Int. No. 1760

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 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. Subchapter 2 of chapter 2 of title 27 of the administrative code of the city of New York is amended by adding a new article 21-A to read as follows:

ARTICLE 21-A

TENANT DATA PRIVACY

§ 27-2051.5 Definitions. As used in this article, the following terms have the following meanings:

Authentication data. The term "authentication data" means the data collected at the point of authentication to grant a user entry to a smart access building through such building's smart access system.

Biometric identifier. The term "biometric identifier" means a retina or iris scan, fingerprint, voiceprint, or record of hand, face geometry or other similar feature.

Minor. The term "minor" means a person under the age of eighteen years.

Reference data. The term "reference data" means the information used for reference by a smart access system at the point of authentication.

Smart access building. The term “smart access building” means a multiple dwelling that utilizes a smart access system.

Smart access system. The term “smart access” means any system that uses electronic or computerized technology, a radio frequency identification card, a mobile phone application, biometric identifier or any other digital technology in order to grant entry to a multiple dwelling.

§ 27-2051.6 Data collection. a. An owner of a smart access building may not collect reference data from a tenant except where such tenant has expressly consented to the use of such smart access building’s smart access system. Such owner may collect only the minimum authentication data and reference data necessary to enable the use of such smart access system in such building, and shall be limited to: (i) the tenant’s name, (ii) the tenant’s apartment number, (iii) the tenant’s preferred method of contact, and, if such smart access system utilizes biometric identifiers (iv) the tenant’s biometric identifier. A copy of such reference data may be retained only by the tenant and by the owner of the tenant’s building if such owner has been given access to such reference data by such tenant. In a building where a smart access system is used to grant entry to a dwelling unit, the owner of such building shall, at the request of the tenant of such dwelling unit, retain for the duration of the tenancy any authentication data and reference data generated in the use of such smart access system to access such dwelling unit.

b. An owner of a smart access building shall destroy any authentication data collected from such smart access system no later than 90 days after such data has been collected. Reference data for any tenant who has permanently vacated a smart access building shall be destroyed no later than 90 days after such tenant has permanently vacated such building. Reference data for any tenant who has withdrawn authorization from an owner who had previously been given access to such reference data pursuant to subdivision a shall be destroyed no later than 90 days after such authorization has been withdrawn. Any data collected in violation of the prohibitions set forth in paragraphs 3, 4, 5 and 6 of subdivision a of section 27-2051.7 shall be destroyed immediately.

c. 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. It shall be unlawful for an owner of a multiple dwelling to collect any information about a tenant's use of internet service.

§ 27-2051.7 Prohibitions. a. It shall be unlawful for any entity that collects data pursuant to section 27-2051.6 to:

1. sell, lease or otherwise disclose such data to another person except pursuant to a subpoena, court ordered warrant or other authorized court ordered process;

2. utilize any form of location tracking in the equipment or software of a smart access system;

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

4. use a smart access system to collect information on the relationship status of tenants and their guests;

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

6. use a smart access system to collect reference data from a person who is not a tenant in such smart access building, except as authorized by the tenant who has granted access to such person;

7. share any such data with a third party unless the tenant has given express authorization and has received in writing: (i) the name of the third party, (ii) the intended use of such data by such third party, and (iii) any privacy policies of such third party; and

8. share any data that may be collected from a smart access system of any minor, unless such entity has received the written authorization of such minor's legal parent or 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 to monitor entrances and exits to the multiple dwelling and to entrances to common areas in such building, including but not limited to laundry rooms, mail rooms, and the like;

2. use a smart access system to limit the time or place of entrance by a guest or any other person authorized by a tenant to enter such building; and

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

§ 27-2051.8 Privacy policies. a. The owner of a smart access building, or an agent thereof, must provide to tenants a written policy that describes, at a minimum:

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

2. the retention schedule of such data;

3. guidelines for permanently destroying such data; and

4. the process used to add persons authorized by the tenant 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, if different from or not included in the policy provided in subdivision a, any written privacy policy of the entity that developed the smart access system utilized in such building.

§ 27-2051.9 Penalties. A person who violates any provision of this article shall be liable for a civil penalty of not more than $6,000 for each violation.

§ 2. This local law takes effect immediately.

AS
LS # 9033, 10404
10/10/19