AINOW

April 30, 2019

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

> **Re:** **Docket Nos. GS210005OD and GS210008OD**
> **<u>Owner's Application for Modification of Services to</u>**
> **<u>Install a Facial Recognition Entry System</u>**

Dear DHCR Administrators:

We write to you from the AI Now Institute ("AI Now") in support of the Brooklyn Legal Services Tenant Rights Coalition's opposition of the application by Atlantic Towers Associates, L.P. ("Owner"), for modification of services to install a facial recognition entry system. The application is for two large rent-stabilized buildings located at 248 Thomas S. Boyland Street, Brooklyn, NY, 11233 and 216 Rockaway Avenue, Brooklyn, NY, 11233. The application for this modification raises significant concerns of accuracy, bias, and threats to the privacy and security of the tenants, and we offer our expert analysis to help the New York State Division of Housing and Community Renewal in its consideration on this application.

AI Now is an interdisciplinary research institute at New York University that researches the social implications of artificial intelligence and other emerging technologies with focus on rights and liberties, labor and automation, bias and inclusion, and safety and critical infrastructure.[1] AI Now produces interdisciplinary research to help ensure that advanced technical systems are accountable to the communities and contexts they are meant to serve, and that they are applied in ways that promote justice and equity. AI Now is concerned about the effects of facial recognition on the rights and liberties of individuals, especially the risks for disproportionate harm to communities of color.[2]

The Owner is seeking to install a StoneLock face recognition entry system as a modification of services. The StoneLock system "uses near-infrared light to identify features that are not visible in a photograph."[3] Based on claims made in its patent application[4] and other

---

[1] AI Now Institute, https://ainowinstitute.org/about.html (Last visited Apr. 18, 2019).
[2] AI Now Institute, *AI Now Report 2018*, 4 (December 2018) https://ainowinstitute.org/AI_Now_2018_Report.pdf; Jon Schuppe, *Facial Recognition Gives Police a Powerful New Tracking Tool. It's Also Raising Alarms*, NBC News, (Jul. 30, 2018). https://www.nbcnews.com/news/us-news/facial-recognition-gives-police-powerful-new-tracking-tool-it-s-n894936
[3] Atlantic Towers Associates, L.P. DHCR Response Letter, 4, Apr. 8, 2019.

public documents[5], we believe the StoneLock system performs this function by deploying a local binary pattern algorithm to perform facial recognition.[6] This local binary pattern algorithm takes an image, like a face, and transforms that image into a grid and each contrast value within the grid is assigned a value. This information is then represented in a preferred form (e.g. histogram or heatmap) for later comparison or analysis. StoneLock uses heatmaps to represent the contrast value grid of the images it captures, so this is why it does not need photographs to perform, but its analysis does rely on calculations of biometric data, similar to other facial recognition systems.[7] We provide this description of our understanding of the StoneLock system because the Owner's April 8, 2019 response letter ("response letter") includes several misleading statements about the technology to refute the tenant's claims, which we hope to clarify in greater detail below.

There are Significant Accuracy Concerns with Most Facial Recognition Systems

The most basic function of a residential entry system is access, and access with facial recognition in this context requires nearly flawless accuracy. While even the most prominent facial recognition systems cannot claim 100 percent accuracy,[8] existing research suggests that accuracy for most systems varies based on an individual's attributes.[9] Specifically, most systems fail to accurately identify non-white individuals, certain age ranges, women, and gender minorities.

---

[4] Patent Appl. Doc. Sept. 7, 2012,
https://patents.google.com/patent/US20170308740A1/en?q=Stonelock&q=Facial+Recognition&assignee=Stone+Lock+Global%2c+Inc.

[5] StoneLock, *STONELOCK® PRO RESOURCES & TECHNICAL SPECIFICATIONS*,
https://www.stonelock.com/resources/.

[6] *See*, Kevin Salton do Prado, *Face Recognition: Understanding LBPH Algorithm*, MEDIUM, (Nov. 10, 2017),
https://towardsdatascience.com/face-recognition-how-lbph-works-90ec258c3d6b (describing the local binary pattern algorithm).

[7] *See*, OpenCV link (a very similar and open source model that other developers and companies use to perform the same functions SafeLock describes).

[8] *See*, Patrick Grother, Mei Ngan, Kayee Hanaoka, *NISTIR 8238, Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification*,6, NIST, (November 2018) https://nvlpubs.nist.gov/nistpubs/ir/2018/NIST.IR.8238.pdf
("Recognition accuracy is very strongly dependent on the algorithm, and more generally on the developer of the algorithm. Recognition error rates in a particular scenario range from a few tenths of one percent up to beyond fifty percent").

[9] *See*, Hachim El Khiyari, Harry Wechsler, *Face Verification Subject to Varying (Age, Ethnicity, and Gender) Demographics Using Deep Learning*, 7 J BIOM BIOSTAT 4 (2016)
https://www.omicsonline.org/open-access/face-verification-subject-to-varying-age-ethnicity-and-genderdemographics-using-deep-learning-2155-6180-1000323.php?aid=82636 (finding that "verification accuracy is relatively lower for females,young subjects in the 18-30 age range, and blacks."); Joy Buolamwini, *Gender shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers*, 2017.
https://dam-prod.media.mit.edu/x/2018/02/05/buolamwini-ms-17_WtMjoGY.pdf (describing how even "[f]or the best performing classifier, darker females were 32 times more likely to be
misclassified than lighter males."); Clare Garvie, Jonathan Frankle, *Facial-Recognition Software Might Have a Racial Bias Problem*, THE ATLANTIC, (Apr. 7 2016)
https://www.theatlantic.com/technology/archive/2016/04/the-underlying-bias-of-facial-recognition-systems/476991/
("...the conditions in which an algorithm is created—particularly the racial makeup of its development team and test photo databases—can influence the accuracy of its results.").

In 2018, the ACLU and the University of California Berkeley tested Amazon's facial recognition system on members of Congress and found significant levels of inaccuracies with the error rate being nearly 40 percent for non-white members and only five percent for white members.[10] Researchers have found similar trends and outcomes with other facial recognition systems, and some companies are beginning to acknowledge these concerns.[11] Just recently, Microsoft turned down facial recognition sales to law enforcement on human rights concerns; concluding it would lead to innocent women and minorities being disproportionately held for questioning at least partly due to the disparity in accuracy.[12]

These accuracy concerns also extend to face recognition systems using infrared imaging. Infrared is an attractive modality because it can analyze images under any lighting condition, but a comprehensive study of infrared facial recognition systems found that infrared imaging is sensitive to several conditions that will exist for the proposed use of the StoneLock system.[13] Researchers have found that infrared imaging for facial recognition is sensitive to the environmental temperature as well as the emotional, physical, and health condition of the subject.[14] For example, research has specifically noted that such systems are affected when the subject wears glasses or consumes alcohol.[15]

While the Owner claims the proposed StoneLock system does not share or exhibit these accuracy concerns due to a process that does not explicitly analyze demographic data, research suggests these accuracy concerns stem from a far deeper problem that cannot be minimized by the system's technical form alone. Research suggests that accuracy, bias and other concerns stem from the lack of diversity in the underlying training data[16] and the nature and subjective decisions of programmers and engineers.[17] In a recent study on intersectional accuracy disparities in commercial facial recognition systems, Researchers Joy Buolamwini and Timnit Gebru, found that a system that can claim 87-94 percent general accuracy could have error rates up to 35 percent for certain groups. A strong contributor was that the datasets were overwhelmingly

[10] AI Now Institute, *AI Now Report 2018*, 4 (December 2018) https://ainowinstitute.org/AI_Now_2018_Report.pdf; Jeffrey Dastin, *Amazon's Face ID Tool Mismatched 28 Members of Congress to Mug Shots: ACLU*, REUTERS, https://www.reuters.com/article/us-amazon-com-facial-recognition/amazons-face-id-tool-mismatched-28-members-of-congress-to-mug-shots-aclu-idUSKBN1KG1K7 (Last visited Apr. 18, 2019).

[11] Nadra Nittle, *Amazon's Facial Analysis Tech Often Mistakes Dark-Skinned Women for Men, Study Shows*, VOX, (Jan. 28, 2019, 6:30 PM), https://www.vox.com/the-goods/2019/1/28/18201204/amazon-facial-recognition-dark-skinned-women-mit-study (Last visited Apr. 18, 2019).

[12] Joseph Menn, Microsoft turned down facial-recognition sales on human rights concerns, REUTERS, https://www.reuters.com/article/us-microsoft-ai/microsoft-turned-down-facial-recognition-sales-on-human-rights-concerns-idUSKCN1RS2FV (last visited Apr. 17, 2019).

[13] Reza Shoja Ghiass, Ognjen Arandjelovic, Abdelhakim Bendada, *Infrared face recognition: A comprehensive review of methodologies and databases*, 47 PATTERN RECOGNITION 2807 (Sept. 2014) https://www.sciencedirect.com/science/article/pii/S0031320314001137.

[14] *Id.* at 2808.

[15] *Id*. at 2808-2811.

[16] Joy Buolamwini, *Gender shades: Intersectional Phenotypic and Demographic Evaluation of Face Datasets and Gender Classifiers*, 2017. https://dam-prod.media.mit.edu/x/2018/02/05/buolamwini-ms-17_WtMjoGY.pdf; Garvie, *supra* note 9.

[17] West, S.M., Whittaker, M. and Crawford, K. (2019). Discriminating Systems: Gender, Race and Power in AI. AI NOW INSTITUTE. Retrieved from https://ainowinstitute.org/discriminatingsystems.html.

composed of lighter skinned subjects leading to substantial disparities in accuracy for darker skinned subject even while retaining high levels of general accuracy.[18] This means that a vendor, like StoneLock, can make claims of high general accuracy, but accuracy concerns for specific, and often non-dominant populations remain.

This research demonstrates the need for thorough evaluation processes. The aforementioned study highlighted facial recognition tools as one of many automated systems that rely on machine learning algorithms that are trained with labeled data, so inherent bias in data sets mean disparate impacts in outcomes. Indeed, the bias that often leads to these inaccuracies and imbalance derives from how a system is developed and not necessarily it's capabilities.[19]

Finally, it is notable that most research on facial recognition is often performed in controlled environments under far more ideal conditions than most tenants would experience under the proposed use of the StoneLock system. In reality, there will be varied conditions and circumstances of the tenants' daily entry into their homes, whether carrying groceries, children, or packages, or in various physical and emotional conditions. Research has demonstrated that conditions[20], including pose, illumination, expression, and environmental conditions can impact the accuracy of automated facial analysis.[21] And these concerns regarding the conditions of the subject and the environment where the technology will be used have also been raised in research on the limitations of the infrared facial recognition.[22] Therefore, there should be heightened scrutiny of the use of such systems in residential settings, where these factors become even more variable.

Bias in Facial Recognition Systems Create Higher Risk of Misidentification and Other Negative Outcomes for Non-White Males.

As discussed above, research on facial recognition systems has almost uniformly found bias in accuracy for individuals who do not present as white males,[23] and that claims of high levels of general accuracy can still often contain and conceal incredibly disparate accuracy rates for specific subgroups.[24] This means that historically non-dominant individuals, like women and non-white communities, are at a higher risk of losing access to entry to their home or other negative outcomes, when accuracy fails. Yet, in the response letter, the owner claims that "[b]ased upon the way the StoneLock system works, there is no danger of discrimination," and

---

[18] Joy Buolamwini, Timnit Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, (2018) https://dam-prod.media.mit.edu/x/2018/02/06/Gender%20Shades%20Intersectional%20Accuracy%20Disparities.pdf; Buolamwini, *supra* note 4.

[19] West, *supra*, note 16.

[20] Jeff Stephens, *The Silent Killer of Facial Recognition Software*, Dignari, http://www.dignari.com/blog/facial-recognition-software (Last visited Apr. 26. 2019).

[21] Manminder Singh, *Varying Illumination and Pose Conditions in Face Recognition*, ScienceDirect, 2016. https://reader.elsevier.com/reader/sd/pii/S1877050916306056?token=3E204FA77727350578D3F53808CA48B08C1B8BE43C1E1D2C188A6E93EE0468A20974EA519EE722CC942038FFE8146922.

[22] Ghiass, *supra* note 12, at 2811 ("In the context of automatic face recognition, the main drawback specific to...infrared spectrum, stems from the fact that the heat pattern emitted by the face is affected by a number of confounding variables, such as ambient temperature, air flow conditions, exercise, postprandial metabolism, illness and drugs.").

[23] Nittle, *supra* note 11.

[24] Buolamwini, Gebru, *supra* note 17.

that there is no need for validation studies that specifically attest for bias and accuracy.[25] Such claims are not only misleading, but false.

The response letter attempts to support these claims by citing a document of StoneLock describing the system and a copy of a safety test report by Underwriter Laboratories.[26] The StoneLock document is not independently verified, nor does it include citation to allow verification of its claims. Additionally, the citations to the safety test report are misleading because the report merely verifies that the StoneLock system's lights are safe, it does not does not validate the capabilities, functions, or efficacy of the system.

Moreover, as discussed above, there is existing research that demonstrates the limitations of infrared face recognition, and a number of confounding variables can further disparate outcomes for different individuals including, "[w]earing clothes, experience stress, blushing, having a headache or an infected tooth."[27] In fact, researchers have suggested that given the high sensitivity of this technology to a range of factors, it is challenging to find persistent and discriminative features for image analysis.[28] Therefore, requests for validation studies of StoneLock and overall concerns of bias are warranted, especially in light of the demographic diversity of the neighborhood.[29]

Facial Recognition Systems Will Adversely Affect the Privacy, Security, and Other Civil Liberties of Tenants.

When facial recognition or other image analysis is combined with CCTV and other camera systems, there is a heightened risk of misuse and abuse. Tenants of the target buildings have already complained about being subject to invasive scrutiny with the use of existing surveillance cameras. Tenants have specifically cited incidents where the building's management tracked the details of items brought in and out of their private residences.[30] Thus, the existence of established intrusive practices increases concerns regarding data usage and sharing with the use of facial recognition.

Facial recognition data is highly attractive to hackers and law enforcement creating high risks of misuse and abuse. The storage of any data exposes tenants to some risks of hackers and law enforcement gaining access to the tenant's detriment. In the response letter, the owner claims that the StoneLock system only stores five percent of the subject's biometric data locally, and that such data cannot be reverse-engineered or otherwise used by a third party.[31] Though the

---

[25] Atlantic Towers Associates, L.P. DHCR Response Letter, 3, Apr. 8, 2019.

[26] *Id.* at Exhibit A & B.

[27] Ghiass, *supra*, note 12, at 2810.

[28] *Id.*

[29] Neighborhood demographics of target buildings are largely populated by women and persons of color. The Census Bureau's 2017 American Community Survey Demographic and Housing Estimates show that about 78 percent of the population in the neighborhood of the target buildings are African American, and only 8 percent are white. The data also estimates that 56 percent of individuals 18 and over are female, and 61 percent of those over 65 also being females. Community Facts, *ACS Demographic and Housing Estimates*,
https://factfinder.census.gov/faces/tableservices/jsf/pages/productview.xhtml?src=CF (Last visited, Apr. 26, 2019).

[30] Sarina Trangle, *Facial Recognition Planned for Brooklyn Apartment Building Outrages Tenants*, ᴀᴍNᴇᴡYᴏʀᴋ, (Mar, 25, 2019) https://www.amny.com/real-estate/facial-recognition-apartments-1.28951805.

[31] Atlantic Towers Associates, L.P. DHCR Response Letter, 2, Apr. 8, 2019.

amount of information stored is limited, these broad claims understates the risks and potential utility of biometric information. For instance, with other biometrical information like DNA and fingerprints, partial, fragmented, and contaminated samples have been used to misidentify individuals.[32] The privacy and security risks might be reduced under StoneLock's model, but it is by no means absent.

Conclusion

Given the issues of accuracy, bias, privacy, and security, we strongly urge DHCR to oppose the pending application for modification of services to install a facial recognition entry system. The owner has failed to provide a meaningful explanation of the need to implement a relatively new technology even in the face of the opposition by the tenants, and the response letter fails to adequately address their very real concerns regarding accuracy, bias, privacy, and safety. As it is the tenants who bear the risks and burdens both with and without the technology, their concerns should be addressed and consent should be required before implementation.

Sincerely,

Rashida Richardson
Director of Policy Research
AI Now Institute

---

[32] Jeremy Peters, *New Rule Allows Use of Partial DNA Matches*, NY TIMES, (Jan. 24, 2010) https://www.nytimes.com/2010/01/25/nyregion/25dna.html (explaining new policy enabling law enforcement to use partial DNA samples and some ramifications); Naomi Elster, *How Forensic DNA Evidence Can Lead to Wrongful Convictions*, DAILY JSTOR, (Dec. 6, 2017), https://daily.jstor.org/forensic-dna-evidence-can-lead-wrongful-convictions/ (describing the risks and damaging effects of law enforcement use of partial DNA samples); Omid Zanganeh, Nandita Bhattacharjee, Bala Srinivasan, *Partial Fingerprint Identification Through Correlation-Based Approach*, SECRYPT, 2014 (highlighting method to compute partial fingerprint data).