Committee on Technology

Irene Byhovsky, Counsel

Charles Kim, Legislative Policy Analyst  
Sebastian Bacchi, Finance Analyst

Committee on Housing and Buildings

Austen Brandford, Counsel

Audrey Son, Counsel

Genan Zilkha, Counsel

Jose Conde, Senior Legislative Policy Analyst

Charles Kim, Legislative Policy Analyst

Sarah Gastelum, Principal Financial Analyst

Luke Zangerle, Financial Analyst

Committee on Consumer Affairs and Business Licensing

Balqees Mihirig, Senior Counsel  
Leah Skrzypiec, Policy Analyst

Andrew Wilber, Financial Analyst



# THE COUNCIL OF THE CITY OF NEW YORK

# COMMITTEE REPORT OF the Infrastructure Division AND THE GOVERNMENTAL AFFAIRS Division

*Jeffrey Baker, Legislative Director*

*Terzah Nasser, Deputy Director, Infrastructure*

*Rachel Cordero, Deputy Director, Governmental Affairs*

**COMMITTEE ON TECHNOLOGY**

Hon. Robert Holden, Chair

**COMMITTEE ON HOUSING AND BUILDINGS**

Hon. Robert Cornegy, Chair

**COMMITTEE ON CONSUMER AFFAIRS AND BUSINESS LICENSING**Hon. Rafael Espinal, Chair

##### **October 7, 2019**

**Oversight:** Facial Recognition Technology and Biometric Data Collection in Businesses and in Residences

**INT. NO. 1170:** By Council Members Torres, Espinal, Rosenthal, Rivera, Moya, Rose, Cornegy, and Lancman

**TITLE:** A Local Law to amend the administrative code of the city of New York, in relation to requiring businesses to notify customers of the use of biometric identifier technology

**ADMINISTRATIVE CODE:** Adds a new subchapter 20 to chapter 5 of title 20.

**INT. NO. 1672:** By Council Members Richards and Kallos

**TITLE:** A Local Law to amend the administrative code of the city of New York, in relation to requiring real property owners to submit registration statements regarding biometric recognition technology utilized on the premises

**ADMINISTRATIVE CODE:** Adds a new chapter 12 to title 10.

**PRECONSIDERED INT. NO\_\_ :** By Council Member Lander

**TITLE:** A Local Law to amend the administrative code of the city of New York and the New York city building code, in relation to defining the term key and requiring building owners to provide keys to residential tenants

**ADMINISTRATIVE CODE:** Amends subdivision a of section 27-2004, amends section 27-2043.

**BUILDING CODE:** Amends section 1002.1.

1. **INTRODUCTION**

On October 7, 2019, the Committee on Technology, chaired by Council Member Robert Holden, the Committee on Housing and Buildings, chaired by Council Member Robert E. Cornegy, Jr., and the Committee on Consumer Affairs and Business Licensing, chaired by Council Member Rafael Espinal, will hold a joint oversight hearing on Facial Recognition Technology and Biometric Data Collection in Businesses and in Residences, and will also consider the following bills: (1) Int. No. 1170, in relation to requiring businesses to notify customers of the use of biometric identifier technology; (2) Int. No. 1672, in relation to requiring real property owners to submit registration statements regarding biometric recognition technology utilized on the premises; and (3) a Preconsidered Introduction, in relation to defining the term key and requiring building owners to provide keys to residential tenants.

Those invited to testify include representatives from the Department of Information Technology, the Department of Buildings, the Department of Consumer and Worker Protection, chambers of commerce, advocacy groups, community-based non-profit organizations, and other interested members of the public.

1. **BACKGROUND**

Technology is rapidly changing, especially when it involves the identification of individuals. Biometric identification has expanded from describing basic physical attributes to now include fingerprint scans, iris scans, retinal scans, voice recognition, DNA tests, and facial recognition.[[1]](#footnote-1) Additionally, newer biometric identification methods are regularly being developed, such as brain signal identification, heart pattern recognition, and finger vein pattern recognition.[[2]](#footnote-2)

Typically, there are two main classes of biometrics data that can be collected on individuals: (1) behavioral characteristics and (2) physiological characteristics.[[3]](#footnote-3)  Behavioral characteristics concern the behavior of an individual, while physiological characteristics concern the shape or composition of the body. Behavioral biometrics include an individual's keystroke, signature, and voice recognition.[[4]](#footnote-4) Physiological biometrics includes facial recognition, fingerprint scanning, hand geometry, iris scanning, and DNA.[[5]](#footnote-5) Facial recognition systems use an individual's physiological information such as facial structure, eye color, size, and shape.[[6]](#footnote-6)

1. **How Does Facial Recognition Technology Work?**

Facial recognition technology uses a complex technological process. Facial recognition technology can identify an individual from a digital image by comparing and analyzing facial patterns.[[7]](#footnote-7) This technology can also compare live captures of individuals or their digital image data to the record of the individual that is stored in the database.[[8]](#footnote-8)

Facial recognition technology begins when video cameras scan an area. Faces within a 35-degree angle of the camera can be extracted from the people in the monitored area.[[9]](#footnote-9) It takes only a split second for the camera to identify a face from among the other images it is monitoring.The software then measures between 14 and 22 of the approximately 80 nodal points that make up an individual's face.Nodal points are those facial features that make each face unique.Nodal points include such characteristics as depth of eye sockets, distance between eyes, and width of nose.Once these points have been identified, the nodal point measurements are turned into a comprehensive numerical code, which is called a faceprint.Within a minute, millions of faceprints can be compared to the database of stored faceprints.[[10]](#footnote-10) Different facial recognition systems can use slightly different methods.[[11]](#footnote-11)

In the past several years, underlying biometric technologies have consistently improved following increased investment and research in facial recognition systems.Newer systems have enhanced accuracy by incorporating neural networks, a machine-learning Artificial intelligence (AI) technique that is used to find an optimal function to solve a task from a large number of inputs.[[12]](#footnote-12)

Facial recognition technology allows for: (1) facial classification, by classifying the face into categories such as an estimation of gender, age or race; (2) verification, by comparing the similarity of previously stored faceprint of any particular individual to a new faceprint and establishing a confidence score that the two individuals are the same; and (3) identification, by comparing a person's facial image to a database of stored faceprints.[[13]](#footnote-13)

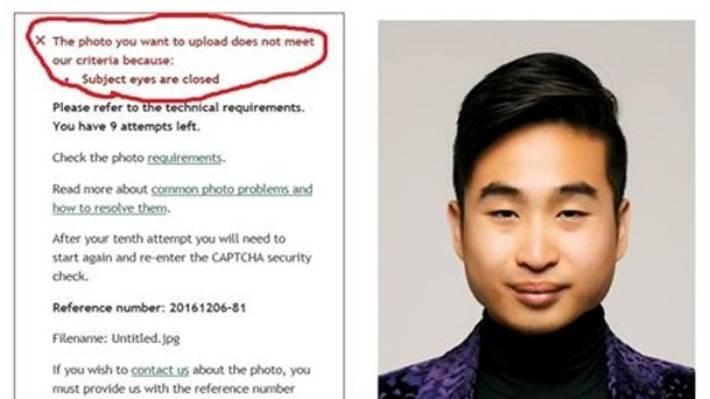
1. **Issues Related to Facial Recognition Technology**
2. **Technological Limitations**

Facial recognition technology is an evolving scientific and diagnostic tool with enormous potential. However, this technology does have limitations. Factors that can affect the accuracy of identification are poor image quality, unusual poses or facial expressions, and the age of the photograph; the more images a database has, “the greater the chance of such errors--either incorrect matches or failure to match photos of people already in the database.”[[14]](#footnote-14)

When these images meet certain professional scientific standards, the accuracy rate when comparing each to one another is high.[[15]](#footnote-15) However, the accuracy rate decreases when there is no standardized photo for comparison or when the comparison comes from a photo from an uncontrolled environment.[[16]](#footnote-16) In other words, when an individual has his or her face partially obscured, or is facing to the side rather than the front, or the lighting is not proper, the verification will be less reliable.[[17]](#footnote-17)

Moreover, even uses of facial recognition technology in controlled environments raise significant concerns about accuracy, especially for women, children, African Americans, and Asians for whom the existing facial recognition algorithms are known to be less accurate.[[18]](#footnote-18)

For example, a New Zealand man of Asian descent had his passport photograph rejected when facial recognition software mistakenly registered his eyes as being closed.[[19]](#footnote-19) The automated system told the 22-year-old engineering student that the photo was invalid because his eyes were closed, even though they were clearly open.[[20]](#footnote-20)



This phenomena can be explained by the use of advances in AI technology. The recent power of AI comes from the use of data-driven deep learning to train increasingly accurate models by using growing amounts of data. However, the strength of these techniques can also be their inherent weakness.

AI systems learn what they are taught. If they are not taught with robust and diverse data sets, accuracy and fairness could be at risk. The heart of the problem lies not with the AI technology itself, per se, but with how the AI systems are trained.[[21]](#footnote-21) For facial recognition to perform as desired ⁠— to be both accurate and fair ⁠— training data must provide a sufficient balance and coverage. The training data sets should be large enough and diverse enough to learn the many ways in which faces inherently differ.[[22]](#footnote-22) The images must reflect the diversity of features in faces we see in the world. Faces may differ according to age, gender and skin color but, as studies have shown, these dimensions are inadequate for characterizing the full range of diversity of faces. Dimensions like face symmetry, facial contrast, and the sizes, distances and ratios of the various attributes of the face (eyes, nose, forehead, etc.), among many others, are important.

Facial recognition systems that are trained within only a narrow context of a specific data set will inevitably acquire bias that skews its learning towards the specific characteristics of that data set. This narrow context appears as underrepresentation or over-representation of certain types of faces in many of the publicly available data sets. [[23]](#footnote-23) Moreover, because faces, unlike fingerprints or DNA[[24]](#footnote-24), change over time software can trigger incorrect results by changes in hairstyle, facial hair, body weight, and the effects of aging.[[25]](#footnote-25)

1. **Data Breach and Cyber Security**

As the use of facial recognition technology becomes more widespread it can give individuals or businesses the possibility to identify almost any person who goes out into public places, surreptitiously or otherwise, tracking movement, location and conduct. This will likely result in numerous private and public databases of information, which may be sold, shared, or used in ways that the consumer does not necessarily understand or consent to. These databases will likely be exposed to security failures and breaches, information leaks by careless or corrupt employees, hackers, or even foreign intelligence agency break-ins.[[26]](#footnote-26)

Biometric information is based on a unique physiological characteristic making it naturally stable and hard to artificially alter.[[27]](#footnote-27) Biometric information is part of a person’s identity. Unlike a password, this information cannot be changed. When cybercriminals access biometric data — fingerprints, retina, facial, or voice — they gain information that can be linked to the identity forever. The potential damage is irreversible,creating a constant fear of information or identity theft.

The expanding collection of data increases the risk of data breaches, which have been ever increasing.Large biometric databases, including the fingerprint database of the Office of Personnel Management, have already been hacked.[[28]](#footnote-28)

Other biometric databases, such as those containing faceprint data, are susceptible to hacking as well.  Earlier this year, the fingerprints of over 1 million people,[[29]](#footnote-29)[1] as well as facial recognition information, unencrypted usernames and passwords, and personal information of employees, were discovered on a publicly accessible database owned by the company Suprema, whose customers include British Metropolitan Police Service, defense contractors and banks.[[30]](#footnote-30)  The vulnerability was uncovered by internet privacy researchers Noam Rotem and Ran Locar who **identified a huge data breach in security platform BioStar 2, which is managed by Suprema.** Suprema describes itself as a "global Powerhouse in biometrics, security and identity solutions," with a product range that "includes biometric access control systems, time and attendance solutions, fingerprint live scanners, mobile authentication solutions and embedded fingerprint modules.” [[31]](#footnote-31) Suprema’s system was designed to provide centralized control for access to secure facilities like warehouses or office buildings. The system is integrated with Biostar 2 to enable the use of fingerprints and facial recognition as part of its methods to identify people attempting to gain access to buildings.[[32]](#footnote-32)

Other biometric databases, such as those containing faceprint data, are susceptible to hacking as well. Only this year, the fingerprints of over 1 million people,[[33]](#footnote-33) as well as facial recognition information, unencrypted usernames and passwords, and personal information of employees, were discovered on a publicly accessible database for the company Suprema, used by the likes of the British Metropolitan Police Service, defense contractors and banks.[[34]](#footnote-34) The internet privacy researchers Noam Rotem and Ran Locar discovered **a huge data breach in security platform BioStar 2, which is managed by Suprema.** Suprema describes itself as a "global Powerhouse in biometrics, security and identity solutions," with a product range that "includes biometric access control systems, time and attendance solutions, fingerprint live scanners, mobile authentication solutions and embedded fingerprint modules."[[35]](#footnote-35)

Its system allows centralized control for access to secure facilities like warehouses or office buildings. Biostar 2 uses fingerprints and facial recognition as part of its methods of identifying people attempting to gain access to buildings.[[36]](#footnote-36)

Alarmingly, stolen biometric identifiers could be used to impersonate consumers, gaining access to personal information and buildings. The use of biometrics for accessing sensitive personal information creates an increased risk of tangible and substantial harm when such information is stolen.

The privacy risks of data breaches may also lead to potential future harm even when stolen consumer data is not yet targeted to directly harm the consumer. The heightened alert following a data breach creates uncertaintly and a form of lost opportunities as individuals take actions to mitigate against and reduce any potential harms or transactional losses.[[37]](#footnote-37)

Although some argue that it is possible to overcome the problem of information leaks or hacks through appropriate security measures, recent sensitive data leaks, numbering hundreds of thousands of military, business, politician and public figures— suggests that nothing is safe.

1. **Privacy-related Issues**

In addition to concerns about data breaches, facial recognition technology also raises a number of privacy concerns. “Unlike other biometric identifiers such as iris scans and fingerprints, facial recognition is designed to operate at a distance, without the knowledge or consent of the person being identified. Individuals cannot reasonably prevent themselves from being identified by cameras that could be anywhere-on a lamppost across the street, attached to an unmanned aerial vehicle, or, now, integrated into the eyewear of a stranger.”[[38]](#footnote-38)

In New York City, as well as many other municipalities, establishments do not inform customers that facial recognition software is being used and it is unclear what companies or businesses do with the data once it has been collected. Information on customers, their behaviors, and their purchasing histories are highly valuable, and there have been numerous incidents of companies collecting this information and either selling it to, or having it harvested by third parties, without the knowledge or consent of consumers. The most recent high-profile case where these practices were employed involved Facebook and the political consulting firm Cambridge Analytica that closed its operations in 2018. It was reported that Cambridge Analytica had harvested information from 50 million Facebook profiles to gather data on voters for its clients involved in the pro-Brexit campaign and Donald Trump’s election.[[39]](#footnote-39) In a similar situation, consumers of the photo storage application Ever, found their images were being used without their explicit consent. The Ever app was marketed and used a cloud-based photo storage system. However, the company then used these photos to develop their own facial recognition software which they then sold to law enforcement, the military, and private companies.[[40]](#footnote-40)

Government agencies have also been accused of mining personal biometric data. For example, earlier this year the *New York Times* reported that Immigration and Customs Enforcement (“ICE”) used facial recognition software to mine state driver’s license databases.[[41]](#footnote-41) Similarly, data from consumer-based surveillance software such as Ring (which uses cameras to monitor a person’s doorbell and/or entryway), is also being shared with law enforcement. Ring, which is now owned by Amazon, has partnered with more than 400 local police departments to send requests for footage to Ring users, on behalf of the police. Users can deny the request, but if the request is granted, police are able to obtain consumer-recorded video footage, without the need for a warrant. In exchange, the police departments promote Ring as an important security device.[[42]](#footnote-42) Indeed, at least one police department in California has offered the Ring devices as a reward to members of the public, in lieu of cash, for information on crimes.[[43]](#footnote-43)

The ubiquity of facial recognition technology also raises serious concerns over where a person can expect a degree of privacy and anonymity. To demonstrate the ease at which this technology can be employed, the *New York Times* conducted its own facial recognition project of people in Bryant Park during an afternoon. They utilized footage taken from three cameras that publicly stream the happenings of the park and ran the images through facial recognition software that cost less than $100. Through this process, the team was able to detect 2,750 faces from a nine-hour period and, using a database created from publicly available photos, they were able to match identities.[[44]](#footnote-44) While being identified as being in Bryant Park one lunchtime might seem innocuous enough, there are dangerous ramifications. For instance, in Hong Kong, facial recognition has been employed by rival sides to identify both protesters and police.[[45]](#footnote-45)

1. **The Use of Facial Recognition Technologies**

Today, biometric technologies that are available for private sector usage are more accurate, less expensive, and readily available from cloud software providers.[[46]](#footnote-46) Fingerprint scanning, facial recognition, and iris scanning are used in everyday technologies such as cell-phones, ATM machines, retail stores, concert halls, and even for building access.[[47]](#footnote-47)

1. **Retail Sector**

Facial recognition is a rapidly growing biometric technology used in the retail sector.[[48]](#footnote-48) Facial recognition is viewed as an important tool in the toolbox of “the future of shopping,” with retailers already experimenting with its potential.Generally, the retail sector uses the technology to reduce theft and to personalize shopping experience.

Services such as FaceFirst offer facial recognition technology specifically targeted towards retailers using “surveillance ... and an underlying software platform that leverages artificial intelligence to [prevent] theft, [fraud,] ... and ... violence.”[[49]](#footnote-49) FaceFirst can scan faces as far as 50 to 100 feet away.[[50]](#footnote-50) When a person walks through a store's entrance, a video camera captures multiple images of the shopper, selects the clearest one, and adds their picture to the store's client database.[[51]](#footnote-51)  FaceFirst software compares that image with other images in its database. If a match occurs, either recognizing the shopper as a suspected shoplifter or important client, the software can alert store employees within seconds of the person's entrance into the store.After being added to the database, the software can recognize the customer on each subsequent visit to the store.Similarly, retailers can pre-set pictures of individuals they wish to track in the system such as individuals suspected of burglaries based on information from nearby stores or police records.[[52]](#footnote-52)

In 2015, Walmart tested a system that scanned the faces of all individuals entering several of its stores; the system could identify suspected shoplifters, and instantly alert store security on their mobile devices.[[53]](#footnote-53)  Target is one popular retailer that also tested facial recognition software “in a small number of Target stores to understand its ability to help prevent fraud and theft.”[[54]](#footnote-54)  Use of facial recognition, however, may not be limited to large national retailers.In March of 2018, the American Civil Liberties Union (“ACLU”) reached out to 20 of the biggest stores in the United States to ask if they use facial recognition technology: the resulting report stated that “of the 20 companies ... contacted, only one was willing to tell [the ACLU] that they don't use it.”[[55]](#footnote-55)

Many facial recognition products presently on the market focus on increasing security through automated facial recognition technology.However, this technology may be less effective as a security measure for private businesses because these businesses lack access to databases held by law enforcement agencies.Customer engagement and marketing capabilities of facial recognition are the projected valuable commodity for retailers. Facial recognition can be used by retailers to connect online with offline behaviors,[[56]](#footnote-56) provide more in-depth demographics, and track in-store product engagement. With this omnichannel approach retails can track “aggregated bits of data collected through loyalty programs, point of sale records and other sources.”[[57]](#footnote-57)

Further, by using multiple tracking technologies, retailers can manipulate the availability, cost, and appeal of an item.[[58]](#footnote-58) This type of pricing, in part, uses existing customer information to determine the ideal cost at which a shopper will purchase a particular product.Consumers provide retailers with this information “whenever they make a credit card purchase[,] ... use free e-mail services, surf [the Internet] for information[,] or engage in social media.”[[59]](#footnote-59) Moreover, retailers can purchase the data obtained by social media platforms, such as shoppers' e-mail addresses and other personal information.[[60]](#footnote-60) This information enables retailers “to develop a broad picture about a consumer, such as identifying that the individual owns a house, runs marathons, eats healthy food, has a premium bank card, and is good in financial health.”[[61]](#footnote-61) Connecting such data to a customers’ faceprint would allow retailers to inflate the price of a product to consumers in the store willing and able to pay more, while offering the same product to other consumers for less money. It is important to note that this information, mostly collected without consumers' knowledge or consent, allows retailers to charge individuals more or less money.

Most consumers remain skeptical about the use of facial recognition technology. A recent survey found that while 75% of consumers would decide not to shop at a shop that employs facial recognition, 55% would feel positively towards the marketing technology use if they themselves would benefit, for example in obtaining personalized discounts.[[62]](#footnote-62) Nevertheless, retailers with facial recognition technology could take advantage of this collected information to further maximize profits.[[63]](#footnote-63)

1. **Entertainment Venues**

As early as the early 2000’s, facial recognition technology has been on the rise at entertainment venues. In January 2001, facial recognition technology was installed at the Raymond James Stadium by the Tampa Police Department to scan the faces of Super Bowl attendees.[[64]](#footnote-64) Since then, this technology has proliferated, and is now used at several entertainment venues including Madison Square Gardens and Barclays Center.[[65]](#footnote-65) In 2018, Live Nation and Ticketmaster invested in Blink Identity, a company that specializes in military-grade facial recognition software.[[66]](#footnote-66)

The details surrounding how this technology will be used is closely guarded, but venues claim that the technology is needed for security and operational purposes in order to determine who is allowed into the building.[[67]](#footnote-67) For example some of artists, like Taylor Swift, use this technology at concerts to track stalkers.[[68]](#footnote-68) Venues also use this technology to identify employees and vendors.[[69]](#footnote-69) Barclay’s Center, in Brooklyn, has teamed up with IDEMIA, which manages the Transportation Security Administration’s PreCheck program, to offer expedited entry lines.[[70]](#footnote-70) Similarly, Live Nation claims that they intend to use the technology to improve the customer experience by linking tickets to faces and offering tailored services.[[71]](#footnote-71)

It is unclear how the data collected through facial recognition technology is managed and stored by entertainment venues. Facial recognition technology can often determine the age range and likely gender of concertgoers.[[72]](#footnote-72) Technology experts warn that this data could be collected and sold to third parties for marketing purposes without the consent of consumers.[[73]](#footnote-73) Several artists and activists have begun to speak out on the use of the technology. Fight For the Future, a nonprofit digital rights group, is campaigning to ban facial recognition software as a law enforcement tool, and recently launched a campaign against the use of the technology at concerts and festivals.[[74]](#footnote-74) Tom Morello, of Rage Against the Machine, Amanda Palmer, Downtown Boys, Anti-Flag, and others have spoken up in support of the campaign.[[75]](#footnote-75) Some musicians have expressed concerns that the technology will be used to target undocumented immigrants.[[76]](#footnote-76) In response, several music festivals, including the Governor’s Ball, in New York City), Bonnaroo in Tennessee, Punk Rock Bowling, in Las Vegas, Electric Forest in Michigan, and Austin City Limits announced that they would not be using the technology.[[77]](#footnote-77)

1. **Casinos**

Notably, casinos began using facial recognition technology years ago.[[78]](#footnote-78)  The technology was introduced as far back as 1994 at the Bally's Las Vegas Hotel and Casino in Las Vegas, Nevada, but the technology at that time was not advanced enough to follow a person or to identify faces unless the person looked straight at the camera.[[79]](#footnote-79) By the early 2000s, facial recognition had become a staple at casinos and today the technology has advanced enough that some casino owners boast they can identify someone through facial recognition with 55% accuracy, despite the person's face being obscured with “a hat, scarf, and glasses,” and sixty-nine percent accuracy “when just glasses were removed.”[[80]](#footnote-80)

1. **Housing**

Landlords in New York City have increasingly been doing away with mechanical keys and replacing traditional locks with so called “smart locks.” Smart locks are most commonly opened with key fobs or with key cards. Smart locks accessible by either key fobs[[81]](#footnote-81) and key cards,[[82]](#footnote-82) which generally use radio-frequency identification (“RFID”) technology, can be found all over the City,[[83]](#footnote-83) including in some New York City Housing Authority properties.[[84]](#footnote-84) More recently, landlords have started installing more sophisticated smart locks, such as those operable through facial recognition software,[[85]](#footnote-85) and mobile applications.[[86]](#footnote-86) The number of smart locks used in residential housing throughout the City, whether accessible with RFID based key fobs and key cards, mobile applications, or facial recognition, is currently unknown. According to a recent article in the *New York Times*, smart locks using Latch–a mobile application–are installed in 1,000 apartment buildings.[[87]](#footnote-87) GateGuard, which bills itself as the “Face Recognition Intercom & AI Doorman” is in over 700 buildings.[[88]](#footnote-88) GateGuard gives tenants the option of entering a building “by punching in a pin, waving a fob or card, using a phone app or relying on facial recognition technology.”[[89]](#footnote-89) Generally, the use of such technology only becomes known when it is the subject of an article,[[90]](#footnote-90) a lawsuit,[[91]](#footnote-91) a Housing & Community Renewal (“HCR”) objection is filed,[[92]](#footnote-92) or it is included in a building’s marketing materials.[[93]](#footnote-93)

There are certain benefits to smart locks. Smart locks allow landlords to easily forbid access to former employees and residents without having to change the locks.[[94]](#footnote-94) Key fobs and key cards can be easily replaced.[[95]](#footnote-95) Mobile phone applications and facial recognition systems do not need to be replaced. Smart locks can be used to provide limited access to the building for deliveries or repairs.[[96]](#footnote-96)

Still, smart locks can pose a number of safety and logistical concerns. For example, key fobs will not work during a blackout and backup power systems can be prohibitively expensive,[[97]](#footnote-97) and may die before power can be restored.[[98]](#footnote-98) Many observant Jews are forbidden from using any smart locks that “trigger” an electronic circuit on certain holidays and on Shabbat,[[99]](#footnote-99) thus leaving them without a means to access their own homes for sometimes days at a time. As discussed above, facial recognition software has both gender and skin-type bias,[[100]](#footnote-100) with error rates as high as 34% for darker-skinned women.[[101]](#footnote-101) This can lead to individuals being accidentally locked out of their apartments. In addition, mobile application based smart locks can sometimes unintentionally or wrongly be used to discriminate against the elderly and others who do not have access to a mobile phone.

In 517-525 West 45th Street, a number of rent-regulated tenants filed suit after their landlord required the use of Latch to access the building’s lobby, which is where the building’s elevator and tenant mailboxes are located.[[102]](#footnote-102) As a result of this change, one 93 year old resident, who had lost site in one eye and was not adept to technology, was unable to leave his apartment.[[103]](#footnote-103)

Nelson Management Group, the owner of Atlantic Plaza Towers, a rent-stabilized apartment building in East New York, sought permission from HCR to install facial recognition software.[[104]](#footnote-104) Residents of the property, which skews female and African American,[[105]](#footnote-105) were concerned that this technology could be used to track tenants.[[106]](#footnote-106) In Atlantic Plaza Towers, this software was part of a greater infringement of privacy by Nelson Management Group. Previously, mail keys were replaced and withheld until a tenant would agree to being photographed.[[107]](#footnote-107) Tenants who organized in the building’s lobby to educate other tenants about the installation of facial recognition software, and were photographed and received letters from Nelson Management Group warning them about congregating in the lobby.[[108]](#footnote-108)

Smart locks can also be used by landlords to harass tenants. The landlord of one Upper West Side building replaced mechanical keys with key fobs. A letter from the management company notifying tenants of this change limited to distribution of key fobs to individuals on the lease.[[109]](#footnote-109) This limited access for home health aides and child caregivers who, while not on the lease, required access. In addition, one 50 year tenant of the property, whose name was listed on the lease but whose wife’s was not, was required to submit a copy of his marriage license before the landlord would consider providing him with an additional key fob.[[110]](#footnote-110)

Although some tenants might appreciate the ability to enter their apartments using a mobile application, a key fob, or their face, tenants are not given a choice as to whether they would like to use such technology. In most cases landlords will request that tenants return their keys once the smart lock is installed,[[111]](#footnote-111) and no not provide tenants with the ability to opt out.[[112]](#footnote-112)

In addition, smart locks pose privacy concerns. Many devices used to access smart locks contain unique identifiers that allow the landlord to monitor who is entering a building and when. RFID based smart locks–such as key fobs and key cards–can record every time the individual using that key fob or key card has entered the building. Similarly, facial recognition technology uses unique identifiers–namely an individual’s face–to record entry. Mobile phone applications further allow landlords to record who enters a building and the time of entrance. When Latch was first installed in 517-525 West 45th Street, the accompanying contract stated “that any information collected through the Latch system goes to the building owner.”[[113]](#footnote-113) At that time the mobile application also included a “GPS function that allow[ed] the building’s owners to monitor their movements and even their social media.” Although the current privacy policy limits some of the information that can be shared with the building owner,[[114]](#footnote-114) the privacy policy can be changed in the future to once again give the landlord access to additional information.

Tenant tracking is particularly troubling for rent-regulated tenants. Although tenants in rent-regulated apartments are entitled to renewal leases,[[115]](#footnote-115) if the apartment is not the tenant’s primary residence, then this can be grounds for eviction or non-renewal of the tenant’s lease.[[116]](#footnote-116) Generally, primary residence requires that the tenant live in the apartment for more than six months of the year.[[117]](#footnote-117) Landlords can use data collected from keyless entry technology to track whether a tenant spends six months of the year in an apartment in order to use this as grounds for eviction–even if a tenant may otherwise meet the primary residence standard or have other mitigating circumstances.[[118]](#footnote-118) Similarly, a landlord can use evidence collected from smart locks systems to intimidate a tenant into vacating a rent-stabilized apartment with threats of eviction.

While smart locks can provide convenience and safety to tenants, in their unchecked and unregulated state they can be used to harass and track tenants. In addition, due to technological issues with facial recognition technology, lawful tenants can be denied access to their homes.

1. **Legislative Analysis**

**Int. 1170, a Local Law to amend the administrative code of the city of New York, in relation to requiring businesses to notify customers of the use of biometric identifier technology**

This bill would require businesses to notify customers if they are collecting biometric identifier information, such as scans of their faces, irises, or fingerprints, and if so, the length of time the information is retained, any relevant privacy policy, and whether the information is shared with third-parties.

This local law takes effect 180 days after it becomes law; provided, however, that the Commissioner of Consumer Affairs may promulgate rules necessary for the implementation of this local law prior to such effective date.

**Int. 1672, a Local Law to amend the administrative code of the city of New York, in relation to requiring real property owners to submit registration statements regarding biometric recognition technology utilized on the premises**

This bill would require real property owners to submit registration statements regarding biometric recognition technology utilized on the premises. The bill would also require the Department of Information Technology to establish a database and provide an annual report to the Mayor and the City Council.

This local law takes effect 90 days after it becomes law, except that the Department of Information Technology and Telecommunications shall take such measures as are necessary for the implementation of this local law, including the promulgation of rules, before such date.

**Preconsidered Int. No. \_\_\_, a Local Law to amend the administrative code of the city of New York and the New York city building code, in relation to defining the term key and requiring building owners to provide keys to residential tenants**

New York City’s Housing Maintenance Code requires owners of dwellings to “provide a key lock in the entrance door to each dwelling unit and at least one key.”[[119]](#footnote-119) The term “key” is not defined as a mechanical, metal key. Similarly, the New York City Building Code requires outside “cylinders of main entrance door locks shall be operated by the tenants' key, which shall not be keyed to also open the tenants' apartment door.”[[120]](#footnote-120) In the Building Code, “key” is not defined as a mechanical, metal key.

This bill would require that building owners provide mechanical keys to residents for both the exterior door of their buildings and the doors to their individual apartments. This bill would also prevent landlords from requiring that tenants use keyless entry technology to enter either their apartment buildings or their individual units.

This local law takes effect 120 days after it becomes law, except that the commissioner of buildings and the commissioner of housing preservation and development may take such measures as are necessary for the implementation of this local law, including the promulgation of rules, before such date.

**IV. CONCLUSION**

The Committees look forward to hearing testimony from the Department of Buildings, the Department of Consumer and Worker Protection, chambers of commerce, advocacy groups, community-based non-profit organizations, and other interested members of the public.

Int. No. 1170

By Council Members Torres, Espinal, Rosenthal, Rivera, Moya, Rose, Cornegy, and Lancman

..Title

A Local Law to amend the administrative code of the city of New York, in relation to requiring businesses to notify customers of the use of biometric identifier technology

..Body

Be it enacted by the Council as follows:

Section 1. Chapter 5 of title 20 of the administrative code of the city of New York is amended by adding a new subchapter 20 to read as follows:

SUBCHAPTER 20

BIOMETRIC IDENTIFIER INFORMATION

§ 20-828 Definitions.

§ 20-829 Disclosure of collection of biometric identifier information.

§ 20-830 Enforcement.

§ 20-831 Private right of action.

§ 20-832 Exceptions.

§ 20-833 Outreach and education.

§ 20-828 Definitions. As used in this subchapter, the following terms have the following meanings:

Biometric identifier information. The term “biometric identifier information” means a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, any of which is collected, retained, converted, stored or shared to identify an individual.

Commercial establishment. The term “commercial establishment” means any premises used for the purpose of carrying on or exercising any trade, business, profession, vocation, or commercial or charitable activity, including but not limited to hospitals, places of entertainment, and food or restaurant establishments.

Customer. The term “customer” means a purchaser or lessee, or a prospective purchaser or lessee, of goods or services from a commercial establishment.

Place of entertainment. The term “place of entertainment” means any privately or publicly owned and operated entertainment facility, such as a theater, stadium, arena, racetrack, museum, amusement park, observatory, or other place where attractions, performances, concerts, exhibits, athletic games, or contests are held.

§ 20-829 Disclosure of collection of biometric identifier information. Any commercial establishment that collects, retains, converts, stores or shares biometric identifier information of customers must disclose such collection, retention, conversion, storage or sharing in the following manner:

a. By placing a clear and conspicuous sign near all of the commercial establishment’s entrances notifying in plain, simple language, in a form and manner prescribed by the commissioner by rule, that biometric identifier information is being collected, retained, converted, stored or shared; and

b. By making available online:

1. The amount of time for which the commercial establishment retains or stores biometric identifier information;

2. The kind of biometric identifier information the commercial establishment collects, retains, converts, stores or shares from its customers;

3. Any privacy policy governing, and any purpose for, the commercial establishment’s collection, retention, conversion, storage or sharing of biometric identifier information of customers, including but not limited to, any protective measures the commercial establishment utilizes to safeguard biometric identifier information; and

4. Whether the commercial establishment shares biometric identifier information with third-parties.

§ 20-830 Enforcement. Whenever the commissioner has reason to believe that a commercial establishment has violated any provision of this subchapter or any rule or regulation promulgated thereunder, the commissioner may, upon proof of violation, direct payment of a civil penalty in the amount of $500 for each day that the commercial establishment is in violation of this subchapter or the rules promulgated thereunder.

§ 20-831 Private right of action. a. Any person who biometric identifier information was collected, retained, converted, stored or shared in violation of this subchapter may commence an action in a court of competent jurisdiction on his or her own behalf against a commercial establishment that is alleged to have violated this subchapter. A prevailing party may recover for each violation:

1. Against a private entity that negligently violates a provision of this subchapter, damages of $1,000;

2. Against a private entity that intentionally or recklessly violates a provision of this subchapter, damages of $5,000;

3. Reasonable attorneys’ fees and costs, including expert witness fees and other litigation expenses; and

4. Other relief, including an injunction, as the court of competent jurisdiction may deem appropriate.

b. In any action brought pursuant to this section, the commissioner may intervene as a matter of right.

§ 20-832 Exceptions. Nothing in this subchapter shall apply to the collection, capturing, conversion, storage, sharing or use of biometric identifier information by government agencies, employees or agents.

§ 20-833 Outreach and education. The commissioner shall conduct outreach and education efforts to inform commercial establishments likely to be affected by this subchapter about its requirements.

§ 2. This local law takes effect 180 days after it becomes law; provided, however, that the commissioner of consumer affairs may promulgate rules necessary for the implementation of this local law prior to such effective date.

SIL

LS #5625

07/24/2018

\*This page intentionally left blank\*

Int. No. 1672

By Council Members Richards and Kallos

..Title

A Local Law to amend the administrative code of the city of New York, in relation to requiring real property owners to submit registration statements regarding biometric recognition technology utilized on the premises

..Body

Be it enacted by the Council as follows:

Section 1. Title 10 of the administrative code of the city of New York is amended by adding a new chapter 12 to read as follows:

CHAPTER 12

TECHNOLOGY

§ 10-1201 Biometric recognition technology. a. Definitions. For the purposes of this section, the following terms have the following meanings:

Biometric data. The term “biometric data” means a physiological, biological, or behavioral characteristic, including but not limited to an iris scan, fingerprint, a hand scan, voiceprint, and thermal or facial characteristics that can be used alone or in combination with each other, or with other information, to establish individual identity.

Biometric recognition technology. The term “biometric recognition technology” means either or both of the following : (i) a process or system that captures biometric data of an individual or individuals; (ii) a process or system that can assist in verifying or identifying an individual or individuals based on biometric data.

Building manager. The term “building manager” means the person designated by the owner of a real property to manage the property on behalf of the owner.

Department. The term department means the department of information technology and telecommunications.

b. Real property owner’s obligation to register. By December 1, 2020, and annually thereafter, every real property owner or building manager that implements biometric recognition technology in a commercial or residential property shall submit, to the department, a registration statement. Such registration statement shall include the following information:

(a) the street address of the property, including borough, block and lot number;

(b) whether the property is commercial or residential;

(c) date when each biometric recognition technology was first utilized;

(d) number of units in the building;

(e) number of tenants in the building;

(f) type of each biometric recognition technology used;

(g) the name of the vendor providing each biometric recognition technology;

(h) the purpose for each use of the technology;

(i) list of all public locations where imaging is performed; and

(j) data retention policy for each biometric recognition technology.

c. Penalty. Any real property owner who fails to register pursuant to subdivision b of this section is liable for a civil penalty of not more than $500 per property unit for the first violation, and not more than $1,000 for each subsequent violation. Such penalties shall be imposed by the department provided that after a notice of failure to register has been issued to a property owner, such owner may cure any resulting first violation by registering within 2 months of the receipt of such notice. Failure to register 2 months after the first violation shall be considered a subsequent violation.

d. Database. The department of information technology and telecommunications shall establish and maintain a publicly searchable database of properties that utilize biometric recognition technology. Updates to such database shall be made no less than 30 days following the annual registration deadline pursuant to subdivision b. Such database shall be made available on the website of the department, shall have the ability to produce reports by query, and shall include, but need not be limited to, the following information for each property:

(1) the location of the property, including the physical address, borough, block and lot number;

(2) the date when each biometric recognition technology was first utilized; and

(3) the type of each biometric recognition technology.

f. Report. No later than one year after the effective date of the local law adding this section, and annually thereafter, the commissioner shall submit to the mayor, the speaker of the council, a report of the following information, based upon registrations filed during the previous year:

(a) the street address of the property, including borough, block and lot number;

(b) whether the property is commercial or residential;

(c) the date when each biometric recognition technology was first utilized;

(d) number of units in the building;

(e) number of tenants in the building;

(f) the type of each biometric recognition technology used;

(g) the name of the vendor providing each biometric recognition technology.

§ 2. This local law takes effect 90 days after it becomes law, except that the department of information technology and telecommunications shall take such measures as are necessary for the implementation of this local law, including the promulgation of rules, before such date.

IB

LS 10489

06/18/19 11:54 am

Preconsidered Int. No.

By Council Member Lander

..Title

A Local Law to amend the administrative code of the city of New York and the New York city building code, in relation to defining the term key and requiring building owners to provide keys to residential tenants

..Body

Be it enacted by the Council as follows:

Section 1. Subdivision a of section 27-2004 of the administrative code of the city of New York is amended by adding a new paragraph 49 to read as follows:

49. The term “key” shall mean a piece of shaped metal with incisions cut to fit the wards of a particular lock, which is inserted into such lock and turned to open or close such lock.

§ 2. Section 27-2043 of the administrative code of the city of New York is amended to read as follows:

§ 27-2043 Door locks [Locks in dwelling unit doors]. a. The owner of a dwelling shall provide a key lock in the entrance door to each dwelling unit and at least one key[.] for each entrance door key lock to each person lawfully entitled to occupancy of such dwelling unit. Such entrance door key lock must be operable at all hours without the use of technology including, but not limited to, a mobile phone application, a keypad, facial recognition technology, biometric scanning, a radio-frequency identification card or other such similar technology. Such owner shall not require such person to utilize such technology if such technology is present in such dwelling. In a class A multiple dwelling such door shall be equipped with a heavy duty latch set and a heavy duty dead bolt operable by a key from the outside and a thumb-turn from the inside. Such owner shall provide each such person with at least one key for each heavy duty dead bolt set for such dwelling unit.

b. Each dwelling unit entrance door in a class A multiple dwelling shall also be equipped with a chain door guard so as to permit partial opening of the door.

c. The owner of a dwelling shall provide key locks in the building entrance doors and other exterior exit doors to such building and shall provide at least one key for each entrance door key lock to each person lawfully entitled to occupancy of a dwelling in such building. Such entrance door key locks must be operable at all hours without the use of technology including, but not limited to, a mobile phone application, a keypad, facial recognition technology, biometric scanning, a radio-frequency identification card or other such similar technology. Such owner shall not require such person to utilize such technology if such technology is present in such building.

§ 3. Section 1002.1 of the New York city building code, as amended by local law 141 for the year 2013, is amended by adding a new definition of “KEY” in alphabetical order to read as follows:

**KEY**. A piece of shaped metal with incisions cut to fit the wards of a particular lock, which is inserted into such lock and turned to open or close such lock.

§ 4. This local law takes effect 120 days after it becomes law, except that the commissioner of buildings and the commissioner of housing preservation and development may take such measures as are necessary for the implementation of this local law, including the promulgation of rules, before such date.

GZ

LS #10391

9.23.19 11:53am

1. Center for Global Development, *Biometrics FAQs*, CGD, 2019, <https://www.cgdev.org/page/biometrics-faqs> [↑](#footnote-ref-1)
2. Li, Cha and Tappert, *Biometric Distinctiveness of Brain Signals Based on EEG*, 2018 IEEE 9th International Conference on Biometrics Theory, Applications and Systems (BTAS), Redondo Beach, CA, USA, pp. 1-6 (2018); R. Palaniappan, and S. M. Krishnan, *Identifying individuals using ECG signals*, Proceedings of International Conference on Signal Processing and Communications, Bangalore, India, pp. 569–572, 11–14 (2004); Mulyono, David & Horng, Shi-Jinn. A study of finger vein biometric for personal identification (2008). [↑](#footnote-ref-2)
3. Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. Marshall L. Rev. 589, 589–92 (2018) (citing Margaret Rouse, Biometrics, [www.searchsecurity.techtarget.com/definition/biometrics](http://www.searchsecurity.techtarget.com/definition/biometrics); *see* generally What is Biometrics?, IDEMIA, [www.morpho.com/en/biometrics](http://www.morpho.com/en/biometrics) (referring to biometrics as all processes used to recognize, authenticate, and identify persons based on certain physical or behavioral characteristics. The characteristics are universal, unique, invariable, recordable, and measurable)). [↑](#footnote-ref-3)
4. Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. Marshall L. Rev. 589, 589–92 (2018) (citing Margaret Rouse, Biometrics, [www.searchsecurity.techtarget.com/definition/biometrics](http://www.searchsecurity.techtarget.com/definition/biometrics); *see* generally What is Biometrics?, IDEMIA, [www.morpho.com/en/biometrics](http://www.morpho.com/en/biometrics) (referring to biometrics as all processes used to recognize, authenticate, and identify persons based on certain physical or behavioral characteristics. The characteristics are universal, unique, invariable, recordable, and measurable)). [↑](#footnote-ref-4)
5. Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. Marshall L. Rev. 589, 589–92 (2018) (citing Margaret Rouse, Biometrics, [www.searchsecurity.techtarget.com/definition/biometrics](http://www.searchsecurity.techtarget.com/definition/biometrics); *see* generally What is Biometrics?, IDEMIA, [www.morpho.com/en/biometrics](http://www.morpho.com/en/biometrics) (referring to biometrics as all processes used to recognize, authenticate, and identify persons based on certain physical or behavioral characteristics. The characteristics are universal, unique, invariable, recordable, and measurable)). [↑](#footnote-ref-5)
6. Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. Marshall L. Rev. 589, 589–92 (2018). [↑](#footnote-ref-6)
7. Tarun Agarwal, *Biometric Sensors—Types and Its Workings*, ELPROCUS, [www.elprocus.com/different-types-biometric-sensors/](http://www.elprocus.com/different-types-biometric-sensors/). [↑](#footnote-ref-7)
8. Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. Marshall L. Rev. 589, 589–92 (2018). [↑](#footnote-ref-8)
9. Kanya A. Bennett, *Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveilance Systems*, 3 N.C. J.L. & Tech. 151 (2001) (citing Kevin Bonsor, *How Facial Recognition Works*, at <http://www.howstuffworks.com/facial-recognition.htm>). [↑](#footnote-ref-9)
10. Kanya A. Bennett, *Can Facial Recognition Technology Be Used to Fight the New Way against Terrorism: Examining the Constitutionality of Facial Recognition Surveilance Systems*, 3 N.C. J.L. & Tech. 151 (2001) (citing Kevin Bonsor, How Facial Recognition Works, at <http://www.howstuffworks.com/facial-recognition.htm>). [↑](#footnote-ref-10)
11. Kanya A. Bennett, *Comment: Can Facial Recognition Technology Be Used to Fight the New War Against Terrorism?: Examining the Constitutionality of Facial Recognition Surveillance Systems*, 3 N.C. J. L. & Tech. 151, 155–56 (2001). [↑](#footnote-ref-11)
12. Yana Welinder & Aeryn Palmer, *Face Recognition, Real-Time Identification, and Beyond, in* Cambridge Handbook of Consumer Privacy, 3-4 (2018); Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 685 (2019). [↑](#footnote-ref-12)
13. Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 621 (2019) (citing FED. TRADE COMM'N, FACING FACTS: BEST PRACTICES FOR COMMON USES OF FACIAL RECOGNITION TECHNOLOGIES 4-5 (2012)). [↑](#footnote-ref-13)
14. Mike Orcutt, *As It Searches for Suspects, the FBI May Be Looking at You*, MIT Tech. Rev. (June 23, 2016), <https://www.technologyreview.com/s/601738/as-it-searches-for-suspects-the-fbi-may-be-looking-at-you/>; Claudia Cuador, *From Street Photography to Face Recognition: Distinguishing Between the Right to Be Seen and the Right to Be Recognized*, 41 Nova L. Rev. 237, 264 (2017). [↑](#footnote-ref-14)
15. Kristine Hamann & Rachel Smith, *Facial Recognition Technology Where Will It Take Us?*, Crim. Just., Spring 2019, at 9, 10. [↑](#footnote-ref-15)
16. Kristine Hamann & Rachel Smith, *Facial Recognition Technology Where Will It Take Us?*, Crim. Just., Spring 2019, at 9, 10. [↑](#footnote-ref-16)
17. Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. Marshall L. Rev. 589, 589–92 (2018). [↑](#footnote-ref-17)
18. Mariko Hirose, *Privacy in Public Spaces: The Reasonable Expectation of Privacy Against the Dragnet Use of Facial Recognition Technology*, 49 Conn. L. Rev. 1591, 1596–98 (2017). [↑](#footnote-ref-18)
19. # James Regan, *New Zealand Passport Robot Tells Applicant of Asian Descent to Open Eyes*, Reuters, December 7, 2016, <https://www.reuters.com/article/us-newzealand-passport-error/new-zealand-passport-robot-tells-applicant-of-asian-descent-to-open-eyes-idUSKBN13W0RL>.

    [↑](#footnote-ref-19)
20. # James Regan, *New Zealand Passport Robot Tells Applicant of Asian Descent to Open Eyes*, Reuters, December 7, 2016, <https://www.reuters.com/article/us-newzealand-passport-error/new-zealand-passport-robot-tells-applicant-of-asian-descent-to-open-eyes-idUSKBN13W0RL>.

    [↑](#footnote-ref-20)
21. Michele Merler, Nalini Ratha, Rogerio Feris, John R. Smith, *IBM Research AI*, IBM T. J. Watson Research Center, April 10, 2019, <https://arxiv.org/pdf/1901.10436.pdf?>. [↑](#footnote-ref-21)
22. Michele Merler, Nalini Ratha, Rogerio Feris, John R. Smith, *IBM Research AI*, IBM T. J. Watson Research Center, April 10, 2019, <https://arxiv.org/pdf/1901.10436.pdf?>. [↑](#footnote-ref-22)
23. Michele Merler, Nalini Ratha, Rogerio Feris, John R. Smith, *IBM Research AI*, IBM T. J. Watson Research Center, April 10, 2019, <https://arxiv.org/pdf/1901.10436.pdf?>. [↑](#footnote-ref-23)
24. Richard Raysman & Peter Brown, *How Has Facial Recognition Impacted the Law?*, N.Y.L.J. (Feb. 9, 2016). [↑](#footnote-ref-24)
25. Kristine Hamann & Rachel Smith, *Facial Recognition Technology Where Will It Take Us?*, Crim. Just., Spring 2019, at 9, 10 (citing Richard Raysman & Peter Brown, *How Has Facial Recognition Impacted the Law?*, N.Y.L.J. (Feb. 9, 2016)). [↑](#footnote-ref-25)
26. Sharon Nakar, Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. Sci. & Tech. L. 88, 109 (2017). [↑](#footnote-ref-26)
27. See, e.g., Arielle Pardes, Facial Recognition Tech Is Ready for Its Post-Phone Future, WIRED (Sept. 10, 2018, 7:00 AM), <https://www.wired.com/story/future-of-facial-recognition-technology/>. [↑](#footnote-ref-27)
28. See, e.g., Anish Malhotra, The World's Largest Biometric ID System Keeps Getting Hacked: The Personal Data of Many Indians Is For Sale on WhatsApp For Less Than $10, VICE: MOTHERBOARD (Jan. 8, 2018, 10:07 AM), <https://motherboard.vice.com/en_us/article/43q4jp/aadhaar-hack-insecure-biometric-id-system>; see also US Government Hack Stole Fingerprints of 5.6 Million Federal Employees, THE GUARDIAN (Sept. 23, 2015, 5:44 PM), https://www.theguardian.com/technology/2015/sep/23/us-government-hack-stole-fingerprints. [↑](#footnote-ref-28)
29. [1] Breach name: BioStar 2, a Suprema-based security platform.

    Date discovered: August 5, 2019. Date announced: August 14, 2019.Number of records: 28 million records of over 1 million people worldwide. Information exposed: Fingerprint data, facial recognition data, face photos of users, unencrypted usernames and passwords, logs of facility access, security levels and clearance, personal details of staff. Biometric data breach: *Database Exposes Fingerprints, Facial Recognition Data of 1 Million People*, Norton, <https://us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html>. [↑](#footnote-ref-29)
30. # Josh Taylor, *Major Breach Found in Biometrics System Used by Banks*, *UK Police and Defence Firms*, The Guardian, August 14, 2019, <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms>.

    [↑](#footnote-ref-30)
31. # Zak Doffman, *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report*, FORBES, August 14, 2019, <https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#7309aded46c6>; Report: Data Breach in Biometric Security Platform Affecting Millions of Users, August 14, 2019, <https://www.vpnmentor.com/blog/report-biostar2-leak/>.

    [↑](#footnote-ref-31)
32. # Josh Taylor, *Major Breach Found in Biometrics System Used By Banks*, *UK Police and Defence Firms*, The Guardian, August 14, 2019, <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms>.

    [↑](#footnote-ref-32)
33. Breach name: BioStar 2, a Suprema-based security platform.

    Date discovered: August 5, 2019. Date announced: August 14, 2019.Number of records: 28 million records of over 1 million people worldwide. Information exposed: Fingerprint data, facial recognition data, face photos of users, unencrypted usernames and passwords, logs of facility access, security levels and clearance, personal details of staff. Biometric data breach: *Database Exposes Fingerprints, Facial Recognition Data of 1 Million People*, Norton, <https://us.norton.com/internetsecurity-emerging-threats-biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data.html>. [↑](#footnote-ref-33)
34. # Josh Taylor, *Major Breach Found in Biometrics System Used By Banks*, *UK Police and Defence Firms*, The Guardian, August 14, 2019, <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms>.

    [↑](#footnote-ref-34)
35. # Zak Doffman, *New Data Breach Has Exposed Millions of Fingerprint and Facial Recognition Records: Report*, FORBES, August 14, 2019, <https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/#7309aded46c6>; Report: Data Breach in Biometric Security Platform Affecting Millions of Users, August 14, 2019, <https://www.vpnmentor.com/blog/report-biostar2-leak/>.

    [↑](#footnote-ref-35)
36. # Josh Taylor, *Major Breach Found in Biometrics System Used By Banks*, *UK Police and Defence Firms*, The Guardian, August 14, 2019, <https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms>.

    [↑](#footnote-ref-36)
37. Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 628–30 (2019) (citing Daniel J. Solove & Danielle Keats Citron, Risk and Anxiety: A Theory of Data-Breach Harms, 96 TEX. L. REV. 737, 759 (2018)). [↑](#footnote-ref-37)
38. Sharon Nakar, Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. Sci. & Tech. L. 88, 96 (2017) (citing Sen. Franken Raises Concerns about Facial Recognition App that Lets Strangers Secretly Identify People, AL FRANKEN | SENATOR FOR MINNESOTA (Feb. 5, 2014), http://www.franken.senate.gov/?p=press\_release&id=2699). [↑](#footnote-ref-38)
39. Carole Cadwalladr, *Revealed: 50 Million Facebook Profiles Harvested For Cambridge Analytica In Major Data Breach*, The Guardian, March 17, 2018, <https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election>. [↑](#footnote-ref-39)
40. Olivia Solon and Cyrus Farivar, *Millions of People Uploaded Photos To The Ever App. Then The Company Used Them To Develop Facial Recognition Tools*, NBC News, May 9, 2019, <https://www.nbcnews.com/tech/security/millions-people-uploaded-photos-ever-app-then-company-used-them-n1003371>. [↑](#footnote-ref-40)
41. Catie Edmondson, *ICE Used Facial Recognition To Mine State Driver’s License Databases*, New York Times, July 7, 2019, <https://www.nytimes.com/2019/07/07/us/politics/ice-drivers-licenses-facial-recognition.html?searchResultPosition=12>. [↑](#footnote-ref-41)
42. Louise Matsakis, *The Ringification of suburban life*, Wired, September 26, 2019, <https://www.wired.com/story/ring-surveillance-suburbs/>. [↑](#footnote-ref-42)
43. Louise Matsakis, *Cops Are Offering Ring Doorbell Cameras in Exchange For Info*, Wired, September 2, 2019, <https://www.wired.com/story/cops-offering-ring-doorbell-cameras-for-information/>. [↑](#footnote-ref-43)
44. Sahil Chinoy, *We built an ‘unbelievable’ (but legal) facial recognition machine*, New York Times, April 16, 2019, <https://www.nytimes.com/interactive/2019/04/16/opinion/facial-recognition-new-york-city.html>. [↑](#footnote-ref-44)
45. Paul Mozur, *In Hong Kong Protests, Faces Become Weapons*, New York Times, July 26, 2019, <https://www.nytimes.com/2019/07/26/technology/hong-kong-protests-facial-recognition-surveillance.html?searchResultPosition=16>. [↑](#footnote-ref-45)
46. Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 621–22 (2019) (citing *See, e.g., Amazon Rekognition*, AWS, https://aws.amazon.com/rekognition/ [https://perma.cc/5792-B4G2]; *see also* Justin Lee, *Credence Research Report Forecasts Biometrics Market to Reach $34.5B by 2022*, Biometric Update (May 8, 2016), <http://www.biometricupdate.com/201605/credence-research-report-forecasts-biometrics-market-to-reach-34-5b-by-2022>. [↑](#footnote-ref-46)
47. *See* Angelica Carrero, *Biometrics and Federal Databases: Could You Be in It?*, 51 J. Marshall L. Rev. 589, 589–92 (2018). [↑](#footnote-ref-47)
48. A recent study found that facial recognition is likely to generate revenue of $9.78 billion by 2023, growing at a compounded annual growth rate of 16.81% between 2017 and 2023; *Global Facial Recognition Market Report 2018*, Cision: PR Newswire (June 5, 2018), <https://www.prnewswire.com/news-releases/global-facial-recognition-market-report-2018-300660163.htm>; Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 685 (2019). [↑](#footnote-ref-48)
49. Nick Coult, *Facial Recognition Software: Coming Soon to Your Local Retailer?*, Crime Rep. (Apr. 23, 2018), <https://thecrimereport.org/2018/04/23/facial-recognition-software-coming-soon-to-your-local-retailer>; Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 685 (2019). [↑](#footnote-ref-49)
50. *See* Chris Burt, *FaceFirst Facial Recognition Coming to Thousands of U.S. Retail Locations*, Biometric Update, Aug. 21, 2018, <https://www.biometricupdate.com/201808/facefirst-facial-recognition-coming-to-thousands-of-u-s-retail-locations>; Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019). [↑](#footnote-ref-50)
51. *See* David Lumb, *Is Facial Recognition The Next Privacy Battleground?*, Fast Co. , Jan. 26, 2015, <http://www.fastcompany.com/3040375/is-facial-recognitionthenext-privacy-battleground>;Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019). [↑](#footnote-ref-51)
52. Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 543–44 (2019). [↑](#footnote-ref-52)
53. Chris Frey, Revealed: How Facial Recognition Has Invaded Shops--and Your Privacy, GUARDIAN (Mar. 3, 2016), <https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto>; *see also* Sapna Maheshwari, *Stores See a Future Without “May I Help You?” (They'll Already Have Your Data),* N.Y. Times (Mar. 10, 2019), <https://www.nytimes.com/2019/03/10/business/retail-stores-technology.html> (discussing that through facial recognition “stores could send automatic text messages and receive theirs profiles to assist them better[,]” allowing stores to “immediately know customers' identities and personal preferences when they arrived”); Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 685 (2019). [↑](#footnote-ref-53)
54. # Jenna Reck, a Target spokesperson, Leticia Miranda, *Thousands of Stores Will Soon Use Facial Recognition*, *And They Won't Need Your Consent*, BuzzFeedNews, August 17, 2018, <https://www.buzzfeednews.com/article/leticiamiranda/retail-companies-are-testing-out-facial-recognition-at>.

    [↑](#footnote-ref-54)
55. # *Are Stores You Shop at Secretly Using Face Recognition on You?*, March 28, 2019, ACLU, <https://www.aclu.org/blog/privacy-technology/surveillance-technologies/are-stores-you-shop-secretly-using-face>.

    [↑](#footnote-ref-55)
56. This approach is called omnichannel. [↑](#footnote-ref-56)
57. Chris Frey, Revealed: How Facial Recognition Has Invaded Shops--and Your Privacy, GUARDIAN (Mar. 3, 2016), <https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto>; *see also* Sapna Maheshwari, *Stores See a Future Without “May I Help You?” (They'll Already Have Your Data),* N.Y. Times (Mar. 10, 2019), <https://www.nytimes.com/2019/03/10/business/retail-stores-technology.html> (discussing that through facial recognition “stores could send automatic text messages and receive theirs profiles to assist them better[,]” allowing stores to “immediately know customers' identities and personal preferences when they arrived”); Elias Wright, *The Future of Facial Recognition Is Not Fully Known: Developing Privacy and Security Regulatory Mechanisms for Facial Recognition in the Retail Sector*, 29 Fordham Intell. Prop. Media & Ent. L.J. 611, 685 (2019). [↑](#footnote-ref-57)
58. Stephanie Pandolph, *Shoppers Expect More Personalization*, Bus. Insider, Oct. 26, 2017, <https://www.businessinsider.com/shoppers-expect-more-personalization-2017-10>; Victoria Greene, *7 Examples of Big Data Personalization*, Big Data, Oct. 11, 2018, <https://bigdata-madesimple.com/7-examples-of-big-data-retail-personalization/>; Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019). [↑](#footnote-ref-58)
59. Akiva A. Miller, *What Do We Worry About When We Worry About Price Discrimination? The Law and Ethics of Using Personal Information for Pricing*, 19 J. Tech. L. & Pol'y 43, 91 (2014); Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019). [↑](#footnote-ref-59)
60. Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019); Seth Schoen, *New Cookie Technologies: Harder to See and Remove, Widely Used to Track You*, Elec. Frontier Found, Sept. 14, 2009, <https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide>. [↑](#footnote-ref-60)
61. Seth Schoen, *New Cookie Technologies: Harder to See and Remove, Widely Used to Track You*, Elec. Frontier Found, Sept. 14, 2009, https://www.eff.org/deeplinks/2009/09/new-cookie-technologies-harder-see-and-remove-wide; Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 569 (2019). [↑](#footnote-ref-61)
62. Sharon Nakar, Dov Greenbaum, *Now You See Me. Now You Still Do: Facial Recognition Technology and the Growing Lack of Privacy*, 23 B.U. J. Sci. & Tech. L. 88, 99–100 (2017). [↑](#footnote-ref-62)
63. Vincent Nguyen, *Shopping for Privacy: How Technology in Brick-and-Mortar Retail Stores Poses Privacy Risks for Shoppers*, 29 Fordham Intell. Prop. Media & Ent. L.J. 535, 557–59 (2019). [↑](#footnote-ref-63)
64. Robert H. Thornburg, *Face Recognition Technology: The Potential Orwellian Implications and Constitutionality of Current Uses Under the Fourth Amendment*, 20 J. Marshall J. Computer & Info. L. 321 (Winter 2002). [↑](#footnote-ref-64)
65. Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, NYT (March 13, 2018), available at: <https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html> [↑](#footnote-ref-65)
66. Maggie Serota, *Ticketmaster Explores Replacing Tickets With Facial Recognition*, Spin Magazine (May 8, 2018), available at: <https://www.spin.com/2018/05/ticketmaster-facial-recognition-blink-live-nation/> [↑](#footnote-ref-66)
67. Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, NYT (March 13, 2018), available at: <https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html> [↑](#footnote-ref-67)
68. Steven Knopper, *Why Taylor Swift Is Using Facial Recognition at Concerts*, RollingStone, December 13, 2018, <https://www.rollingstone.com/music/music-news/taylor-swift-facial-recognition-concerts-768741/>. [↑](#footnote-ref-68)
69. Kevin Draper, *Madison Square Garden Has Used Face-Scanning Technology on Customers*, NYTimes, March 13, 2018, <https://www.nytimes.com/2018/03/13/sports/facial-recognition-madison-square-garden.html>. [↑](#footnote-ref-69)
70. *Id.* [↑](#footnote-ref-70)
71. Maggie Serota, *Ticketmaster Explores Replacing Tickets with Facial Recognition*, Spin Magazine, May 8, 2018, <https://www.spin.com/2018/05/ticketmaster-facial-recognition-blink-live-nation/>. [↑](#footnote-ref-71)
72. *Id*. [↑](#footnote-ref-72)
73. Wendy Mesley, *The Weekly Briefing*, CBC News, Interview with Takara Small, May 20, 2018, <https://www.youtube.com/watch?v=6lpHzPMcAI0>. [↑](#footnote-ref-73)
74. Amanda Gersten, *Musicians and Activists Speak Out Against Ticketmaster’s Investment in Facial Recognition Technology*, Paste Magazine, September 10, 2019, <https://www.pastemagazine.com/articles/2019/09/musicians-and-activists-speak-out-against-ticketma.html>. [↑](#footnote-ref-74)
75. *Id*. [↑](#footnote-ref-75)
76. Dan Reilly, *Musicians and Fans Unite to Keep Facial Recognition Tech Out of Concerts*, Fortune Magazine, September 30, 2019, <https://fortune.com/2019/09/30/ban-facial-recognition-live-events-music-festivals-concerts/>. [↑](#footnote-ref-76)
77. *Id*.; Ben Kaye, Bonnaroo, *Electric Forest, Austin City Limits Festivals Say They Won’t Use Facial Recognition Tech*, Consequence of Sound, September 30, 2019, <https://consequenceofsound.net/2019/09/bonnaroo-electric-forest-austin-city-limit-festivals-facial-recognition/>. [↑](#footnote-ref-77)
78. *See* Dan Koeppel, *Casino Hackers*, CNN, Oct. 23, 2006, <http://www.cnn.com/2006/TECH/07/13/popsci.gambling/>; Stacy Norris, *"... and the Eye in the Sky Is Watching Us All" - the Privacy Concerns of Emerging Technological Advances in Casino Player Tracking*, 9 UNLV GAMING L.J. 269, 291 (2019). [↑](#footnote-ref-78)
79. Stacy Norris, *"... and the Eye in the Sky Is Watching Us All" - the Privacy Concerns of Emerging Technological Advances in Casino Player Tracking*, 9 UNLV GAMING L.J. 269, 291 (2019) (citing Jamie Condliffe, *Facial recognition is getting incredibly powerful, and even more controversial*, Bus. Insider, Sept. 8, 2017, <http://www.businessinsider.com/facial-recognition-controversy-improvement-2017-9>). [↑](#footnote-ref-79)
80. Stacy Norris, *"... and the Eye in the Sky Is Watching Us All" - the Privacy Concerns of Emerging Technological Advances in Casino Player Tracking*, 9 UNLV GAMING L.J. 269, 291 (2019) (citing Jamie Condliffe, *Facial recognition is getting incredibly powerful, and even more controversial*, Bus. Insider, Sept. 8, 2017, <http://www.businessinsider.com/facial-recognition-controversy-improvement-2017-9>). [↑](#footnote-ref-80)
81. Marianne Schaefer, *Key Fobs: Security Fix or Money Pit?*, Habitat Magazine, Aug. 2016, <https://www.habitatmag.com/Publication-Content/Building-Operations/2016/2016-August/Key-Fobs> [↑](#footnote-ref-81)
82. Caleb LaPointe, *What Are RFID Key Cards and How Do They Work?*, Handytrac, Sep. 14, 2018 <https://www.handytrac.com/how-rfid-key-cards-work>. [↑](#footnote-ref-82)
83. Shaefer, *supra* note 107. [↑](#footnote-ref-83)
84. Press Release, *NYCHA Announces Completion Of Major CCTV*, Security Upgrades At 31 Developments Citywide, Jan. 19, 2016 <https://www1.nyc.gov/site/nycha/about/press/pr-2015/Nycha-Completes-Major-cctv-Security-Upgrades-31-Developments.page>. [↑](#footnote-ref-84)
85. Elizabeth Kim, *Brooklyn Landlord Wants To Install Facial Recognition Tech At Rent-Stabilized Complex*, Gothamist, Mar. 25, 2019 <https://gothamist.com/news/brooklyn-landlord-wants-to-install-facial-recognition-tech-at-rent-stabilized-complex>. [↑](#footnote-ref-85)
86. Corina Knoll, *When a Phone App Opens Your Apartment Door, but You Just Want a Key*, NY Times, Mar. 23, 2019, <https://www.nytimes.com/2019/03/23/nyregion/keyless-apartment-entry-nyc.html>. [↑](#footnote-ref-86)
87. *Id*. [↑](#footnote-ref-87)
88. Sarina Trangle, *Privacy Concerns Mount Over Tech-Based Apartment Building Access*, AMNY, Sep. 22, 2019 <https://www.amny.com/real-estate/apartment-access-privacy-concerns-1.29927187>. [↑](#footnote-ref-88)
89. *Id.* [↑](#footnote-ref-89)
90. Claudia Irizarry Aponte, *Williamsburg Loft Building’s Tenants See Hopes To Stay Fade*, The City, Sep. 16, 2019 <https://thecity.nyc/2019/09/williamsburg-loft-buildings-tenants-see-hopes-to-stay-fade.html>; *see also* Elizabeth Kim, *'We're Like Guinea Pigs': How An Affordable Lower East Side Complex Got Facial Recognition*, Gothamist, Sep. 18, 2019, <https://gothamist.com/news/were-guinea-pigs-how-affordable-lower-east-side-complex-got-facial-recognition>. [↑](#footnote-ref-90)
91. Knoll, *supra* note 112. [↑](#footnote-ref-91)
92. Kim, *supra* note 113. [↑](#footnote-ref-92)
93. HPD And HDC Join Omni NY, Bank Of America, And Partners To Celebrate The Completion Of A New 176-Unit Affordable Housing Development In The Bronx, Feb., 17, 2017, <https://www1.nyc.gov/site/hpd/about/press-releases/2017/02/02-17-17.page>. [↑](#footnote-ref-93)
94. A.J. Sidransky, *Keys, Key Fobs, and Door Codes Controlling Access to Your Building*, Cooperator, Apr. 2009 <https://cooperator.com/article/keys-key-fobs-and-door-codes/full> [↑](#footnote-ref-94)
95. *Id.* [↑](#footnote-ref-95)
96. *Id.* [↑](#footnote-ref-96)
97. Shaefer, *supra* note 107. [↑](#footnote-ref-97)
98. Sidransky, *supra* note 120. [↑](#footnote-ref-98)
99. Kathianne Boniello, *Orthodox Jewish tenants sue building over electronic key fobs*, NY Post, Aug. 1, 2015, <https://nypost.com/2015/08/01/orthodox-jewish-tenants-sue-building-over-electronic-key-fobs>. [↑](#footnote-ref-99)
100. Larry Hardesty, *Study Finds Gender And Skin-Type Bias In Commercial Artificial-Intelligence Systems*, MIT News Office, Feb. 11, 2018 <http://news.mit.edu/2018/study-finds-gender-skin-type-bias-artificial-intelligence-systems-0212>. [↑](#footnote-ref-100)
101. *Id.* [↑](#footnote-ref-101)
102. Isabel Vincent, *Hell’s Kitchen residents suing over keyless apartment entry*, NY Post, Mar. 16, 2019 <https://nypost.com/2019/03/16/hells-kitchen-residents-suing-over-keyless-apartment-entry>. [↑](#footnote-ref-102)
103. Alfred Ng, *Tenants worry smart-home tech could be abused by landlords*,CNET, Apr. 4, 2019 <https://www.cnet.com/news/tenants-worry-smart-home-tech-could-be-abused-by-landlords> [↑](#footnote-ref-103)
104. Sarina Trangle, *Facial recognition planned for Brooklyn apartment building outrages tenants*, AMNY, Mar. 25, 2019 <https://www.amny.com/real-estate/facial-recognition-apartments-1.28951805>. [↑](#footnote-ref-104)
105. *Id.* [↑](#footnote-ref-105)
106. Monica Melton, *Lawmaker Who Challenged Facial Recognition In Majority Black Building Introduces New Bill For Public Housing*, Forbes, Jul. 23, 2019 <https://www.forbes.com/sites/monicamelton/2019/07/23/hud-bill-blocking-facial-recognition-wont-stop-landlords-plans-to-install-in-majority-black-building/#221df61324f8>. [↑](#footnote-ref-106)
107. Ginia Bellafante, *The Landlord Wants Facial Recognition in Its Rent-Stabilized Buildings. Why?*, NY Times, Mar. 28, 2019, <https://www.nytimes.com/2019/03/28/nyregion/rent-stabilized-buildings-facial-recognition.html>. [↑](#footnote-ref-107)
108. *Id.* [↑](#footnote-ref-108)
109. *Key Fob Fight Brewing Between Tenants, Landlord Of Upper Manhattan Apartment Building*, CBS Local, Nov. 14, 2018 <https://newyork.cbslocal.com/2018/11/14/key-fob-fight-brewing-between-tenants-landlord-of-upper-manhattan-apartment-building>. [↑](#footnote-ref-109)
110. *Id.* [↑](#footnote-ref-110)
111. Aponte, *supra* note 116. [↑](#footnote-ref-111)
112. Tanvi Misra, *The Tenants Fighting Back Against Facial Recognition Technology*, Citylab, May 7, 2019 <https://www.citylab.com/equity/2019/05/facial-recognition-tech-surveillance-security-amazon-ring/588436>. [↑](#footnote-ref-112)
113. Vincent, *supra* note 128. [↑](#footnote-ref-113)
114. <https://www.latch.com/privacy-policy>. [↑](#footnote-ref-114)
115. DHCR # 4 Lease Renewal in Rent Stabilized Apartments, <https://hcr.ny.gov/system/files/documents/2018/09/orafac4.pdf> [↑](#footnote-ref-115)
116. NY RENT STAB § 2524.4(c); *see also* *Primary Residence,*  <https://www1.nyc.gov/site/rentguidelinesboard/resources/primary-residence.page> [↑](#footnote-ref-116)
117. Emily Myer, *The insider's guide to rent-stabilized apartments: Essential knowledge for New York renters,* Brick Underground*,*  Sep. 24, 2019 <https://www.brickunderground.com/blog/2015/01/rent_stabilization_misconceptions> [↑](#footnote-ref-117)
118. *See Katz Park Ave. Corp. v Jagger*, 11 NY3d 314, 317, 898 NE2d 17, 18-19 [2008] (“The Code does not define ‘primary residence’ except to say that ‘no single factor shall be solely determinative,’ and to list ‘evidence which may be considered’ in making the determination. An appellate court has defined the term as ‘an ongoing, substantial, physical nexus with the ... premises for actual living purposes.’”) [↑](#footnote-ref-118)
119. Admin Code § 27-2043. [↑](#footnote-ref-119)
120. New York City Building Code § 1008.4.1. [↑](#footnote-ref-120)