STATE OF NEW YORK

2078--A

2023-2024 Regular Sessions

IN SENATE

January 18, 2023

Introduced by Sens. KAVANAGH, KRUEGER -- read twice and ordered printed, and when printed to be committed to the Committee on Housing, Construction and Community Development -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the multiple dwelling law and the multiple residence law, in relation to the use of smart access systems and the information that may be gathered from such systems

The People of the State of New York, represented in Senate and Assembly, do enact as follows:

Section 1. The multiple dwelling law is amended by adding a new section 50-b to read as follows:

§ 50-b. Electronic or computerized entry systems. 1. Definitions. For the purposes of this section, the following terms shall have the following meanings:

a. "Account information" means information that is used to grant a user entry or access to any online tools that are used to manage user accounts related to a smart access system.

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

c. "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 that can be used

EXPLANATION--Matter in *italics* (underscored) is new; matter in brackets [-] is old law to be omitted.

LBD00692-07-3

alone or in combination with each other, or with other information, to establish individual identity.

d. "Critical security vulnerability" means a security vulnerability that has a significant risk of resulting in an unauthorized access to an area secured by a smart access system.

e. "Reference data" means 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 class A multiple dwelling, dwelling unit of such building, or common area of such building.

f. "Security breach" means any incident that results in unauthorized access of data, applications, services, networks or devices by bypassing underlying security mechanisms. A "security breach" occurs when an individual or an application illegitimately enters a private, confidential or unauthorized logical information technology perimeter.

g. "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 access to a class A multiple dwelling, common areas in such multiple dwelling, or to an individual dwelling unit in such multiple dwelling.

h. "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.

i. "User" means a tenant or lawful occupant of a class A multiple dwelling, and any person a tenant or lawful occupant has requested, in writing or through a mobile application, be granted access to such tenant or lawful occupant's dwelling unit and such building's smart access system.

2. Entry. a. Where an owner installs or plans to install a smart access system on any entrance from the street, passageway, court, yard, cellar, or other common area of a class A multiple dwelling, such system shall not rely solely on a web-based application to facilitate entrance but shall also include a key fob, key card, digital key or passcode for tenant use.

b. Owners may provide various methods of entry into individual apartments including a mechanical key or a smart access system of a key fob, key card or digital key, provided, however that such smart access system shall not rely solely on a web-based application.

c. Notwithstanding paragraph a or b of this subdivision, owners shall provide a non-electronic means of entry where requested by the tenant or lawful occupant due to a religious preference.

d. All lawful tenants and lawful occupants shall be provided with a key, key fob, digital key or key card at no cost to such tenants and lawful occupants. The term "lawful occupants" shall include children under the age of eighteen who shall be issued a key, key fob, digital key or key card if a parent or guardian requests such child be provided with one. Tenants and lawful occupants may also receive up to four additional keys, key fobs, digital keys or key cards at no cost to the tenant or lawful occupant for employees or guests. The term "guests" shall include family members and friends who can reasonably be expected to visit on a regular basis or visit as needed to care for the tenant, lawful occupant, or the dwelling unit if the tenant or lawful occupant is away. Employees, including contractors, professional caregivers or other services providers, may have an expiration date placed on their key, key card, digital key or key fob, which may be extended upon the tenant's or lawful occupant's request. Tenants or lawful occupants may

request a new or replacement key, key fob, digital key or key card at any time throughout the course of the tenancy or occupancy. The owner or their agent shall provide the first replacement key, key fob, digital key or key card to the tenant or lawful occupant free of charge. The cost of second and subsequent replacement cards shall not be more than what the owner paid for the replacement up to and not exceeding twenty-five dollars.

e. The owner shall not set limits on the number of keys, key fobs, digital keys or key cards a tenant or lawful occupant may request.

f. Any door that has a smart access system shall have backup power or an alternative means of entry to ensure that the entry system continues to operate during a power outage. An owner, or their agent, shall routinely inspect the backup power and shall replace according to system specifications. Owners or their agents shall provide tenants and lawful occupants with information about whom to contact in the event that the tenant, lawful occupant or the tenant's or lawful occupant's children, guests or employees become locked out.

3. Notice. Owners or their agents shall provide notice to a tenant or lawful occupant at the time the tenant or lawful occupant signs the lease, or when the smart access system is installed, of the provisions of subdivision two of this section.

4. Data collection. a. If a smart access system is utilized to gain entrance to a class A multiple dwelling, the only reference, authentication, and account information gathered by any smart access system shall be limited to account information necessary to enable the use of such smart access system, or reference data, including the user's name, dwelling unit number and other doors or common areas to which the user has access, the preferred method of contact for such user, information used to grant a user entry or to access any online tools used to manage user accounts related to such building, lease information including move-in and, if available move-out dates, and authentication data such as time and method of access for security purposes and a photograph of access events for security purposes. For smart access systems that rely on the collection of biometric data and which have already been installed at the time this section shall have become a law, biometric identifier information may be collected pursuant to this section in order to register a user for a smart access system. No new smart access systems that rely on the collection of biometric data shall be installed in class A multiple dwellings for three years after the effective date of this section.

(i) The owner of the multiple dwelling may collect only the minimum data required by the technology used in the smart access system to effectuate such entrance and protect the privacy and security of such users.

(ii) The owner or agent of the owner shall not request or retain, in any form, the social security number of any tenant or lawful occupant as a condition of use of the smart access system.

(iii) The owner, agent of the owner, or the vendor of a smart access system on behalf of the owner may record each time a key fob, key card, digital key or passcode is used to enter the building, but shall not record any departures.

(iv) A copy of such data may be retained for reference at the point of authentication by the smart access system. Such reference data shall be retained only for tenants or lawful occupants or those authorized by the tenant, lawful occupant, or owner of the multiple dwelling.

(v) The owner of the multiple dwelling or any third party shall destroy or anonymize authentication data collected from or generated by such smart access system within a reasonable time, but not later than ninety days after the date collected.

(vi) Reference data for a user shall be destroyed or anonymized within ninety days of (1) the tenant or lawful occupant permanently vacating the dwelling, or (2) a request by the tenant or lawful occupant to withdraw authorization for those previously authorized by the tenant or lawful occupant.

b. (i) An entity shall not capture biometric identifier information of an individual to gain entrance to a class A multiple dwelling unless the person is a tenant or lawful occupant or a person authorized by the tenant or lawful occupant, and informs the individual before capturing the biometric identifier information; and receives their express consent to capture the biometric identifier information.

(ii) Any entity that possesses biometric identifier information of an individual that is captured to gain entrance to a class A multiple dwelling:

(1) Shall not sell, lease or otherwise disclose the biometric identifier information to another person unless pursuant to any law, grand jury subpoena or court ordered warrant, subpoena, or other authorized court ordered process.

(2) Shall store, transmit and protect from disclosure the biometric identifier information using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits and protects confidential information the person possesses; and

(3) Shall destroy the biometric identifier information within a reasonable time, but not later than forty-eight hours after the date collected, except for reference data. If any prohibited information is collected, such as the likeness of a minor or a non-tenant, the information shall be destroyed immediately.

c. The owner of the multiple dwelling, or the managing agent, shall develop and provide to tenants and lawful occupants written procedures which describe the process used to add persons authorized by the tenant or lawful occupant to the smart access system on a temporary or permanent basis, such as visitors, children, their employees, and caregivers to such building.

(i) The procedures shall clearly establish the owner's retention schedule and guidelines for permanently destroying or anonymizing the data collected.

(ii) The procedures shall not limit time or place of entrance by such people authorized by the tenant or lawful occupant except as requested by the tenant or lawful occupant.

5. Prohibitions. a. No form of location tracking, including but not limited to satellite location based services, shall be included in any equipment, key, or software provided to users as part of a smart access system.

b. It shall be prohibited to collect through a smart access system the likeness of a minor occupant, information on the relationship status of tenants or lawful occupants and their guests, or to use a smart access system to collect or track information about the frequency and time of use of such system by a tenant or lawful occupant and their guests to harass or evict a tenant or lawful occupant or for any other purpose not expressly related to the operation of the smart access system.

c. Information that is acquired via the use of a smart access system shall not be used for any purposes other than granting access to and monitoring building entrances and shall not be used as the basis or support for an action to evict a lessee, tenant, or lawful occupant, or an administrative hearing seeking a change in regulatory coverage for an individual or unit. However, a tenant or lawful occupant may authorize their information to be used by a third party, but such a request shall clearly state who will have access to such information, for what purpose it will be used, and the privacy policies which will protect their information. Under no circumstances shall a lease or a renewal be contingent upon authorizing such use. Smart access systems may use third-party services to the extent required to maintain and operate system infrastructure, including cloud-based hosting and storage. The provider or providers of third-party infrastructure services shall meet or exceed the privacy protections set forth in this section and shall be subject to the same liability for breach of any of the requirements of this section.

d. Information and data collected shall not be made available to any third party, unless authorized as described in paragraph c of this subdivision, including but not limited to law enforcement, except upon a grand jury subpoena or a court ordered warrant, subpoena, or other authorized court ordered process.

6. Storage of information. Any information or data collected shall be stored in a secure manner to prevent unauthorized access by both employees and contractors and those unaffiliated with the owner or their agents, except as otherwise provided in this section. Future or continuing tenancy shall not be conditioned upon consenting to the use of a smart access system.

7. Software issues. Whenever a company that produces, makes available or installs smart access systems discovers a security breach or critical security vulnerability in their software, such company shall notify customers of such vulnerability within a reasonable time of discovery but no later than twenty-four hours after discovery and shall make software updates available and take any other action as may be necessary to repair the vulnerability within a reasonable time, but not longer than thirty days after discovery. Smart access systems and vendors shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected. In the event that a security breach or critical security vulnerability that pertains to the embedded software or firmware on the smart access systems is discovered, smart access systems and their vendors shall:

a. be able to create updates to the firmware to correct the vulnerabilities;

b. contractually commit to customers that the smart access system or vendor will create updates to the embedded software or firmware to remedy the vulnerabilities; and

c. make such security-related software or firmware updates available for free to customers for the duration of the contract between the building and smart access systems.

8. Waiver of rights; void. Any agreement by a lessee or tenant of a dwelling waiving or modifying their rights as set forth in this section shall be void as contrary to public policy.

9. Penalties. a. A person who violates this section shall be subject to a civil penalty of not more than five thousand dollars for each violation. The attorney general may bring an action to recover the civil penalty.

b. Where an owner or their agent uses a smart access system to harass or otherwise deprive a tenant or lawful occupant of any rights available under law, such owner or agent shall be subject to a civil penalty of ten thousand dollars for each violation.

c. For purposes of this subdivision, each day the violation occurs shall be considered a separate violation.

10. Rent regulated dwellings. Installation of a smart access system pursuant to this section in a dwelling subject to the emergency tenant protection act of nineteen hundred seventy-four, the emergency housing rent control law, the local emergency housing rent control act, or the rent stabilization law of nineteen hundred sixty-nine shall constitute a modification of services requiring the owner of such dwelling or their agent to apply to the division of housing and community renewal for approval before performing such installation. Such installation shall not qualify as a basis for rent reduction.

11. Exemptions. a. Nothing herein shall apply to multiple dwellings owned or managed by an entity subject to 42 U.S.C. § 1437 et seq., or any of its subsidiaries.

b. Nothing in this section shall limit the authority of the division of housing and community renewal to impose additional requirements regarding smart access systems installed in multiple dwellings for which the division is required to approve substitutions or modifications of services.

§ 2. The multiple residence law is amended by adding a new section 130-a to read as follows:

§ 130-a. Electronic or computerized entry systems. 1. Definitions. For the purposes of this section, the following terms shall have the following meanings:

(a) "Account information" means information that is used to grant a user entry or access to any online tools that are used to manage user accounts related to a smart access system.

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

(c) "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 that can be used alone or in combination with each other, or with other information, to establish individual identity.

(d) "Critical security vulnerability" means a security vulnerability that has a significant risk of resulting in an unauthorized access to an area secured by a smart access system.

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

(f) "Security breach" means any incident that results in unauthorized access of data, applications, services, networks or devices by bypassing underlying security mechanisms. A "security breach" occurs when an indi-

vidual or an application illegitimately enters a private, confidential or unauthorized logical information technology perimeter.

(g) "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 access to a multiple dwelling, common areas in such multiple dwelling, or to an individual dwelling unit in such multiple dwelling.

(h) "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.

(i) "User" means a tenant or lawful occupant of a multiple dwelling, and any person a tenant or lawful occupant has requested, in writing or through a mobile application, be granted access to such tenant or lawful occupant's dwelling unit and such building's smart access system.

2. Entry. (a) Where an owner installs or plans to install a smart access system on any entrance from the street, passageway, court, yard, cellar, or other common area of a multiple dwelling, such system shall not rely solely on a web-based application to facilitate entrance but shall also include a key fob, key card, digital key or passcode for tenant use.

(b) Owners may provide various methods of entry into individual apartments including a mechanical key or a smart access system of a key fob, key card or digital key, provided, however that such smart access system shall not rely solely on a web-based application.

(c) Notwithstanding paragraph (a) or (b) of this subdivision, owners shall provide a non-electronic means of entry where requested by the tenant or lawful occupant due to a religious preference.

(d) All lawful tenants and lawful occupants shall be provided with a key, key fob, digital key or key card at no cost to such tenants and lawful occupants. The term "lawful occupants" shall include children under the age of eighteen who shall be issued a key, key fob, digital keys or key card if a parent or guardian requests such child be provided with one. Tenants and lawful occupants may also receive up to four additional keys, key fobs, digital keys or key cards at no cost to the tenant or lawful occupant for employees or guests. The term "guests" shall include family members and friends who can reasonably be expected to visit on a regular basis or visit as needed to care for the tenant, lawful occupant, or the dwelling unit if the tenant or lawful occupant is away. Employees, including contractors, professional caregivers or other services providers, may have an expiration date placed on their key, key card, digital key or key fob, which may be extended upon the tenant or lawful occupant's request. Tenants or lawful occupants may request a new or replacement key, key fob, digital key or key card at any time throughout the course of the tenancy. The owner or their agent shall provide the first replacement key, key fob, digital key or key card to the tenant or lawful occupant free of charge. The cost of second and subsequent replacement cards shall not be more than what the owner paid for the replacement up to and not exceeding twenty-five dollars.

(e) The owner shall not set limits on the number of keys, key fobs, digital keys or key cards a tenant or lawful occupant may request.

(f) Any door that has a smart access system shall have backup power or an alternative means of entry to ensure that the entry system continues to operate during a power outage. An owner, or their agent, shall routinely inspect the backup power and shall replace according to system specifications. Owners or their agents shall provide tenants and lawful

occupants with information about whom to contact in the event that the tenant, lawful occupant or the tenant's or lawful occupant's children, guests or employees become locked out.

3. Notice. Owners or their agents shall provide notice to a tenant or lawful occupant at the time the tenant or lawful occupant signs the lease, or when the smart access system is installed, of the provisions of subdivision two of this section.

4. Data collection. (a) If a smart access system is utilized to gain entrance to a multiple dwelling, the only reference, authentication, and account information gathered by any smart access system shall be limited to account information necessary to enable the use of such smart access system, or reference data, including the user's name, dwelling unit number and other doors or common areas to which the user has access, the preferred method of contact for such user, information used to grant a user entry or to access any online tools used to manage user accounts related to such building, lease information including move-in and, if available move-out dates, and authentication data such as time and method of access for security purposes and a photograph of access events for security purposes. For smart access systems that rely on the collection of biometric data and which have already been installed at the time this section shall have become a law, biometric identifier information may be collected pursuant to this section in order to register a user for a smart access system. No new smart access systems that rely on the collection of biometric data shall be installed in multiple dwellings for three years after the effective date of this section.

(i) The owner of the multiple dwelling shall collect only the minimum data required by the technology used in the smart access system to effectuate such entrance and protect the privacy and security of such users.

(ii) The owner or agent of the owner shall not request or retain, in any form, the social security number of any tenant or lawful occupant as a condition of use of the smart access system.

(iii) The owner, agent of the owner, or the vendor of a smart access system on behalf of the owner may record each time a key fob, key card, digital key or passcode is used to enter the building, but shall not record any departures.

(iv) A copy of such data may be retained for reference at the point of authentication by the smart access system. Such reference data shall be retained only for tenants or lawful occupants or those authorized by the tenant, lawful occupant, or owner of the multiple dwelling.

(v) The owner of the multiple dwelling or any third party shall destroy or anonymize authentication data collected from or generated by such smart access system within a reasonable time, but not later than ninety days after the date collected.

(vi) Reference data for a user shall be destroyed or anonymized within ninety days of (1) the tenant or lawful occupant permanently vacating the dwelling, or (2) a request by the tenant or lawful occupant to withdraw authorization for those previously authorized by the tenant or lawful occupant.

(b) (i) An entity shall not capture biometric identifier information of an individual to gain entrance to a multiple dwelling unless the person is a tenant or lawful occupant or a person authorized by the tenant or lawful occupant, and informs the individual before capturing the biometric identifier information; and receives their express consent to capture the biometric identifier information.

(ii) Any entity that possesses biometric identifier information of an individual that is captured to gain entrance to a multiple dwelling:

(1) Shall not sell, lease or otherwise disclose the biometric identifier information to another person unless pursuant to any law, grand jury subpoena or court ordered warrant, subpoena, or other authorized court ordered process.

(2) Shall store, transmit and protect from disclosure the biometric identifier information using reasonable care and in a manner that is the same as or more protective than the manner in which the person stores, transmits and protects confidential information the person possesses; and

(3) Shall destroy the biometric identifier information within a reasonable time, but not later than forty-eight hours after the date collected, except for reference data. If any prohibited information is collected, such as the likeness of a minor or a non-tenant, the information shall be destroyed immediately.

(c) The owner of the multiple dwelling, or the managing agent, shall develop and provide to tenants and lawful occupants written procedures which describe the process used to add persons authorized by the tenant or lawful occupant to the smart access system on a temporary or permanent basis, such as visitors, children, their employees, and caregivers to such building.

(i) The procedures shall clearly establish the owner's retention schedule and guidelines for permanently destroying or anonymizing the data collected.

(ii) The procedures shall not limit time or place of entrance by such people authorized by the tenant or lawful occupant except as requested by the tenant or lawful occupant.

5. Prohibitions. (a) No form of location tracking, including but not limited to satellite location based services, shall be included in any equipment, key, or software provided to users as part of a smart access system.

(b) It shall be prohibited to collect through a smart access system the likeness of a minor occupant, information on the relationship status of tenants or lawful occupants and their guests, or to use a smart access system to collect or track information about the frequency and time of use of such system by a tenant or lawful occupant and their guests to harass or evict a tenant or lawful occupant or for any other purpose not expressly related to the operation of the smart access system.

(c) Information that is acquired via the use of a smart access system shall not be used for any purposes other than granting access to and monitoring building entrances and shall not be used as the basis or support for an action to evict a lessee, tenant, or lawful occupant, or an administrative hearing seeking a change in regulatory coverage for an individual or unit. However, a tenant or lawful occupant may authorize their information to be used by a third party, but such a request shall clearly state who will have access to such information, for what purpose it will be used, and the privacy policies which will protect their information. Under no circumstances shall a lease or a renewal be contingent upon authorizing such use. Smart access systems may use third-party services to the extent required to maintain and operate system infrastructure, including cloud-based hosting and storage. The provider or providers of third-party infrastructure services shall meet or exceed the privacy protections set forth in this section and shall be

subject to the same liability for breach of any of the requirements of this section.

(d) Information and data collected shall not be made available to any third party, unless authorized as described in paragraph (c) of this subdivision, including but not limited to law enforcement, except upon a grand jury subpoena or a court ordered warrant, subpoena, or other authorized court ordered process.

6. Storage of information. Any information or data collected shall be stored in a secure manner to prevent unauthorized access by both employees and contractors and those unaffiliated with the owner or their agents, except as otherwise provided in this section. Future or continuing tenancy shall not be conditioned upon consenting to the use of a smart access system.

7. Software issues. Whenever a company that produces, makes available or installs smart access systems discovers a security breach or critical security vulnerability in their software, such company shall notify customers of such vulnerability within a reasonable time of discovery but no later than twenty-four hours after discovery and shall make software updates available and take any other action as may be necessary to repair the vulnerability within a reasonable time, but not longer than thirty days after discovery. Smart access systems and vendors shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information collected. In the event that a security breach or critical security vulnerability that pertains to the embedded software or firmware on the smart access systems is discovered, smart access systems and their vendors shall:

(a) be able to create updates to the firmware to correct the vulnerabilities;

(b) contractually commit to customers that the smart access system or vendor will create updates to the embedded software or firmware to remedy the vulnerabilities; and

(c) make such security-related software or firmware updates available for free to customers for the duration of the contract between the building and smart access systems.

8. Waiver of rights; void. Any agreement by a lessee or tenant of a dwelling waiving or modifying their rights as set forth in this section shall be void as contrary to public policy.

9. Penalties. (a) A person who violates this section shall be subject to a civil penalty of not more than five thousand dollars for each violation. The attorney general may bring an action to recover the civil penalty. An individual injured by a violation of this section may bring an action to recover damages. A court may also award attorneys' fees to a prevailing plaintiff.

(b) Where an owner or their agent uses a smart access system to harass or otherwise deprive a tenant or lawful occupant of any rights available under law, such owner or agent shall be subject to a civil penalty of ten thousand dollars for each violation.

(c) For purposes of this subdivision, each day the violation occurs shall be considered a separate violation.

10. Rent regulated dwellings. Installation of a smart access system pursuant to this section in a dwelling subject to the emergency tenant protection act of nineteen hundred seventy-four, the emergency housing rent control law, the local emergency housing rent control act, or the rent stabilization law of nineteen hundred sixty-nine shall constitute a modification of services requiring the owner of such dwelling or their agent to apply to the division of housing and community renewal for

approval before performing such installation. Such installation shall not qualify as a basis for rent reduction.

11. Exemptions. (a) Nothing herein shall apply to multiple dwellings owned or managed by an entity subject to 42 U.S.C. § 1437 et seq., or any of its subsidiaries.

(b) Nothing in this section shall limit the authority of the division of housing and community renewal to impose additional requirements regarding smart access systems installed in multiple dwellings for which the division is required to approve substitutions or modifications of services.

§ 3. Severability. If any provision of this act, or any application of any provision of this act, is held to be invalid, that shall not affect the validity or effectiveness of any other provision of this act, or of any other application of any provision of this act, which can be given effect without that provision or application; and to that end, the provisions and applications of this act are severable.

§ 4. This act shall take effect on the one hundred eightieth day after it shall have become a law.