneLock, claims in its privacy policy[1] to require each data subject's informed consent to collection, that promise cannot be realized in this context because the Owner has stated that this system will be the only way of entering the building, foreclosing any meaningful consent or opt-out. As a government entity, the Office of Rent Administration should take seriously the emerging reality that government collection of data of this magnitude and specificity, without knowing and informed consent, has constitutional implications. In June 2018, the Supreme Court ruled that law enforcement must obtain warrants before obtaining granular, compiled location data on an individual.[2] Permitting landlords to collect mountains of data on their tenants – in violation of the technology company's own affirmative consent guarantees, and in the total absence of rules governing its sharing with government entities, third parties, or law enforcement – is not only a sea change in tenant rights, but one with serious legal implications.

Accuracy and Racial Disparities

The NYCLU, ACLU, and other civil rights groups have repeatedly warned that facial recognition technology poses an acute threat to civil liberties and civil rights. However, this threat would not be borne equally by all tenants – the underlying algorithms produce racially biased and gendered results.[3] Facial recognition technology has repeatedly been proven to perform less accurately on African Americans, women, and people under 30. A 2018 study identified error rates of up to 34.7 percent for darker skinned females in a common, commercial face classification system.[4]

Last year, the ACLU of Northern California highlighted[5] how this bias plays out in Amazon's face recognition system, Rekognition. The program falsely matched photographs of 28 members of Congress with mugshot photos. While people of color made up approximately 20 percent of members of Congress generally, they constituted nearly 40 percent of the false matches returned by the algorithm.

---

[1] StoneLock Privacy Policy (May 3, 2018), https://www.stonelock.com/wp-content/uploads/2018/05/StoneLock-Privacy-Statement-v18.05.23.pdf.

[2] Nathan Freed Wessler, *The Supreme Court's Groundbreaking Privacy Victory for the Digital Age*, ACLU.org (June 22, 2018), https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-groundbreaking-privacy-victory-digital-age.

[3] Steve Lohr, *Facial Recognition is Accurate – If You're a White Guy*, NEW YORK TIMES (Feb. 9, 2018), https://www.nytimes.com/2018/02/09/technology/facial-recognition-race-artificial-intelligence.html.

[4] Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification, 2018*, http://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf.

[5] Jacob Snow, *Amazon's Face Recognition Falsely Matched 28 Members of Congress with Mugshots*, ACLU.org (July 26, 2018), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/amazons-face-recognition-falsely-matched-28.

StoneLock claims to have a false acceptance rate of 0.0004 percent[6] but has not published any tests that confirm this. The company does not list any additional information such as other error rates, false rejection rates, and whether it performs differently on different skin tones. Despite repeated requests from tenants, the Owner and StoneLock have not published independent audits and studies of the proposed facial recognition system. Such tests should be mandatory before installing a biometric identification system in the homes of people. Tenants of rent-stabilized housing should not be subjected to unproven, potentially biased, and insecure technology.

The consequences of facial recognition technology's race problem could be particularly dire in the housing context. Women and tenants of color face the real possibility that they – or their guests – could be misidentified as intruders by their own front doors. The results are predictable; not only might tenants lose reliable access to their own homes based on their sex or race, but could disproportionately face inconvenience, security resources, or even a law enforcement response – all for the use of inaccurate and biased technology installed without their explicit consent. It is clear that such an entry system represents a major modification to tenants' rights and conditions of housing and access.

Conclusion

For the above reasons, we believe that the installation of a facial recognition system represents a fundamental change in the landlord–tenant relationship, and one that seriously affects the fundamental rights of tenants. We therefore respectfully urge HCR to decline the Owner's application for its installation.

Sincerely,

The New York Civil Liberties Union

[6] StoneLock Go, Specifications, 2, https://www.stonelock.com/wp-content/uploads/2019/02/StoneLock-GO_Overview.pdf (last visited Apr. 30, 2019)