Int. No. 1760-A

By Council Members Levine, Kallos, Rivera, Brannan, Cabrera, Rosenthal, Menchaca, Reynoso, Cornegy, Chin, Ampry-Samuel, Holden, Louis, Lander, Koo, Maisel, Rose, Ayala, Gibson, Grodenchik, Powers, Moya, Adams, Koslowitz, Salamanca, Levin, Barron and the Public Advocate (Mr. Williams)

A Local Law to amend the administrative code of the city of New York, in relation to tenant data privacy

Be it enacted by the Council as follows:

Section 1. Title 26 of the administrative code of the city of New York is amended by adding a new chapter 30 to read as follows:

CHAPTER 30

TENANT DATA PRIVACY

§ 26-3001 Definitions. As used in this chapter, the following terms have the following meanings:

Authentication data. The term "authentication data" means the data generated or collected at the point of authentication in connection with granting a user entry to a smart access building, common area or dwelling unit through such building's smart access system, except that it does not include data generated through or collected by a video or camera system that is used to monitor entrances but not grant entry.

Biometric identifier information. The term "biometric identifier information" means a physiological, biological or behavioral characteristic that is used to identify, or assist in identifying, an individual, including,

but not limited to: (i) a retina or iris scan; (ii) a fingerprint; (iii) a voiceprint; (iv) a scan or record of a palm, hand or face geometry; (v) gait or movement patterns; or (vi) any other similar identifying characteristic.

Dwelling unit. The term "dwelling unit" has the same meaning as in section 27-2004 of the housing maintenance code.

Minor. The term "minor" means a person under the age of 18 years, except a person over the age of 15 years who is married, a parent, serving in the military, or has been found financially independent by a court order.

Multiple dwelling. The term "multiple dwelling" has the same meaning as in section 27-2004 of the housing maintenance code.

Owner. The term "owner" has the same meaning as in section 27-2004 of the housing maintenance code.

Reference data. The term "reference data" means the information against which authentication data is verified at the point of authentication by a smart access system in order to grant a user entry to a smart access building, dwelling unit of such building or a common area of such building.

Smart access building. The term "smart access building" means a class A multiple dwelling, as such term is defined in section 27-2004 of the housing maintenance code, that utilizes a smart access system.

Smart access system. The term "smart access system" means any system that uses electronic or computerized technology, a radio frequency identification card, a mobile phone application, biometric identifier information, or any other digital technology in order to grant entry to a class A multiple dwelling, common areas in such multiple dwelling or to an individual dwelling unit in such multiple dwelling.

Third party. The term "third party" means an entity that installs, operates or otherwise directly supports a smart access system, and has ongoing access to user data, excluding any entity that solely hosts such data.

User. The term "user" means a tenant of a smart access building, and any person a tenant has requested, in writing or through a mobile application, be granted access to such tenant's dwelling unit and such building's

smart access system.

§ 26-3002 Data collection. a. An owner of a smart access building or third party may not collect reference data from a user for use in a smart access system except where such user has expressly consented, in writing or through a mobile application, to the use of such smart access building's smart access system. Such owner or third party may collect only the minimum amount of authentication data and reference data necessary to enable the use of such smart access system in such building, and may not collect additional biometric identifier information from any users. Such smart access system may only collect, generate or utilize the following information:

1. the user's name;

2. the dwelling unit number and other doors or common areas to which the user has access using such smart access system in such building;

3. the user's preferred method of contact;

4. the user's biometric identifier information if such smart access system utilizes biometric identifier information;

5. the identification card number or any identifier associated with the physical hardware used to facilitate building entry, including radio frequency identification card, bluetooth or other similar technical protocols;

6. passwords, passcodes, user names and contact information used singly or in conjunction with other reference data to grant a user entry to a smart access building, dwelling unit of such building or common area of such building through such building's smart access system, or to access any online tools used to manage user accounts related to such building;

7. lease information, including move-in and, if available, move-out dates; and

8. the time and method of access, solely for security purposes.

b. An owner of a smart access building and any third party shall destroy any authentication data

collected from or generated by such smart access system in their possession no later than 90 days after such data has been collected or generated, except for authentication data that is retained in an anonymized format.

c. Reference data for any tenant who has permanently vacated a smart access building shall be removed, or anonymized where removal of such data would render the smart access system inoperable, from the smart access system no later than 90 days after such tenant has permanently vacated such building. Reference data for any user that has been granted access to such tenant's dwelling unit and is not a tenant of such smart access building shall be removed, or anonymized where removal of such data would render the smart access system inoperable, from the smart access system no later than 90 days after access expires. Reference data for any user who has withdrawn authorization from an owner or third party who had previously been given access to such reference data pursuant to subdivision a shall be removed, or anonymized where removal of such data would render the smart access system inoperable, from the smart access system no later than 90 days after such authorization has been withdrawn. The same time frame shall apply when a tenant withdraws a request that a guest be granted access to such tenant's dwelling unit via the smart access system, if such guest is not also a tenant of such smart access building.

d. Reference data collected solely for the operation of such smart access system for a tenant who has permanently vacated a smart access building shall be destroyed no later than 90 days after a tenant has permanently vacated a smart access building or has withdrawn authorization from the owner of such smart access building or a third party. Reference data collected solely for use of such smart access system for any user that has been granted access to such tenant's dwelling unit and is not a tenant of such smart access building shall be destroyed within the same timeframe, following such user's withdrawal of authorization, such tenant's withdrawal of the request that such user be granted access to such tenant's dwelling unit via the smart access system or such tenant's permanent vacation. Any data collected in violation of the prohibitions set forth in paragraphs 3, 4, 5 and 6 of subdivision a of section 26-3003 shall be destroyed immediately.

e. An owner of a smart access building and any third party that has an obligation to destroy data

pursuant to this section shall not be required to destroy any data that:

1. is necessary to detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, or prosecute those responsible for that activity;

2. is necessary to debug to identify and repair errors that impair existing intended functionality;

3. is protected speech under the United States or New York state constitution; or

4. is necessary to comply with another law or legal obligation.

f. Any information that an owner of a multiple dwelling collects about a tenant's use of gas, electricity or any other utility shall be limited to such tenant's total monthly usage, unless otherwise required by law. It shall be unlawful for an owner of a multiple dwelling to collect any information about a tenant's use of internet service, except that in a multiple dwelling in which internet service is provided directly from an owner to tenants, the landlord may collect such information if such information is aggregated and anonymized, or necessary for billing purposes. g. Notwithstanding the provisions of subdivision a, an owner may retain, separate from the smart access system, a record of the unique identification number or other unique identifier associated with the physical hardware used to facilitate building entry, including key cards or other similar technical protocols, and the dwelling unit number associated with such unique identifier, solely for the purpose of deactivating or activating the key card or other hardware associated with such unique identifier.

h. Notwithstanding any other provision of this section, reference data may be retained and utilized by a smart access system pursuant to a user request, in writing or through a mobile application, that such user's reference data be retained for longer than 90 days.

§ 26-3003 Prohibitions. a. It shall be unlawful for any owner of a smart access building or third party that collects reference data or authentication data pursuant to section 26-3002 to:

1. sell, lease or otherwise disclose such data to another person except:

(a) pursuant to any law, subpoena, court ordered warrant, other authorized court ordered process or active law enforcement investigation;

(b) to a third party that operates or facilitates the operation of such building's smart access system, provided that the user has given express authorization, in writing or through a mobile application, and has received in writing, in advance of such authorization: (i) the name of the third party, (ii) the intended use of such data by such third party, and (iii) any privacy policy of such third party;

(c) for data collected pursuant to subdivision f of section 26-3002, to an entity employed, retained or contracted by the owner to improve the energy efficiency of such building;

(d) to a guest as expressly authorized, in writing or through a mobile application, by a tenant; or

(e) as otherwise required by law;

2. utilize any satellite navigation system or other similar system in the equipment or software of a smart access system to track the location of any user of a smart access system outside of the building using such smart access system;

3. use a smart access system to capture the reference data of any minor, except as authorized in writing by such minor's parent or legal guardian;

4. use a smart access system to deliberately collect information on or track the relationship status of tenants and their guests, except as otherwise required by law;

5. use a smart access system to collect or track information about the frequency and time of use of such system by a tenant and their guests to harass or evict a tenant;

6. use a smart access system to collect reference data from a person who is not a tenant in such smart access building who has not given express consent, in writing or through a mobile application, provided that reference data may be collected for any employee or agent of an owner in a smart access building, and

7. share any data that may be collected from a smart access system regarding any minor, unless such entity has received the written authorization of such minor's parent or legal guardian.

b. It shall additionally be unlawful for any owner of a smart access building, or an agent thereof, to:

1. utilize data collected through a smart access system for any purpose other than: (i) to grant access to

and monitor entrances and exits to the smart access building, and to common areas in such building, including but not limited to laundry rooms, mail rooms, and the like, and (ii) to grant access to dwelling units in such buildings that use a smart access system to grant entry into dwelling units;

2. use a smart access system to limit the time of entry into the building by any user except as requested by a tenant;

3. require a tenant to use a smart access system to gain entry to such tenant's dwelling unit; and

4. use any information collected through a smart access system to harass or evict a tenant.

§ 26-3004 Privacy policies. a. The owner of a smart access building, or an agent thereof, must provide to tenants a written policy in plain language that describes, at a minimum, the following information if it is not included in the privacy policy described in subdivision b:

1. the data elements to be collected by the smart access system;

2. the names of any entities or third parties the owner will share such data elements with, and the privacy policies of any such entities or third parties;

3. the protocols and safeguards the owner will provide for protecting such data elements;

4. the retention schedule of such data;

5. the protocols the owner will follow to address any suspected or actual unauthorized access to or disclosure of such data elements, including notification of users;

6. guidelines for permanently destroying or anonymizing such data or removing such data from the smart access system; and

7. the process used to add and remove persons who have provided written consent on a temporary basis to the smart access system.

b. The owner of a smart access building, or an agent thereof, shall make available to tenants any written privacy policy of the entity that developed the smart access system utilized in such building, or any written privacy policy of the entity that currently operates the smart access system utilized in such building.

§ 26-3005 Security measures and safeguards. A smart access system must implement stringent security measures and safeguards to protect the security and data of tenants, guests and other individuals in smart access buildings. Such security measures and safeguards must, at a minimum, include data encryption, the ability of the user to change the password if the system uses a password and firmware that is regularly updated to enable the remediation of any security or vulnerability issues.

§ 26-3006 Private right of action. a. A lawful occupant of a dwelling unit, or a group of such occupants, in a smart access building may bring an action alleging an unlawful sale of data in violation of paragraph one of subdivision a of section 26-3003 in any court of competent jurisdiction. If such court finds that a person is in violation of such paragraph for the unlawful sale of data, such court shall, in addition to any other relief such court determines to be appropriate:

1. Award to each such occupant per each unlawful sale of such occupant's data: (i) compensatory damages and, in such court's discretion, punitive damages, or (ii) at the election of each occupant, damages ranging from $200 to $1,000; and

2. Award to such occupants reasonable attorneys' fees and court costs.

b. Nothing in this section shall relieve any such occupant or occupants from any obligation to pay rent or any other charge for which such occupant or occupants are otherwise liable to a person found to be in violation of this chapter. Nothing in this section shall affect any other right or responsibility of an occupant or owner afforded to such person pursuant to a lawful lease.

c. This section does not limit or abrogate any claim or cause of action a person has under common law or by other law or rule. The provisions of this section are in addition to any other remedies that may be provided for under common law or by other law or rule.

§ 26-3007 Education efforts. The department of housing preservation and development shall inform tenants and owners about the provisions of this chapter by, at a minimum, including information about this chapter on its website and in the housing information guide for tenants and owners described in section 26-

1102.

§ 2. This local law takes effect 60 days after it becomes law, except that no owner of an existing smart access building shall be liable for a violation of chapter 30 of title 26 of the administrative code of the city of New York, as added by section one of this local law, until January 1, 2023, in order to allow such owner to replace or upgrade such building's smart access system to comply with the provisions of this local law.

AS
LS # 9033, 10404
4/21/21 9:54 p.m.