

# STATE OF NEW YORK

2078--B

Cal. No. 1016

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 -- recommitted to the Committee on Housing, Construction and Community Development in accordance with Senate Rule 6, sec. 8 -- reported favorably from said committee, ordered to first and second report, ordered to a third reading, amended and ordered reprinted, retaining its place in the order of third reading

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:

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

3 § 50-b. Electronic or computerized entry systems. 1. Definitions. For  
4 the purposes of this section, the following terms shall have the follow-  
5 ing meanings:

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

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

15 c. "Biometric identifier information" means a physiological, biolog-  
16 ical or behavioral characteristic that is used to identify, or assist in  
17 identifying, an individual, including, but not limited to: (i) a retina

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

LBD00692-11-4

1 or iris scan, (ii) a fingerprint, (iii) a voiceprint, (iv) a scan or  
2 record of a palm, hand, or face geometry, (v) gait or movement patterns,  
3 or (vi) any other similar identifying characteristic that can be used  
4 alone or in combination with each other, or with other information, to  
5 establish individual identity.

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

9 e. "Reference data" means information against which authentication  
10 data is verified at the point of authentication by a smart access system  
11 in order to grant a user entry to a class A multiple dwelling, dwelling  
12 unit of such building, or common area of such building.

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

18 g. "Smart access system" means any system that uses electronic or  
19 computerized technology, a radio frequency identification card, a mobile  
20 phone application, biometric identifier information, or any other  
21 digital technology in order to grant access to a class A multiple dwell-  
22 ing, common areas in such multiple dwelling, or to an individual dwell-  
23 ing unit in such multiple dwelling.

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

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

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

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

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

45 d. All lawful tenants and lawful occupants shall be provided with a  
46 key, key fob, digital key or key card at no cost to such tenants and  
47 lawful occupants. The term "lawful occupants" shall include children  
48 under the age of eighteen who shall be issued a key, key fob, digital  
49 key or key card if a parent or guardian requests such child be provided  
50 with one. Tenants and lawful occupants may also receive up to four addi-  
51 tional keys, key fobs, digital keys or key cards at no cost to the  
52 tenant or lawful occupant for employees or guests. The term "guests"  
53 shall include family members and friends who can reasonably be expected  
54 to visit on a regular basis or visit as needed to care for the tenant,  
55 lawful occupant, or the dwelling unit if the tenant or lawful occupant  
56 is away. Employees, including contractors, professional caregivers or

1 other services providers, may have an expiration date placed on their  
2 key, key card, digital key or key fob, which may be extended upon the  
3 tenant's or lawful occupant's request. Tenants or lawful occupants may  
4 request a new or replacement key, key fob, digital key or key card at  
5 any time throughout the course of the tenancy or occupancy. The owner  
6 or their agent shall provide the first replacement key, key fob, digital  
7 key or key card to the tenant or lawful occupant free of charge. The  
8 cost of second and subsequent replacement cards shall not be more than  
9 what the owner paid for the replacement up to and not exceeding twenty-  
10 five dollars.

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

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

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

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

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

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

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

55 (iv) A copy of such data may be retained for reference at the point of  
56 authentication by the smart access system. Such reference data shall be

1 retained only for tenants or lawful occupants or those authorized by  
2 the tenant, lawful occupant, or owner of the multiple dwelling.

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

7 (vi) Reference data for a user shall be destroyed or anonymized within  
8 ninety days of (1) the tenant or lawful occupant permanently vacating  
9 the dwelling, or (2) a request by the tenant or lawful occupant to with-  
10 draw authorization for those previously authorized by the tenant or  
11 lawful occupant.

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

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

21 (1) Shall not sell, lease or otherwise disclose the biometric identi-  
22 fier information to another person unless pursuant to any law, grand  
23 jury subpoena or court ordered warrant, subpoena, or other authorized  
24 court ordered process.

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

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

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

41 (i) The procedures shall clearly establish the owner's retention sche-  
42 dule and guidelines for permanently destroying or anonymizing the data  
43 collected.

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

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

51 b. It shall be prohibited to collect through a smart access system the  
52 likeness of a minor occupant, information on the relationship status of  
53 tenants or lawful occupants and their guests, or to use a smart access  
54 system to collect or track information about the frequency and time of  
55 use of such system by a tenant or lawful occupant and their guests to

1 harass or evict a tenant or lawful occupant or for any other purpose not  
2 expressly related to the operation of the smart access system.

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

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

25 6. Storage of information. Any information or data collected shall be  
26 stored in a secure manner to prevent unauthorized access by both employ-  
27 ees and contractors and those unaffiliated with the owner or their  
28 agents, except as otherwise provided in this section. Future or contin-  
29 ing tenancy shall not be conditioned upon consenting to the use of a  
30 smart access system.

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

44 a. be able to create updates to the firmware to correct the vulner-  
45 abilities;

46 b. contractually commit to customers that the smart access system or  
47 vendor will create updates to the embedded software or firmware to reme-  
48 dy the vulnerabilities; and

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

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

55 9. Penalties. a. A person who violates this section shall be subject  
56 to a civil penalty of not more than five thousand dollars for each

1 violation. The attorney general may bring an action to recover the civil  
2 penalty.

3 b. Where an owner or their agent uses a smart access system to harass  
4 or otherwise deprive a tenant or lawful occupant of any rights available  
5 under law, such owner or agent shall be subject to a civil penalty of  
6 not more than ten thousand dollars for each violation.

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

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

18 11. Exemptions. a. Nothing herein shall apply to multiple dwellings  
19 owned or managed by an entity subject to 42 U.S.C. § 1437 et seq., or  
20 any of its subsidiaries, or multiple dwellings that are primarily occu-  
21 ped by transient occupants for a period of less than thirty days.

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

27 § 2. The multiple residence law is amended by adding a new section  
28 130-a to read as follows:

29 § 130-a. Electronic or computerized entry systems. 1. Definitions. For  
30 the purposes of this section, the following terms shall have the follow-  
31 ing meanings:

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

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

41 (c) "Biometric identifier information" means a physiological, biolog-  
42 ical or behavioral characteristic that is used to identify, or assist in  
43 identifying, an individual, including, but not limited to: (i) a retina  
44 or iris scan, (ii) a fingerprint, (iii) a voiceprint, (iv) a scan or  
45 record of a palm, hand, or face geometry, (v) gait or movement patterns,  
46 or (vi) any other similar identifying characteristic that can be used  
47 alone or in combination with each other, or with other information, to  
48 establish individual identity.

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

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

1 (f) "Security breach" means any incident that results in unauthorized  
2 access of data, applications, services, networks or devices by bypassing  
3 underlying security mechanisms. A "security breach" occurs when an indi-  
4 vidual or an application illegitimately enters a private, confidential  
5 or unauthorized logical information technology perimeter.

6 (g) "Smart access system" means any system that uses electronic or  
7 computerized technology, a radio frequency identification card, a mobile  
8 phone application, biometric identifier information, or any other  
9 digital technology in order to grant access to a multiple dwelling,  
10 common areas in such multiple dwelling, or to an individual dwelling  
11 unit in such multiple dwelling.

12 (h) "Third party" means an entity that installs, operates or otherwise  
13 directly supports a smart access system, and has ongoing access to user  
14 data, excluding any entity that solely hosts such data.

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

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

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

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

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

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

55 (f) Any door that has a smart access system shall have backup power or  
56 an alternative means of entry to ensure that the entry system continues

1 to operate during a power outage. An owner, or their agent, shall  
2 routinely inspect the backup power and shall replace according to system  
3 specifications. Owners or their agents shall provide tenants and lawful  
4 occupants with information about whom to contact in the event that the  
5 tenant, lawful occupant or the tenant's or lawful occupant's children,  
6 guests or employees become locked out.

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

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

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

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

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

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

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

48 (vi) Reference data for a user shall be destroyed or anonymized within  
49 ninety days of (1) the tenant or lawful occupant permanently vacating  
50 the dwelling, or (2) a request by the tenant or lawful occupant to with-  
51 draw authorization for those previously authorized by the tenant or  
52 lawful occupant.

53 (b) (i) An entity shall not capture biometric identifier information  
54 of an individual to gain entrance to a multiple dwelling unless the  
55 person is a tenant or lawful occupant or a person authorized by the  
56 tenant or lawful occupant, and informs the individual before capturing

1 the biometric identifier information; and receives their express consent  
2 to capture the biometric identifier information.

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

5 (1) Shall not sell, lease or otherwise disclose the biometric identi-  
6 fier information to another person unless pursuant to any law, grand  
7 jury subpoena or court ordered warrant, subpoena, or other authorized  
8 court ordered process.

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

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

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

25 (i) The procedures shall clearly establish the owner's retention sche-  
26 dule and guidelines for permanently destroying or anonymizing the data  
27 collected.

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

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

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

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

1 or exceed the privacy protections set forth in this section and shall be  
2 subject to the same liability for breach of any of the requirements of  
3 this section.

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

9 6. Storage of information. Any information or data collected shall be  
10 stored in a secure manner to prevent unauthorized access by both employ-  
11 ees and contractors and those unaffiliated with the owner or their  
12 agents, except as otherwise provided in this section. Future or continu-  
13 ing tenancy shall not be conditioned upon consenting to the use of a  
14 smart access system.

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

28 (a) be able to create updates to the firmware to correct the vulner-  
29 abilities;

30 (b) contractually commit to customers that the smart access system or  
31 vendor will create updates to the embedded software or firmware to reme-  
32 dy the vulnerabilities; and

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

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

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

45 (b) Where an owner or their agent uses a smart access system to harass  
46 or otherwise deprive a tenant or lawful occupant of any rights available  
47 under law, such owner or agent shall be subject to a civil penalty of  
48 not more than ten thousand dollars for each violation.

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

51 10. Rent regulated dwellings. Installation of a smart access system  
52 pursuant to this section in a dwelling subject to the emergency tenant  
53 protection act of nineteen hundred seventy-four, the emergency housing  
54 rent control law, the local emergency housing rent control act, or the  
55 rent stabilization law of nineteen hundred sixty-nine shall constitute a  
56 modification of services requiring the owner of such dwelling or their

1 agent to apply to the division of housing and community renewal for  
2 approval before performing such installation. Such installation shall  
3 not qualify as a basis for rent reduction.

4 11. Exemptions. (a) Nothing herein shall apply to multiple dwellings  
5 owned or managed by an entity subject to 42 U.S.C. § 1437 et seq., or  
6 any of its subsidiaries, or multiple dwellings that are primarily occu-  
7 ped by transient occupants for a period of less than thirty days.

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

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

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