

**NYS HOUSING & COMMUNITY RENEWAL  
OFFICE OF RENT ADMINISTRATION/MCI UNIT**

---

**IN THE MATTER OF  
THE OWNER'S APPLICATION  
FOR MODIFICATION OF SERVICES**

**Docket Nos: GS2100050D  
GS2100080D**

**Premises:  
249 Thomas S. Boyland Street  
Brooklyn, NY, 11233**

**TENANTS OF ATLANTIC PLAZA TOWERS**

---

**216 Rockaway Avenue  
Brooklyn, NY, 11233**

Brooklyn Legal Services (“BLS”) hereby appears on behalf of 134 tenants of 216 Rockaway Avenue and 249 Thomas S. Boyland Street, Brooklyn, New York (collectively known as, “Atlantic Plaza Towers”) and demands that all papers in this proceeding be served upon the undersigned at the office and address stated below. This submission is offered in further opposition to the applications that Atlantic Towers Associates, L.P. (the “Owner”) filed with the New York State Homes and Community Renewal (“HCR”) in July 2018 “seeking to install a biometric security and identity verification system, more commonly known as a facial recognition system, in lieu of the keyless key fob system currently in place of at the building.”<sup>1</sup> As we understand that these applications present an issue of first impression for HCR, the tenants of Atlantic Plaza Towers seek a determination from HCR that the utilization of facial recognition technology has no place in their buildings, nor in any rent regulated apartment in New York, for the reasons set forth herein.<sup>2</sup>

---

<sup>1</sup> Owner’s Application for Modification of Services for 216 Rockaway Avenue dated July 3, 2018, and Owner’s Application for Modification of Services for 249 Thomas S. Boyland dated July 3, 2018, both attached hereto as **Exhibit 1** (hereinafter, “Owner’s Application”).

<sup>2</sup> The undersigned attorneys make this submission based on their personal knowledge of the facts contained in this submission, or based on the information provided to them by their clients and the information contained in the files kept in their offices.

## PRELIMINARY STATEMENT

Currently, at Atlantic Plaza Towers, a towering 22-story building sporting new signage and blue lights, a rent-stabilized tenant approaches her residence's entry door, watched by a camera sitting on the left of the doorway. She opens the first door, walks in, and then scans her key fob to open a second door. Through the second door she faces a security guard desk, which is sometimes manned and sometimes empty. To her right is yet a third door that will again require another scan of the fob. Each time she scans her key fob, which is associated with a personal identification number linked to her, a record of her entry is created. Over half of dozen 360 degree cameras watch her as she traverses the newly renovated lobby, checks her mail, and enters the elevator to her floor. More cameras continue to track her in the elevator, and still others continue the task as she steps into the hallway. She is watched as she does her laundry, as she takes out her trash. There is very little that she can do in the complex—other than walk down or up the internal staircases—that the Owner cannot monitor. This is by design, and the Owner's management regularly reminds her, and all 717 of her neighbors, that this is their reality through letters, the imposition of fines, and security footage of alleged offenses. Despite having this level of control over the tenants, the Owner now seeks to add an additional layer of surveillance—a facial recognition entry system that will collect biometric data from tenants' bodies that is unique to them and cannot ever be replaced if compromised, over which the Owner will have unfettered autonomy.

To be sure, the implications of allowing the Owner to deploy this facial recognition technology on the tenants of Atlantic Plaza Tower are significant. The tenant population at Atlantic Plaza Towers consists of approximately 90% or more people of color, more than 80% women; and a large number of elders and minors. Far from being considered an “amenity”

by the tenants, or a “cool” upgrade as suggested by the Owner (a self-described “tech geek”), the tenants see the proposed installation of a facial recognition system as further intrusion into the quiet enjoyment of their private home lives. They certainly do not view the proposed system as something that benefits them, but rather that only serves to harm them.

There are a number of aspects involved with the Owner’s modification of services application that represent a dramatic shift in the historic relationship between landlords and tenants, including: (i) the conditioning of the tenants’ entry into their home (the place where constitutional protections are most robust) on the mandatory surrender of their most sensitive biological data to multiple private corporations; (ii) the unprecedented amassing of a database with real-time, granular details of every tenants’ movements and associations; and (iii) the total absence of statutory, caselaw, or agency rules governing the sharing of the tenants’ biological data with governmental agencies, third parties, or law enforcement. None of these are traditional elements of landlord-tenant relationships in New York. This agency, therefore, must seriously evaluate whether it is willing to open all of these doors into uncharted territories in the name of an unsubstantiated security risk purportedly in existence at Atlantic Pacific Towers.

The Owner dismisses the significance of this additional intrusion by equating biometric data to a mere photograph, and claiming that because HCR permits the installation of key fob systems that HCR should readily apply that precedent to rubberstamp the Owner’s application. However, this cavalier and underdeveloped comparison should concern HCR. HCR has already signaled that it understands this significant difference and does not view the substitution of a key fob system with facial recognition technology to be the same exchange in services as it did metal keys to key fobs. More than once, and as recently as July 2018, HCR has affirmed that owners are not required to obtain agency approval prior to installing a key fob/keycard system because

“the only difference in obtaining access to the premises is that a card key will be used, instead of a metal key,”<sup>3</sup> and that such failure does not “form[ ] the basis for granting the tenant a rent reduction.”<sup>4</sup> However, in February 2019, HCR issued a rent reduction order against an owner that installed a “Gate Guard/Teman” intercom system that operates by facial recognition because the change was done without agency approval.<sup>5</sup> While the order does not provide any reasoning for the decision, this suggests that HCR recognizes the inherent difference between entering a building with a physical key, whether it metal or plastic, and using information derived from a person’s body to do so.

The tenants respectfully request that HCR consolidate Docket Number GS210005OD and Docket Number GS210008OD pursuant to Rent Stabilization Code Section 2527.5(f), order a hearing pursuant to Section 2527.5(h) for the testimony of tenants and experts, and ultimately deny the Owner’s Application pursuant to Section 2527.6.

### **PROCEDURAL FACTS**

Contrary to the Owner’s letter submission to HCR dated April 8, 2019,<sup>6</sup> which disingenuously suggested that only 5.7% of tenants object to the proposed installation, hundreds of Atlantic Plaza Towers tenants have made clear to HCR that they oppose the Owner’s Application. Some, but not all, of the tenants of 249 Thomas S. Boyland and 216 Rockaway Avenue received notices from HCR about the Owner’s Application in September and October

---

<sup>3</sup> Matter of the Administrative Appeal of Sanders et al., DHCR Admin. Rev. Docket. No. TI410005RT et al., April 28, 2006.

<sup>4</sup> Matter of the Administrative Appeal of 164-03 LLC, DHCR Admin. Rev. Docket No. EW110010RO, issued July 26, 2018.

<sup>5</sup> Order Reducing Rent for Rent Stabilized Tenant(s), Docket No. GV-430003-B, issued February 1, 2019.

<sup>6</sup> See Letter from Horing Welikson & Rosen PC to HCR Office of Rent Administration, dated April 8, 2019, attached hereto as **Exhibit 2** (hereinafter “Owner’s April 8 Letter”).

2018, respectively.<sup>7</sup> Tenants held a meeting in mid-October 2018 where the tenants in attendance unanimously voted against the installation. Days later, tenants collectively returned hundreds of responses—nearly 350—indicating to HCR that they objected to the Owner’s Application, along with a letter outlining several reasons for their objection,<sup>8</sup> many of which are further developed in this submission. The Atlantic Towers Tenants Association also submitted a letter in opposition dated October 21, 2018 further explaining the tenants’ concerns and asking for the Owner’s Application to be rejected.<sup>9</sup>

Given the significant implications of the technology being proposed, tenants reached out to BLS in late November 2018 for possible representation in the instant HCR proceedings. A group of tenants thereafter retained BLS, who sent HCR a letter dated January 9, 2019 requesting an extension of time for the tenants to gather further information and submit an additional response through counsel. This letter was signed by almost 250 tenants and NYS Assemblywoman Latrice Walker, and was accompanied by a support letter from NYC Council Member Alicka Ampry-Samuel.<sup>10</sup> The request for an extension came only a few months after tenants received notice of the Owner’s Application, and therefore the Owner’s claim that such a

---

<sup>7</sup> The Owner filed its Application in the midst of renovations of the lobby, which included moving and replacing the tenants’ mailboxes. As a result, when HCR sent out notices, tenants reported that many tenants did not receive a copy in their mailbox. Other tenants report receiving their notice within days of, or after, the 20-day response period.

<sup>8</sup> See Notices of Commencement of Proceeding Upon Owner’s Application for Modification of Services, completed and signed by various Atlantic Plaza Towers tenants, and Letter from Atlantic Plaza Towers tenants, dated October 20, 2018, both attached hereto as **Exhibit 3**. These are only the responses collectively submitted by the tenants; many other tenants submitted their responses individually to HCR.

<sup>9</sup> See Letter from Atlantic Towers Tenants Association, dated October 21, 2018, attached hereto as **Exhibit 4**.

<sup>10</sup> See Letter from Brooklyn Legal Services to HCR Office of Rent Administration/MCI Unit, dated January 8, 2019 (hereinafter “BLS January 8 Letter”), and Letter from Council Member Alicka Ampry-Samuel, both attached hereto as **Exhibit 5**.

request is “merely a delaying tactic”<sup>11</sup> should be given no weight, particularly considering that the Owner’s Application was three pages long and provided little to no information about the technology it proposed to install.

Upon receipt of BLS’s January 9 letter, counsel to the Owner proposed that each side’s counsel, the Owner, and the Owner’s security representative meet on February 7, 2019 to discuss the facial recognition system and the tenants’ concerns. It was only at BLS’s insistence that a small group of tenants participated in this meeting; the Owner initially resisted their inclusion. What the tenants learned at this meeting is detailed further below, and after this meeting tenants had additional questions and continued to carry many of the same concerns. BLS wrote to the Owner’s counsel for further information, and received no response. Having also received no response from HCR regarding the tenants’ request for an extension, BLS sent a follow-up letter to HCR on March 23, 2019, which informed HCR of the unanswered questions posed to the Owner and included additional tenant signatures.<sup>12</sup>

On April 8, 2019, the Owner submitted a letter to HCR that included further information regarding the proposed facial recognition entry system and responded to BLS’s January 8 Letter.<sup>13</sup> On April 12, 2019, Council Member Ampry-Samuel received a letter from HCR approving her request, which was made on behalf of the tenants, for an extension through May 13, 2019.<sup>14</sup> The tenants now timely submit this opposition. The tenants’ battle against the

---

<sup>11</sup> See Exhibit 2 (Owner’s April 8 Letter) at 1.

<sup>12</sup> See Letter from Brooklyn Legal Services to HCR Office of Rent Administration/MCI Unit, dated March 22, 2019, attached hereto as **Exhibit 6**.

<sup>13</sup> See Exhibit 2 (Owner’s April 8 Letter).

<sup>14</sup> See Letter from HCR to Council Member Ampry-Samuel, dated April 12, 2019, attached hereto as **Exhibit 7**. We understand this letter to grant the tenants’ January 8, 2019 and March 22, 2019 requests for an extension, though HCR has not sent any such confirmation directly to BLS. To the extent that HCR has not already formally granted the tenants’ request, the tenants

Owner's Application has garnered attention from the media,<sup>15</sup> and the following organizations and individuals offer amicus letters supporting the tenants' opposition, which are included in the attached Appendix:

- The New York Civil Liberties Union;
- AI Now;
- Professor Christopher Gilliard, PhD, Macomb College; and
- Joy Buolamwini, MIT Algorithmic Bias researcher joined by prominent AI researchers.<sup>16</sup>

### THE CURRENT SECURITY SYSTEM

The metal key locks at the entrance of both buildings of Atlantic were replaced with a key fob system in or around 2009. Tenants are currently assigned a single key fob that gives them access to the front lobby of either 249 Thomas S. Boyland Street or 216 Rockaway Avenue (depending on which building they live in), the courtyard entrances at the back of their building, and the parking garage entrance. Tenants must enter through three separate doors before reaching

---

have undoubtedly demonstrated good cause pursuant to 9.N.Y.C.R.R. § 2527.5(d) in light of the first impression nature of the Owner's Application seeking to install a facial recognition entry system, the significance of the tenants' biometric data at stake, and the potential wide-sweeping impact of a decision in this proceeding on all of New York State's rent regulated tenants.

<sup>15</sup> See e.g., Gina Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, N.Y. Times, Mar. 28, 2019, <https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html> (last visited Apr. 30, 2019); Sarina Trangle, *Facial recognition planned for Brooklyn apartment building outrages tenants*, amNew York, Mar. 25, 2019, <https://www.amny.com/real-estate/facial-recognition-apartments-1.28951805> (last visited Apr. 30, 2019); Elizabeth Kim, *Brooklyn Landlord Wants to Install Facial Recognition at Rent-Stabilized Complex*, Gothamist, Mar. 25, 2019, [http://gothamist.com/2019/03/25/facial\\_recongnition\\_building.php](http://gothamist.com/2019/03/25/facial_recongnition_building.php) (last visited Apr. 30, 2019), all attached hereto as **Exhibit 8**.

<sup>16</sup> Ms. Buolamwini's amicus letter is not included with the current submission, but will be sent under separate cover to HCR prior to May 13, 2019. BLS reserves the tenants' right to further supplement this submission up to and through May 13, 2019, and expects that HCR will continue to exercise its discretion to accept further materials after this date until it makes a decision on the Owner's Application.

the lobby of their building, and two of the doors require a swipe of the key fob. After going through the first entry door, which is open to the public, a tenant swipes a key fob to open the second door, which leads to the security desk where visitors sign in, and then swipes to open the third door to the building lobby that leads to the elevators and mailboxes. A tenant's key fob will only open the door to which the Owner has granted them access, giving the Owner full control over what space each individual tenant may enter. For instance, even if every member of the household shares the family car, only the key fob assigned to the tenant of record will open the door to the parking lot.

Guests enter the building through the front door, then use an intercom system—which includes the full name and apartment number of each tenant—to find the tenant they are visiting. The tenant can then remotely, through a cell phone or landline, allow their guest entry through the second entry door. However, that does not permit the guest access through the third door, and a tenant must either come down to let in their guest or rely on the security guard to permit access.

In addition to this complex system of key fob entry points and locked doors, the tenants' safety at Atlantic Plaza Towers is closely monitored by a 24-hour attended lobby and state-of-the-art security cameras.<sup>17</sup> With dome cameras installed at every corner of the lobby and a 360-degree camera positioned throughout, the surveillance system will catch each step from the moment a tenant walks up the walkway, through the vestibule, past the front desk, and to the mailboxes. The cameras will watch the tenant whether they choose to walk to the community room, to the elevators, or through the back doors leading to the shared courtyard. Their elevator ride and walk to and from their apartment door will be recorded by the cameras installed inside

---

<sup>17</sup> Nelson Management Group, Atlantic Plaza Towers, <https://nelsonmanagementgroup.net/portfolio/atlantic-plaza-towers/> (last visited Apr. 30, 2019).



the elevator shaft, near the elevator doors, and the ends of each floor. Outdoor surveillance cameras will also keep a watchful eye on tenants taking out the trash, walking to the car or to the grocery store, or enjoying the fresh air from the open space between the two buildings.

Though the current high-tech security system efficiently protects the tenants residing at Atlantic Plaza Towers, tenants have identified a few gaps in the system that the Owner should address. First, the 24-hour security guard is not always present at the front desk of both buildings when a tenant's key fob does not work or a guest wishes to be let in, and therefore tenants and guests cannot enter past the third door. The Owner previously employed three security guards at any time, allowing the third guard to cover the desk when another went on break, did security rounds, or attended to maintenance work in the lobby; now tenants only see two security guards allocated to the two buildings, meaning that the desk is unattended when the security guard is otherwise occupied. Second, tenants have often attempted to gain access with their key fobs, only to discover it is not working. At times this is due to the Owner shutting off the key fob without warning, which is tantamount to an illegal lockout, but other times the key fobs simply stop working for no known reason. Third, there is currently no backup generator or system in place for when the key fob system is suspended in a blackout. The last time such a blackout occurred, in 249 Thomas S. Boyland in 2018, the entrance doors to the building were left wide open overnight as there was no option for using a metal key to gain access.

### **THE PROPOSED FACIAL RECOGNITION SYSTEM**

The proposed facial recognition entry system is a biometric security and identity verification system run by StoneLock that takes a face scan of an individual to permit access. There is little to no information about the technology included in the Owner's three-page application, including basic details; in fact, until tenants read statements made by the Owner in a

news article, they had no idea which of the three various StoneLock products the Owner was proposing to install (turns out it is StoneLock Go). The only information that the tenants have about the proposed system is based on: (1) what the Owner’s security representative, Gregory Keeling from New York Security Solutions, Inc., told them at a meeting on February 7, 2019; (2) StoneLock marketing materials;<sup>18</sup> and (3) an unsigned and undated document titled “Residential Use of StoneLock Facial Recognition,” which the Owner attached to its April 8 Letter.<sup>19</sup>

#### A. How StoneLock Allegedly Works

It is clear from the material provided that the facial recognition system utilizes new and untested technology that has only been deployed in commercial buildings to-date—even though the Owner’s security officer claimed at the February 7 meeting that it had been installed in at least two residential buildings.<sup>20</sup> The promotional material describes a frictionless experience in which tenants would simply walk up to a StoneLock Go device that scans their face from up to three feet away using near-infrared waves (“NIR”), and grants access after matching the tenant’s current biometric heatmap to the heatmap template, which represents 5% of a user’s unique facial features and is stored in its system.<sup>21</sup> According to StoneLock, all of the data associated with the biometric information is stored as an encrypted reference file, or authentication code, in its proprietary StoneLock Gateway system. While StoneLock claims that the system is closed (i.e., StoneLock cannot access the data), the Owner is the entity with full access and control over

---

<sup>18</sup> See StoneLock Promotional Flyer and StoneLock Privacy Policy, last updated May 23, 2018, both attached hereto as **Exhibit 9**.

<sup>19</sup> See Exhibit 2 (Owner’s April 8 Letter) at Exhibit A.

<sup>20</sup> See Exhibit 2 (Owner’s April 8 Letter) at page 4 (“There is also no available list of buildings that have installed the StoneLock system because, until now, the main focus of StoneLock has been corporate and governmental security.”). Mr. Keeling represented that he did not have the addresses off the top of his head but that he would locate the information and share. That information has not been forthcoming.

<sup>21</sup> See Exhibit 9 (StoneLock Promotional Flyer).

the Gateway system.<sup>22</sup> The promotional materials also state the biometric information is only usable in conjunction with the proprietary algorithm software of a StoneLock system, which has already been deployed in the commercial security sector.<sup>23</sup>

A key feature of the proposed system that the Owner conveniently omits from any of the material shared with HCR or the tenants is that the StoneLock system obtains photographic images, i.e., JPEG files, of each tenant at the time of enrollment and of any individual whose heatmap scan does not match a template on file.<sup>24</sup> The Owner has not shared any assurances that the frictionless StoneLock Go device will not use NIR waves from three feet away to scan the tenants' guests or other individuals standing in the vestibule at the building entrance.

With respect to potential data breaches, at the February 7 meeting, Mr. Keeling claimed the Gateway system will be protected by a 256-bit encryption, which simultaneously claimed could be hacked in two years (likely believing that the tenants would be impressed by the length of time). Two years is not a particularly long period of time considering that many of the tenants have resided at Atlantic Plaza Towers for decades, some since the complex opened in the late 1960s. Further, neither Mr. Keeling nor the Owner in any of its submissions has explained how the Owner, who admittedly reigns over the data, will access the data. Will it use a computer, laptop, or phone to do so? How will that device be protected or encrypted? The tenants have been provided with no information about how they will be protected from potential data breaches.

What is particularly puzzling about the proposed system is that it will not entirely replace the current key fob entry system, nor will it address any of the gaps in the current security

---

<sup>22</sup> See Exhibit 2 (Owner's April 8 Letter) at Exhibit A.

<sup>23</sup> See Exhibit 9 (StoneLock Privacy Policy); Exhibit 2 (Owner's April 8 Letter) at Exhibit A.

<sup>24</sup> See Exhibit 9 (StoneLock Privacy Policy).

system. The Owner informed tenants at the February 7 meeting that the StoneLock terminal will be placed at the second entrance door to enter the lobby prior to where the 24-hour attendant is stationed, but a key fob will still be required to enter the third door, the parking garage, and the back entrance to the shared courtyard. And like with the current system, the Owner has not provided any information on what would happen in a blackout when the StoneLock security system is not operational.

**B. The Owner Has Not Provided The Necessary Information To Assess The Accuracy And Bias Of The StoneLock System**

The Owner cannot guarantee that the tenants will have uninterrupted access to their homes without producing not only studies on the accuracy and bias of the proposed StoneLock facial recognition system, but also sharing the process for continuous monitoring of error rates should the proposed system be installed.

Mr. Keeling boasted a 100% accuracy rate at the February 7 meeting and the Owner maintains no tests for the system's accuracy and bias exist because the StoneLock algorithm does not read the race, gender or age of an individual.<sup>25</sup> Even prevailing facial analysis systems owned and operated by leading technology companies, such as IBM, Microsoft, and a Chinese company called Megvii, makers of Face++, cannot make such a guarantee because there is not a single facial recognition system on the market today that is flawless. By construction, these systems are based on statistical methods which must account for uncertainty. Study after study has proven that these artificial intelligence systems “rely on machine learning algorithms . . . trained with biased data [that] have resulted in algorithmic discrimination.”<sup>26</sup> These particular facial

---

<sup>25</sup> See Exhibit 2 (Owner's April 8 Letter) at Exhibit A..

<sup>26</sup> J. Buolamwini and T. Gebru, *Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification*, Conference on Fairness, Accountability and Transparency, 77–91 (2018), available at <https://www.media.mit.edu/publications/gender-shades-intersectional->

recognition systems have been “proven to perform better on lighter-skinned men than darker-skinned individuals and women.”<sup>27</sup>

Following Gender Shades, the leading study on the impact demographic and phenotypic characteristics (i.e., gender and skin type, respectively) have on automated facial analysis accuracy, another study performed for the Science and Technology Directorate of the Department of Homeland Security (“DHS-S&T”) demonstrated similar algorithm performance issues using benchmarks accounting for phenotypic characteristics (i.e., physical skin properties that vary amongst different ethnicities).<sup>28</sup> In addition to other demographic factors, the DHS-S&T study used skin reflectance as one of the benchmarks to test facial biometric systems. Skin reflectance is a phenotypic measure that relies on light intensity measurement at specific wavelengths to determine the physical skin properties, instead of capturing color spaces optimized for human perception to determine “skin color.”<sup>29</sup> The study discovered that skin reflectance, and not racial category, was a better way to assess for accuracy. The performance of a face recognition system was found to be less efficient or accurate for people with lower (or darker) skin reflectance.<sup>30</sup>

---

accuracy-disparities-in-commercial-gender-classification/, (last visited Apr. 30, 2019); see also Matt Wood, *Face recognition researcher fights Amazon over AI bias*, AP News, 2019, available at <https://www.apnews.com/24fd8e9bc6bf485c8aff1e46ebde9ec1> (last visited Apr. 30, 2019).

<sup>27</sup> Id.

<sup>28</sup> C. M. Cook, J. J. Howard, Y. B. Sirotin, J. L. Tipton and A. R. Vemury, “Demographic Effects in Facial Recognition and Their Dependence on Image Acquisition: An Evaluation of Eleven Commercial Systems,” *IEEE Transactions on Information Forensics and Security*, 2019, available at <http://jjhoward.org/pubs/demographic-effects-image-acquisition.pdf> (last visited Apr. 30, 2019).

<sup>29</sup> Id. at 3.

<sup>30</sup> Id. at 2.

Not only are the benchmarks used to test for diverse demographics and phenotypic attributes extremely important, but so are the conditions in which the facial recognition system is tested. Did the system undergo real-world testing that accounts for the day-to-day use of the biometric data, or was it only performed in a controlled lab-setting? Additionally, is there a deployment process in place to allow for on-going reporting that continuously monitors the error rates for demographic and phenotypic characteristics? And how will the results of that on-going reporting be shared with the tenants and general public to ensure there is no predictable algorithmic bias with the StoneLock system, as the Owner claims?

In order to uphold its claims for accuracy and bias, the Owner must share the machine-learning techniques and the training data used to build the algorithm used by the StoneLock facial recognition system. Without this information or any independent validation studies on the biometric performance that test for demographic and phenotypic characteristics, there is no guarantee the system will not discriminate against thousands of black and brown tenants, who are predominantly women and identify mostly as African, African-American, or Latino.

Further, the Owner provides the Underwriter Laboratories (UL) certifications for the near-infrared (NIR) light used by StoneLock,<sup>31</sup> but fails to provide any studies backing Mr. Keeling other dubious claims on February 7, 2019 that weather conditions, lighting, clothing, eyewear and other variations in facial features or expressions have no impact on the accuracy of a StoneLock face scan. This cannot be true given the abundance of international research on the challenges with using near-infrared (NIR) waves to scan an individual's biometrics.<sup>32</sup> One study

---

<sup>31</sup> See Exhibit 2 (Owner's April 8 Letter) at Exhibit B.

<sup>32</sup> See R.S. Ghiass, O. Arandjelović, A. Bendada, and X. Maldague. *Infrared face recognition: A comprehensive review of methodologies and databases*, Pattern Recognition (2014), available at <https://arxiv.org/pdf/1401.8261.pdf> (last visited Apr. 30, 2019), see also, C. Chen and A. Ross, *Evaluation of Gender Classification Methods on Thermal and Near-infrared Face Images*, West

found that wearing clothes, feeling stressed, blushing, a headache or infected tooth could limit the use of biometric data acquired by NIR in facial recognition systems.<sup>33</sup> Sunlight sensitivity could also impact matching NIR face scans, “similar[ly] to matching visible spectrum images.”<sup>34</sup>

Without any studies or proof the system has been tested, the Owner is relying solely on StoneLock’s claim that the facial recognition has been successfully adopted by Fortune 100 companies. This is a futile analogy because the demographic makeup of Fortune 100 companies is nowhere equivalent to the demographic and phenotypic characteristics of the tenants residing at Atlantic Plaza Towers. It is especially troubling if the Owner has not even requested the information from StoneLock. Would one not want to see tests proving accuracy and lack of bias when making such an excessive purchase that could impact the daily lives of thousands of tenants?<sup>35</sup>

Given the ample research on accuracy and bias limitation of NIR face scans, HCR should wonder why the Owner continues to refuse to provide any studies on the effectiveness of the StoneLock facial recognition system.

---

Virginia University (2011), available at [https://www.academia.edu/2729887/Evaluation\\_of\\_gender\\_classification\\_methods\\_on\\_thermal\\_and\\_near-infrared\\_face\\_images](https://www.academia.edu/2729887/Evaluation_of_gender_classification_methods_on_thermal_and_near-infrared_face_images) (access Apr. 30, 2019) and N. Narang and T. Bourlai, *Gender and Ethnicity Classification using Deep Learning in Heterogeneous Face Recognition*, published in 2016 International Conference on Biometrics (ICB), IEEE, DOI: 10.1109/ICB.2016.7550082 (2016).

<sup>33</sup> Id.

<sup>34</sup> Id.

<sup>35</sup> The Owner attempts to paint a rosy picture by referencing the “successful” installation of facial recognition technology at Knickerbocker Village in the Lower East Side neighborhood of Manhattan. BLS has spoken to one tenant, who stated that he was denied access on numerous occasions by the facial scan and that he has heard of other tenants having similar issues, particularly elderly tenants. As the tenants only received a copy of the Owner’s April 8 Letter on April 25, 2019 through counsel, which is the first time the Owner references the experience of other complexes to support its Application, BLS reserves the tenants’ rights to submit affidavits or other documentation with respect to the Owner’s position on Knickerbocker Village.

## ARGUMENT

### THE OWNER HAS FAILED TO DEMONSTRATE THAT FACIAL RECOGNITION TECHNOLOGY IS AN ADEQUATE OR NECESSARY SUBSTITUTE FOR THE CURRENT SECURITY SYSTEM

An owner must provide and maintain “required services,” meaning the same space and services that the landlord was maintaining or required to maintain on the applicable “base date” and any additional services provided thereafter.<sup>36</sup> Required services include, but are not limited to, repairs, decorating, and maintenance, the furnishing of light, heat, hot and cold water, and, most relevant to the instant proceeding, security.<sup>37</sup> The Rent Stabilization Code provides that “an owner may file an application to modify or substitute required services, at no change in the legal regulated rent on the grounds that such modification or substitution is not inconsistent with the [Rent Stabilization Law] or this Code.”<sup>38</sup> Such modification of services “may be made if the proposed change is an ‘adequate substitute.’”<sup>39</sup>

Here, the Owner is desperate in its attempt to convince HCR that replacing the key fob system with a facial recognition entry system is “similar to those [modifications where key fob/keycard systems replaced metal key locks] which DHCR has consistently determined to be an adequate substitution of services and is not inconsistent with the Rent Stabilization Law or

---

<sup>36</sup> 9 N.Y.C.R.R. § 2520.6(r)(1).

<sup>37</sup> Id.

<sup>38</sup> See, e.g., Matter of the Administrative Appeal of Court, DHCR Admin. Rev. Docket No. DR430034RT, July 29, 2016; see also 9 N.Y.C.R.R. § 2522.4(e).

<sup>39</sup> Matter of Bazile v. Rubin, 165 A.D.3d 793, 794 (2d Dep’t 2018); citing Matter of Shahid v. New York State Div. of Hous. & Community Renewal, 84 A.D.3d 822, 823 (2d Dep’t 2011); see also Matter of Various Tenants of 63-60 98th St., Admin. Review Docket No. BW110035RT, issued Aug. 21, 2015 (“It has been long-standing DHCR policy that an application for modification of services may be granted when it is determined that the proposed modification is an adequate substitute.”).



Code.”<sup>40</sup> Without much discussion, the Owner cites to several HCR orders granting a modification of services from a traditional key entry system to a keyless card or fob system, each of which include a consistent set of conditions that the owner must abide by or face a potential reduction of services.<sup>41</sup> The Owner claims, in conclusory fashion, that “[t]he criteria set forth in [the orders] can be equally applied to the proposed facial recognition system.”<sup>42</sup> It is not an accident that the Owner fails to discuss these “criteria” with any specificity or apply any criteria to the proposed system—the very nature of a facial recognition entry system is at unequivocal odds with HCR precedent relating to key fobs/keycards.

Significantly, it would be categorically impossible for HCR to impose, or thereafter for the Owner to adhere to, many of the conditions that HCR has found necessary in order for key fob/keycard systems to serve as a lawful modification in service. Those conditions are all reflected in the order attached to the Owner’s April 8 Letter as Exhibit E:

1. Entry into the building may be accessed by electronic key fobs/keycards only.
7. Tenants will be given electronic key fobs/keycards based on information on file with the landlord.
8. Tenants and lawful occupants are to receive free electronic key fobs/keycards. In this regard, there is no limit to the number of key fobs/keycards which may be issued for an apartment. Occupants of the apartment include children who are to be issued key fobs/keycards if their parent/guardian requests it. Tenants may also receive up to four additional key fobs/keycards at no charge for employees and/or

---

<sup>40</sup> See Exhibit 1 (Owner’s Application) at page 2; see also Exhibit 2 (Owner’s April 8 Letter) at pages 5-6 (stating that the “facial recognition system is much more than an adequate substitute for a key fob system”).

<sup>41</sup> See Exhibit 1 (Owner’s Application) at page 2, (citing to Matter of Court, *supra*; Matter of the Administrative Appeal of Aulov/Mosheyev, DHCR Admin. Rev. Docket No. DX110002RT, December 21, 2016; Matter of Sanders, *supra* *aff’d* Stuyvesant Town-Peter Cooper Village Tenant’s Assoc. v. Metropolitan Life Ins. Co., 12 Misc.3d 1194(A) (Sup. Ct., N.Y. Co. 2006); Matter of the Administrative Appeal of Said, DHCR Admin. Rev. Docket No. FO430069RT, March 21, 2018.

<sup>42</sup> See Exhibit 2 (Owner’s April 8 Letter) at pages 5-6.

guests. Guests include family members and friends, who can be expected to visit on a regular basis or visit as needed to care for a tenant or the apartment if the tenant is away. Employees, who may be contractors, professional care givers, etc. may have an expiration date electronically placed on the key fob/keycard, which may be extended upon request of the tenant.

10. Each person receiving a key fob/keycard is required to sit for a photo to be electronically associated with such key fob/keycard in the security system database; however, minors are not required to have their photo taken.
11. Individuals obtaining a key fob/keycard must provide appropriate proof of identity, but the owner may not record any data (i.e., driver's license number).
12. Owner may not request or retain, in any form, the social security number of more than one tenant or legal occupant for each apartment unless the security deposit is kept in a joint type of an account.
14. The only information to be stored in the system database is the key fob/keycard holder's name, address, and picture. No other personal information is to be stored in the database and the database may not be linked to any other database where personal information of residents is to be stored.<sup>43</sup>

Importantly, in this case, unlike the key fob/keycard for metal key cases, the Owner is not even replacing the current key fob system. Facial recognition technology is simply an additional, unnecessary invasive layer which the Owner has yet to establish provides any additional or needed security.

The Court of Appeals has held that the “rent-stabilization program is an exceptional regulatory scheme that enables a specifically targeted group of tenants to maintain housing in New York City” and that “the rent-stabilization laws . . . provide a benefit conferred by the government through regulation aimed at a population that the government deems in need of protection.”<sup>44</sup> The Court concludes that “[a]ffordable housing is an essential need.”<sup>45</sup> To

---

<sup>43</sup> Exhibit 2 (Owner's April 8 Letter) at Exhibit E; see also Matter of Court, *supra*; Matter of Sanders, *supra*; Matter of the Administrative Appeal of Benish, DHCR Admin. Rev. Docket No. FO430024RT, September 20, 2017.

<sup>44</sup> Matter of Santiago-Monteverde, 24 N.Y.3d 283, 291 (2014).

<sup>45</sup> Id. at 292.

mandate the surrender of tenants' biometric data to their landlord as a quid pro quo to maintaining access to their rent-stabilized apartments is surely not in the spirit of, nor consistent with, the Rent Stabilization Law and Code. Such violation of the privacy and civil liberties of rent-stabilized tenants is an entirely untenable position. While a regulatory scheme, the Rent Stabilization Law and Code undoubtedly are not meant to regulate tenants' biometrics, and certainly not landlords' unfettered control of and access to tenants' biometrics.

Accordingly, HCR should reject the Owner's application in its entirety and find that facial recognition technology is not an adequate substitute for the existing security system.

**I. THE PROPOSED SYSTEM DOES NOT PROVIDE ENHANCED SECURITY**

It is clear the only security threat the Owner appears to be concerned with by proposing to install face recognition technology is the financial security of his investment, not the safety and well-being of the tenants at Atlantic Plaza Towers.

The Owner has not been able to identify a single security or safety issue at Atlantic Plaza Towers that is not fully addressed by the current security system, other than to trump up the hypothetical future threat of key fob duplication in an attempt to support the hollow claim that the proposed facial recognition security system will provide greater security to the building and tenants than currently exists. In Matter of Sanders et al., the seminal HCR key fob/keycard decision, a major component of HCR reasoning in finding key fob/keycard systems to be an adequate substitute for metal key locks was that the new security system was "a clear-improvement in security."<sup>46</sup> On the contrary, the installation of facial recognition technology at Atlantic Plaza Towers will provide no significant additional security benefit and will fail to address any security gaps that in fact do exist in the current system.

---

<sup>46</sup> Matter of Sanders, supra.

The level of security touted in Matter of Sanders, where HCR accepted the NYPD opinion that access control cards equipped with photo identification capability would increase the level of security,<sup>47</sup> already exists in the current security system. The key fob system is already assigned to individual tenants and their movement is already tracked and stored in an access control database capable of generating a report of each tenant's movement into the building. The high-tech surveillance cameras in the lobby and throughout the building further track movement in the building and are also capable of providing photo identification. In the last ten years, tenants have not faced any significant safety concerns, and the current security system is able to effectively address any security risks in the building. For instance, when someone was stealing packages delivered to tenants, the security cameras swiftly helped the Owners identify and stop the individual from committing further theft.

The only reason provided by the Owner to justify this drastic addition of a facial recognition system is that key fobs can now more readily be duplicated. During the February 7 meeting between the Owner and a group of tenants, the Owner's security representative, Mr. Keeling made this assertion, and this claim is also made in the Owner's Application, which attaches screenshots of two websites, Clone My Key and Key Card Ninja, seemingly picked at random, that no tenant at Atlantic Plaza Towers is alleged to have used.<sup>48</sup> When asked directly whether any illicit key fob duplication had occurred, the Owner could point to no security incident involving a duplicate key fob at Atlantic Plaza Towers. In fact, the only example of key fob duplication that the Owner could point to during the February 7 meeting occurred at another property he owned in Manhattan, and it involved a tenant copying key fobs in order to rent their unit on the AirBnB website.

---

<sup>47</sup> See id.; see also Stuyvesant Town-Peter Cooper Village, 12 Misc.3d 1194(A).

<sup>48</sup> See Exhibit 1 (Owner's Application).

Ironically, despite pointing to the threat posed by key fobs as the main justification for the proposed system, key fobs will continue to be a major component of the buildings' security system. At the February 7 meeting, the Owner explained that the proposed system will not entirely replace the current key fob entry system. The StoneLock terminal will be placed at the second entrance door to enter the area where the 24-hour attendant is stationed, but a key fob will still be required to enter the third door, the parking garage, and the back entrance to the shared courtyard. In Matter of the Administrative Appeal of 120 West 97th Street, one of the conditions set by HCR was that "[e]ntry to the building, garage and laundry rooms will be accessed by electronic key cards only."<sup>49</sup> Conditions such as this imposed by HCR ensured that the key fob/keycard system was enforced uniformly and that that building actually benefitted from the enhanced security provided by the new system. Here, the fact that the Owner's proposed modification would still require tenants to use their key fob to fully access the building and surrounding amenities begs the question: how much added security could the StoneLock Gateway at the first entry point of the building possibly be providing?

The answer is that the proposed system does not provide any enhanced security, and could in actuality diminish the security proffered to tenants in light of the unanswered questions with respect to accuracy and bias.<sup>50</sup> Further, the proposed system does nothing to address the actual gaps in the current security system. Without a properly staffed security detail at the front desk, tenants will still continue to be forced to wait for someone to open the door every time the facial recognition system fails to permit access. Guests and any unauthorized persons will still be able to follow a tenant that opens the door into the building. And the door will remain wide open

---

<sup>49</sup> DHCR Admin. Rev. Docket No. XH410021RT et al., July 6, 2011; see also Exhibit 2 (Owner April 8 Letter) at Exhibit E ("Entry into the building may be accessed by electronic key fobs/keycards only.").

<sup>50</sup> See Proposed Security System, supra pages 12-15.

in a blackout, just as has been in the past because both the current key fob system and the newly proposed facial recognition system operate on electricity. When asked the same question in several different ways—what additional security benefits does this proposed facial recognition system offer—the Owner admitted that other than addressing potential key fob duplication, no improvement in security would be reaped by the tenants.

What the Owner did confirm would be gained by the installation of a facial recognition entry system was ensuring that the “right” people are entering the building. Responding to a tenant’s question asking why he chose Atlantic Plaza Towers amongst the dozen residential complexes he owns for the installation, the Owner said that the proposed facial recognition technology was in line with the recent renovations completed to the lobbies of the two buildings to attract new tenants to fill the vacant units in the building. Attracting new tenants to a gentrifying community for profit is not remotely close to the same thing as providing the tenants currently residing at Atlantic Plaza Towers with greater security, nor should it serve as the basis for a modification of services that will adversely impact the tenants.<sup>51</sup>

The proposed facial recognition system does not only exploit tenants for the purpose of profiting the Owner, but they are further exploited for their biometric information to improve the StoneLock facial recognition algorithm. The StoneLock product is a machine-learning system, whose algorithmic performance is trained by the input of diverse biometric information. In the end, StoneLock profits from an improved algorithm that it can use to market future sales—

---

<sup>51</sup> Additionally, should HCR approve this modification, on top of using the facial recognition system and control of the tenants’ biometric data to increase his profits, the Owner could additionally attempt to pass the costs of the security system onto the tenants through a Major Capital Improvement by later arguing that the modification was not only an adequate substitute, but in fact an improvement. Such a result would be unfathomable.

profits that the tenants to whom the biometric data belongs and from whom the data is mined, will never see.<sup>52</sup>

Without any evident security improvements made by the proposed facial recognition system, the only actors to benefit from its installation are the Owner and StoneLock in the form of money—definitely not the tenants who will not be any safer in their homes than they are now.

If the Owner genuinely wanted to improve the security at Atlantic Plaza Towers and his true concern is speculative widespread duplication of key fobs, then he could start by upgrading the 10-year old key fob system. Just like any technology, key fob entry systems are regularly improved and upgraded by their manufacturers to ensure better service and quality and there are key fob systems that are extremely secure (to the extent the current system is proven not to be). This would also address any vulnerability in the key fob entry points that is unaddressed with the proposed system. Even more simply, the Owner can reinstate a third security guard to ensure the security desk is in fact manned 24-hours a day and purchase a generator or battery that would maintain services in the event of a blackout. Installing unregulated and untested facial recognition technology that collects and stores the biometric data of a predominantly black and brown community should not be sanctioned by HRC in a residential building when other less invasive means are available.

**II. HCR CANNOT ESTABLISH ADEQUATE RESTRICTIONS TO A FACIAL RECOGNITION ENTRY SYSTEM FOR PROTECTING TENANTS AGAINST UNWARRANTED PRIVACY INVASION AND ABUSES BY THE OWNER**

The invasion of privacy inherent to a facial recognition entry system, owned and controlled by one's landlord, cannot be avoided or alleviated. In approving key fob/keycard systems as an adequate substitute for metal key locks, HCR addressed tenants' privacy concerns

---

<sup>52</sup> It is unclear whether the Owner stands to profit from any kind of arrangement with StoneLock for access to what amounts to a 718 unit data set.

by setting specific conditions to safeguard tenants' personal and confidential information.<sup>53</sup>

HCR has consistently held that any database or record keeping associated with or used in conjunction with the key fob/keycard system may not contain any tenant's confidential or personal information.<sup>54</sup> Such sensitive information not to be recorded or photocopied includes: "Social Security number,"<sup>55</sup> "driver's license numbers and passport numbers"<sup>56</sup>, "identification papers . . . whether redacted or not,"<sup>57</sup> and "birth certificate[s]."<sup>58</sup>

Here, such restrictions are emphatically unattainable. A facial recognition entry system necessitates the collection and recording of information far more personal and confidential than a driver's license or passport number—a tenant's biometric data. Without recording this information, the system is literally unworkable. Therefore, the measures that HCR put in place with respect to the modifications from a metal key to a key fob/keycard to protect against privacy invasion and abuses by the owner will be ineffective as to the proposed facial recognition system. As a result, to approve the installation of such a system, HCR will have to determine that it is consistent with the rent laws for the Owner to collect and record sensitive personal

---

<sup>53</sup> See Matter of Court, *supra* (holding that "the Rent Administrator's order establishes adequate restrictions for protecting the tenants against unwarranted privacy invasion and abuses by the owner").

<sup>54</sup> See e.g. Matter of Sanders, *supra*; Matter of Court, *supra*; Matter of Benish, *supra*; Exhibit 2 (Owner's April 8 Letter) at Exhibit E.

<sup>55</sup> See, e.g., Exhibit 2 (Owner's April 8 Letter) at Exhibit E; Terrace Court Tenant's Ass'n v. Terrace Court, LLC, Index No. 103382/2005 (Sup. Ct., N.Y. Cnty. Aug. 25, 2005) (holding that "while this Court finds that defendant has the right to request picture identification from the occupants of its building prior to distributing the keys to them, defendant has not established either a legal right or a compelling need to mandate disclosure of their social security numbers"). The only exception to the prohibition against collection of Social Security numbers is as to the tenant of record who is owed the security deposit, as that information was presumed to already be included in the tenant file at the time of the modification.

<sup>56</sup> Matter of Sanders, *supra*.

<sup>57</sup> Matter of Benish, *supra*.

<sup>58</sup> Id.



information from thousands of tenants, occupants, guests, and employees, a stark departure from previous precedent. Such a determination will need to be made against the backdrop of a barren landscape of regulation, where no laws or rules exist regarding the Owner's obligations in collecting, storing, and sharing the tenants' information.

**A. Biometric Data Is Personal Identifying Information That HCR Has Restricted Owners From Collecting And Retaining**

The Owner would like HCR to believe that biometric data is the equivalent of a photograph. The Owner, in its application, baldly concludes that "as DHCR has found that it was reasonable to require each individual receiving a key fob to sit for a photo to be electronically associated with the key fob in the landlord's database, use of the facial recognition system is likewise reasonable."<sup>59</sup> What exactly is so similar is unclear. What is clear, however, are the stark differences between a photograph and biometric data.

It is universally understood that "biometric data typically refers to any information that is used to identify a natural person based upon unique physiological identifiers (e.g., fingerprint, face, eye, or voice)."<sup>60</sup> The Owner's proposed "biometric security and identity verification system"<sup>61</sup> identifies a person based upon the biometric data (the unique physiological identifier) of his/her face. Notably, biometric data is further considered to be personal identifying information, "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable

---

<sup>59</sup> See Exhibit 1 (Owner's Application) at page 2.

<sup>60</sup> Jonh T. Wolak, Mitchell Boyarsky, and Randy A. Gray, Daniel J. Tucker, Outside Counsel, *The Biometric Standards: How New York Measures Up in the Face of Biometric Use Regulations*, NYLJ, Jun. 4, 2018 at S3, col 1.

<sup>61</sup> See Exhibit 1 (Owner's Application).

to a specific individual.”<sup>62</sup> In the context of HCR precedent, biometric data is more aptly compared to a unique identifier such as a Social Security number or driver’s license number or passport number in that it is associated with one individual. Even this is inaccurate and inadequate, as biometric data cannot be simply reissued, and therefore the ramifications of having one’s biometric data compromised mandates an even higher threshold of restriction and oversight.

Once the proper comparison is thus made, that between biometric data and personal and confidential information (as opposed to a photograph),<sup>63</sup> it becomes clear that the proposed facial recognition entry system cannot comply, as the Owner has asserted, with the conditions set by HCR in its findings that key fob/keycard systems are adequate substitutes for metal key locks. HCR have been very clear that for a modification to be lawful, an owner is prohibited from collecting and/or associating personal information in a security system in order to safeguard a tenant’s privacy and identity.

This incompatibility between the proposed system and HCR precedent is highlighted further when applied to minors. It is well-established that tenants in rent-stabilized apartments are entitled to keys for each occupant over the age of ten (10) at the request of a

---

<sup>62</sup> U.S. General Services Administration, Rules and Policies - Protecting PII - Privacy Act, <https://www.gsa.gov/reference/gsa-privacy-program/rules-and-policies-protecting-pii-privacy-act> (last updated Sep. 24, 2018); see also An Act relative to consumer data privacy, Bill No. 120, Massachusetts Senate (2019) (states that “personal information” includes pseudonymized information because it “is capable of being associated with [...] a particular consumer.”).

<sup>63</sup> Moreover, even assuming arguendo that biometric data is similar to a photograph, HCR precedent has justified permitting the taking of photographs because there “is a clear improvement in security and that as the inconvenience to the tenants to take a few moments to have their photographs taken, is limited possibly to a single occasion” (Matter of Sanders, supra), and “whatever inconvenience a tenant may incur in having to have his photograph taken is more than compensated by the security that is provided by the card key system” (id.). Here, there is no improvement in security demonstrated by the Owner, see Point I, infra, and the collection of biometric data will be daily and continuous.

parent/guardian.<sup>64</sup> However, although entitled to a key fob, minors do not have to sit for a photograph, as HCR has invariably set conditions “which prohibit the recording of data and the photographing of minors.”<sup>65</sup> Without being able to record any data or take a picture of the minor tenant, the proposed facial recognition system cannot operate. What follows, of course, is the question, how will the Owner or HCR be able to protect the privacy rights of minors while still permitting entry of minors into the building? The Owner has conveniently and characteristically not offered an answer, and HCR cannot set any restrictions to do so with respect to the proposed modification as it did in connection with the key fob/keycard systems.

**B. Lack Of Regulation Leaves Tenants Susceptible To Abuses By The Owner, Law Enforcement, Or Other Third Parties**

The collection, use, and storage of biometric data by the Owner pose significant risks to the tenants’ individual privacy rights, particularly where the Owner has not shown any good faith efforts to address the tenants’ legitimate privacy and civil liberties concerns or implement any protective measures against a data breach. Facial recognition entry systems should not be deployed in residential buildings, particularly without rigorous standards for automated facial analysis systems, mandatory accuracy and bias testing, and a process in place for regularly informing the public about the complications associated with the use of such technology. Particularly alarming is the lack of any regulation in New York for the use of biometric data or facial recognition systems. Illinois is the first state to have passed any such regulation, providing a private right of action to those whose biometric data is compromised or collected without their

---

<sup>64</sup> See Matter of the Administrative Appeal of Various Tenants of 1048 Union St., DHCR Admin. Rev Docket No. UK230058-RT, Apr. 27, 2007.

<sup>65</sup> Matter of Benish, *supra*.

knowledge and consent by a company subject to the regulation.<sup>66</sup> Texas and Washington followed suit with their own attempts to regulate this new frontier of technology.<sup>67</sup>

Without any regulation in place to protect tenants before or after a data breach, tenants are left susceptible to identify theft, which is already a very real and serious threat to a person's ability to recover in low-income communities of color. Biometric identifiers, like facial heatmaps, reveal sensitive information, not only because they are unique characteristics, but because they are permanent. A data breach would expose tenants whose biometric data is stored with the Owner to severe privacy and security threats. Even if the StoneLock facial recognition system stores only an encrypted reference file, or authentication code, and not the actual biometric identifier, the growing rate of data breaches across commercial industries cast serious doubts on claims that the biometric information the tenants provide will always be safe.<sup>68</sup> Most distressing is the fact that, unlike a compromised password or stolen credit card and bank information, a person's biometric identifier can never be replaced.<sup>69</sup>

---

<sup>66</sup> See Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/1 et seq. (West 2016) (BIPA requires the private entity obtain a written release from the individual after it notifies individuals of the use of their biometric identifiers or biometric information and inform them of the period for which it will be collected, stored, and used.).

<sup>67</sup> See Tex. Bus. & Com. Code § 503.001(a) et seq. and Rev.Code Wash (ARCW) §19.375 et seq.

<sup>68</sup> See Charles Warzel & Stuart A. Thompson, *Tech Companies Say they Care*, NY Times, Apr. 10, 2019, <https://www.nytimes.com/interactive/2019/04/10/opinion/tech-companies-privacy.html>; see also Danny Palmer, *The Hacking Strategies that will Dominate 2019*, ZDNet, Feb. 15, 2019, <https://www.zdnet.com/article/the-hacking-strategies-that-will-dominate-in-2019/>.

<sup>69</sup> See Claire Gartland, *Biometrics are a Grave Threat to Privacy*, NY Times, Jul. 5, 2016, <https://www.nytimes.com/roomfordebate/2016/07/05/biometrics-and-banking/biometrics-are-a-grave-threat-to-privacy> ("[I]nstead of credit monitoring, will breached companies offer their customers plastic surgery?").

Furthermore, other than the Owner’s pinky promise that it will not share the data collected,<sup>70</sup> there is nothing protecting the tenants from the Owner sharing such data with governmental agencies such as the NYPD or ICE, with or without a subpoena, or selling it to third-parties. The Owner attempts to direct attention away from its decisive control over the tenants’ data by focusing on the fact that StoneLock system is a “closed system” and that “StoneLock does not have access to the data.”<sup>71</sup> However, even if true, whatever StoneLock may or may not be able to do is not determinative: the Owner is the customer who, even according to StoneLock’s self-serving statement, is the only entity with access to the data.<sup>72</sup> And, again, there are currently no laws in New York State regulating what the Owner may choose to do with that authority.

Even more, the Owner misleadingly claims that the data collected by the StoneLock system is “worthless.”<sup>73</sup> It does so by making the seriously flawed assertion that the biometric data is pseudonymized and cannot be “reverse engineer[ed]” to identify a particular individual. For one, the pseudonymized data is linked to a specific tenant at Atlantic Plaza Towers, whose movement is tracked by the face scan of their physical unique identifier—which is why the data is only “pseudo-anonymous.” Moreover, the perfectly centered, clear photo images captured by the StoneLock facial recognition system at enrollment—which the Owner and StoneLock conveniently fail to mention—is associated with data tracking the tenant’s movement and will be ripe for use by law enforcement agencies to target tenants at Atlantic Plaza Towers.

---

<sup>70</sup> See Exhibit 2 (Owner’s April 8 Letter) at page 4 (“Neither the owner nor the system interacts, or shares data, with NYPD or ICE.”). Notably, the Owner did not address how it would or would not share the data in the Owner’s Application, and even in its April 8 Letter, it does not disavow sharing any data with third-parties other than law enforcement.

<sup>71</sup> Id.

<sup>72</sup> Id. (“Only the owner of the system has access to the data.”).

<sup>73</sup> Id.

Additionally, there is currently nothing to stop the widespread installation of StoneLock Go devices, including for use by law enforcement agencies which could use the data collected by the Owner to be scanned by their own StoneLock Go device. Something like this has already begun to happen at airports around the country where third-party airlines are using facial recognition scans that utilize data collected by the government.<sup>74</sup> In the fast-paced, ever-changing world of technology, what is “worthless” today will certainly not remain so tomorrow.

Without legislation governing the collection, storage, or use of biometric information, the tenants have no meaningful recourse to make themselves whole again should the Owner’s negligence lead to a data breach or should it share the data with a third-party. Although HCR may, as it has previously done in key fob/keycard cases, impose a condition that the Owner is prohibited from sharing the data collected with any third-parties, the tenant’s only remedy for a violation of that restriction would be to seek a rent reduction from HCR.<sup>75</sup> By no means is a rent-reduction order an adequate response to compromised biometric data, and the tenants respectfully assert that the limited scope of HCR’s jurisdiction and authority means that it cannot be the front-line of implementing regulation of this technology.

---

<sup>74</sup> See James Felton, *This Conversation Between a Passenger and an Airline Should Absolutely Terrify You*, IFLScience, Apr. 22, 2019, available at <https://www.iflscience.com/technology/this-conversation-should-terrify-you-viral-thread-about-airport-tech-is-creeping-out-the-internet/> (last visited Apr. 30, 2019).

<sup>75</sup> See Matter of Court, *supra* (“[S]hould the owner violate any of the terms and conditions established in the Rent Administrator’s order, the tenants may file an application for a rent reduction with the agency.”).

### **III. THE PROPOSED FACIAL RECOGNITION ENTRY SYSTEM VIOLATES THE RENT STABILIZATION LAW AND CODE**

#### **A. Requiring Tenants to Provide Their Biometric Data To The Owner Is a Change In The Terms And Conditions Of Their Lease**

An owner is required to offer a rent-stabilized tenant a renewal lease “on the same terms and conditions as the expired lease, except where the owner can demonstrate that the change is necessary in order to comply with a specific requirement of law or regulation applicable to the building or to leases for housing accommodations subject to the RSL, or with the approval of the DHCR.”<sup>76</sup> Repeated throughout HCR key fob/keycard precedent is that the approved modification does not constitute a change in the terms and conditions of a tenant’s lease because the keys would be provided “based on information on file with the [owner].”<sup>77</sup>

As discussed in Point I.A, surpa, in order to conclude that its proposed modification is consistent with Rent Stabilization Law and Code,<sup>78</sup> the Owner relies entirely on its faulty comparison that the biometric data collected by the proposed facial recognition system is the equivalent of a photograph. It states: “The tenants do not have to be concerned about pictures since the key fob system has already taken pictures.”<sup>79</sup> As an initial matter, this is an outright lie. The key fob system was installed in or about 2009, almost a decade ago, and tenants were never required to sit for a photograph in connection with their key fob. The Owner only recently

---

<sup>76</sup> 9 N.Y.C.R.R. § 2522.5(g)(1); see Century Operating Corp. v. Popolizio, 60 N.Y.2d 483 (1983); David v. NYC Conciliation & Appeals Bd., 59 N.Y.2d 714 (1983).

<sup>77</sup> Exhibit 2 (Owner’s April 8 Letter) at Exhibit E; see also Stuyvesant Town-Peter Cooper Village, supra (“DHCR reasonably pointed out that Met Life would not obtain additional information from the residents of the complex that it does not already have or is now entitled to request.”); Matter of 120 West 97th Street, supra (“the data gathered by the owner for the new system is information the owner already has or is entitled to request”); Matter of Benish, supra; Matter of Court, supra.

<sup>78</sup> Exhibit 2 (Owner’s April 8 Letter) at page 5.

<sup>79</sup> Exhibit 2 (Owner’s April 8 Letter).

demanded that tenants take a photograph, for a new mailbox key for the newly renovated mailboxes, not for purposes of bolstering the key fob system. Reasonably, not understanding the connection between a mailbox key and a photograph, not all tenants complied, and there remain tenants who still have not received a mailbox key, and others who refused to take a photograph but were given a key. And, not surprisingly, the Owner rolled out this newly hatched mailbox key photograph requirement in July and August 2018, after the Owner had filed the instant application, in an effort to lay a foundation for the Owner's argument that it is not demanding anything new from tenants in connection with its proposed modification.

Furthermore, as explained in more detail infra, even if the Owner did have a photograph in each tenant's file, a tenant's biometric data is not a photograph and is new information not currently "on file" with the Owner. As StoneLock makes clear, "[a]ll users of StoneLock products" will need to be "authentica[ed] by StoneLock Products,"<sup>80</sup> which Mr. Keeling explained on February 7 would require the system to "learn" about the tenants. Further, the StoneLock system registers and utilizes a user's biometric data and separately captures a JPEG photograph (a fact the Owner fails to disclose), which are distinguished in StoneLock's Privacy Policy.<sup>81</sup> Put simply, without the tenants providing any additional or new information, the proposed facial recognition system cannot function.

Accordingly, requiring tenants to provide their biometric data, which is personal and confidential information never before collected by the Owner, is a complete change in terms and conditions of tenants' leases in contravention with the Rent Stabilization Law and Code.<sup>82</sup>

---

<sup>80</sup> Exhibit 9 (StoneLock Privacy Policy) at page 2.

<sup>81</sup> See id. at 3 ("There is no biometric data derived from this [JPEG] photograph by a StoneLock product.").

<sup>82</sup> See Matter of Sanders, supra (holding that the building's new electronic card key access system "does not constitute a change in the terms and conditions of the lease, as the evidence



**B. A Facial Recognition Entry System Will Decrease Or Limit Lawful Access To The Subject Premises**

Mandating the submission of one's biometric data in order to enter a building naturally diminishes access to the building. When such a building is residential, the resulting restricted access is further complicated and problematic. Where HCR has approved a keyless entry system as an adequate substitute for metal key locks, the agency has qualified that in addition to each tenant and lawful occupant receiving a key fob/keycard, tenants are to be issued four additional key fobs/keycards at no charge for the use of tenants' guests and invitees.<sup>83</sup> HCR has issued rent reductions where owners have refused to provide such keys, finding the owner's actions "were unjustifiably restrictive and interfered with the tenant's rights and access to the subject building."<sup>84</sup>

The manner in which the Owner addresses this issue reflects its misunderstanding of what is required under HCR precedent, stating: "[f]riends, family and home health aides will be able to enter the building. There will be no loss of quiet enjoyment because the intercom system will continue to provide entry to those who do not live at the property."<sup>85</sup> Family, friends, and employees such as home health aides should not be relegated to use of the intercom system and the presence of the security guard to let them in, particularly for elderly tenants or tenants with

---

shows that there will be no recording of driver's license numbers and passport numbers, etc."); Stuyvesant Town-Peter Cooper Village, *supra* at \*3 ("DHCR reasonably pointed out that Met Life would not obtain additional information from the residents of the complex that it does not already have or is now entitled to request.").

<sup>83</sup> See Matter of Sanders, *supra*; Matter of 120 West 97th Street, *supra*; Matter of Court, *supra*; Matter of Benish, *supra*; Exhibit 2 (Owner's April 8 Letter) at Exhibit E.

<sup>84</sup> Matter of the Administrative Appeal of Akelius Real Estate Mgmt, LLC, Admin. Rev. Docket No. EV210029RO, issued July 13, 2017.

<sup>85</sup> Exhibit 2 (Owner's April 8 Letter) at page 2.

mobility issues or other disabilities. Tenants have the right to provide the key to their building to their friends and family, to allow access to their apartments whether or not they are present.

All that HCR has required that guests and invitees present to an owner is a government-issued photo-ID card in order to receive a key fob/keycard.<sup>86</sup> Here the Owner is asking HCR to provide it with permission to collect biometric data from each and every guest and invitee that enters the building. Not only that, but the StoneLock system will take and store JPEG photographs of every person who enters the building, whether an authorized user or not. This imposition will necessarily have the effect of decreasing and limiting lawful access to the buildings. Friends and family may choose not to visit frequently, or decline to care for a tenant or their apartment in order to avoid the intrusive nature of the facial recognition entry system. The tenants have the right, under Real Property Law 235b, to have a roommate, and some need a roommate in order to afford their rent; will a Craigslist post for a roommate now have to disclose “you will have to provide biometric data to the landlord”? Should multiple, ever-changing home health aides have to register as a “user” of the StoneLocke system to care for tenants? The pictures of FedEx and food delivery persons taken and stored? All of the privacy concerns outlined above with respect to tenants are now extended to an innumerable group of people who touch Atlantic Plaza Towers in a multitude of ways.

The Owner’s request to collect biometric data from each and every guest, invitee, or employee of the tenants is a significant departure from HCR precedent and can have no other result than to decrease or limit lawful access to the buildings. This proposed expansion of the Owner’s rights over the tenants’ should be denied by HCR.

---

<sup>86</sup> See Matter of Said, *supra*; Matter of Sanders, *supra*; Matter of Benish, *supra*.

**C. The Tenants, Not The Owner Or HCR, Should Have Agency Over Their Biometric Data And Whether And To Whom It Is Shared**

Even if validation studies exist showing the StoneLock system is fully accurate and unbiased, the current administrative proceeding reflects a state agency deciding, at the behest of a landlord, whether or not a tenant should be forced to surrender their biometric information. Such a process raises public policy concerns surrounding the level of agency that these tenants, primarily people of color, should have over their own biometric information.

Consent and biometric data go hand-in-hand where regulation over this data exists. Illinois' BIPA and the European Union's General Data Protection Regulation ("GDPR"), both require explicit consent from an individual before their biometric data is collected, used, or retained.<sup>87</sup> GDPR goes even further by designating biometric data, such as face scans, as "sensitive data" that is subject to special protections that give people control over their biometric data.<sup>88</sup> Yet, the Owner has made it clear that "residents would not be given the option to opt out of security protocols" if HCR permits the installation of the proposed facial recognition entry system,<sup>89</sup> and nowhere in its Application or April 8 Letter does the Owner state that it intends to seek written consent from the tenants before collecting, using, and storing their unique biometric identifier. This position is even contradictory to StoneLock's Privacy Policy, which boasts

---

<sup>87</sup> BIPA 740 ILCS 14/15(b)(3); EU General Data Protection Regulation (GDPR) 2016/679, OJ 2016 L 119/1, Art. 9.

<sup>88</sup> GDPR, Art. 9.

<sup>89</sup> Exhibit 8 (*Facial recognition planned for Brooklyn apartment building outrages tenants*, amNewYork).

compliance with BIPA and GDPR and advises customers to “include an explicit consent” in the process of registering a user to its facial recognition system.<sup>90</sup>

Ultimately, if HCR is to approve the Owner’s Application, the only way that tenants would retain their agency over their biometric data would be to move from their homes, where some have lived for decades and raised generations of family. Forcing tenants into such a position would be tantamount to agency-sanctioned waiver of the invaluable benefit of a rent-stabilized apartment, which is expressly against public policy. Even then, whether tenants would even meaningfully have the option to decline and move out is unclear in light of the current housing crisis in New York, where it affordable housing is a challenge. Such a result, cannot be consistent with the rent laws.

#### **IV. FURTHER SURVEILLANCE FROM FACIAL RECOGNITION TECHNOLOGY IS A TANGIBLE HARM AND INTERFERES WITH A TENANT’S RIGHT TO QUIET ENJOYMENT**

The Owner’s installation of facial recognition technology will only serve to further surveil a group of black and brown tenants, for whom privacy concerns are a very real threat. Whether the act of surveillance is at the hands of private actors or the state, it “is often the gateway to very tangible harms.”<sup>91</sup> In addition to surveillance by law enforcement that too often ensues in violence, black and brown communities are only further pushed to the margins because surveillance and the feeling of being watched generates a fear and uncertainty that leads people to “self-police” and it inhibits activity in the public space.<sup>92</sup>

---

<sup>90</sup> Exhibit 9 (StoneLock Privacy Policy) at page 2. It is worth noting, even with this self-declaration of compliance with the BIPA and GDPR, that StoneLock can alter its Privacy Policy at any given time, as is the regular practice of technology companies today.

<sup>91</sup> Chris Gilliard, *Privacy’s not an abstraction*, Fast Company, Mar. 25, 2019, <https://www.fastcompany.com/90323529/privacy-is-not-an-abstraction> (last visited Apr. 30, 2019).

<sup>92</sup> See id.

The current security system, which effectively tracks the every movement of tenants in and out of the building, has already accomplished a chilling effect on the tenants. The Owner has engineered a comprehensive surveillance system that extends to almost every inch of Atlantic Plaza Tower, allowing the Owner to collect an incredible amount of information on the private lives of the tenants. This has ensued in tenants self-policing, which has chilled tenant participation in the Tenant Association and community activities. Tenants are afraid to open their doors to neighbors or advocates knocking, or attend meetings in the community room lest they be seen by the Owner on camera. Tenants have reported having to be cognizant of what they are wearing in order to throw away their garbage down the hallway, and tenants expend energy restraining themselves from engaging in activities that they do not want others to see, such as something as seemingly trivial as singing or dancing by themselves in the elevator after a good day at work.

While the mere presence of the cameras is enough to impede on the quiet enjoyment of their homes, the Owner goes further, actively using the information collected from its security system to harass and threaten tenants. Receiving a letter from the Owner with an accompanying screenshot of themselves from the building's security cameras is an everyday occurrence across the two buildings. From garbage removal to balcony décor, weekend guests to hallway goings-on, the Owner is not pleased with what it sees. Within days of the alleged misconduct, tenants find a letter slipped under their door.<sup>93</sup> Tenants have also received letters where the Owner includes a screenshot of the tenant carrying a large cardboard box into their apartment, and the

---

<sup>93</sup> See, e.g., Letter from Owner's General Manager Kevin Rafferty to Maria Cardenas, dated Mar. 14, 2013 and Letter from Owner's General Manager Kevin Rafferty to Courtney Williams, dated Apr. 19, 2019, both attached hereto as **Exhibit 10**.

Owner demands to know what the box contains. Moreover, the Owner does not just limit itself to policing what tenants do, but also monitors what tenants fail to do through its surveillance.

Unsurprisingly, the Owner has taken to using its security camera footage to threaten tenants for participating in lawful tenant organizing activity, such as disseminating flyers for upcoming meetings and speaking with their neighbors in the lobby about the Owner's application to install facial recognition technology in their building. For instance, the Owner sent a letter, dated October 25, 2018, to tenants who had been organizing with screenshots of the security camera footage showing the tenants standing in the lobby of 249 Thomas S. Boyland.<sup>94</sup> Each of the five tenants who received the letter is identified by their apartment number, and the letter states in part, "Let me make something clear, this is not your building, you are a resident of our building."<sup>95</sup> On March 23, 2019, the Owner escalated its efforts to stifle tenant organizing by calling the police to control tenant movement inside the building.<sup>96</sup> Again, the tenants were in the lobby speaking with other tenants about their opposition to the Owner's application to install a facial recognition entry system in their buildings.

The proposed facial recognition system will add another layer of surveillance that will only further diminish the quiet enjoyment of their homes.<sup>97</sup> The act of surveillance already "intrudes upon people's rights to move about in public in relative obscurity if they so wish,"<sup>98</sup>

---

<sup>94</sup> Letter from Owner's General Manager Kevin Rafferty to various tenants, dated Oct. 25, 2018, attached hereto **Exhibit 11**.

<sup>95</sup> Id.

<sup>96</sup> Surveillance photographs of Mar. 23, 2019 provided by Owner's counsel to BLS, attached hereto as **Exhibit 12**.

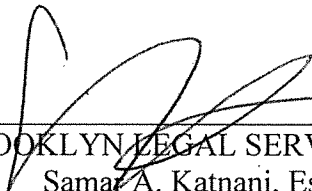
<sup>97</sup> 9 N.Y.C.R.R. § 2525.2(a) (it is unlawful for a person to engage in any course of conduct which "interferes with, or disturbs, . . . the privacy, comfort, peace, repose or quiet enjoyment of the tenant . . . or is intended to cause the tenant to vacate such housing accommodation or not exercise any right afforded to the tenant under this Code.")

<sup>98</sup> Christopher Gilliard, PhD, *Privacy's not an abstraction*, supra.

but this right is even greater when it comes to the privacy one is afforded in their home. The act of surveillance makes one feel they are being watched, which impedes on one's human dignity. The sanctity of the home is a fundamental right,<sup>99</sup> and HCR should protect these residential spaces from such intrusion.

Accordingly, for all of the reasons laid out above, the tenants urge HCR to support their rejection of an experimental facial recognition system from which HCR can provide no adequate protection and which violates the Rent Stabilization Law and Code.

Dated: April 30, 2019  
Brooklyn, New York



---

BROOKLYN LEGAL SERVICES  
By: Samar A. Katnani, Esq.  
Mona R. Patel, Esq.  
Elizabeth Reardon, Esq.  
*Attorneys for Atlantic Plaza Towers Tenants*  
105 Court Street, 4th Floor  
Brooklyn, NY 11201  
(718) 233-6393

---

<sup>99</sup> See Kyllo v. United States, 533 U.S. 27, 33 (2001) (recognizing that a home is a place “where privacy expectations are most heightened”).