

STATE OF NEW YORK

48--B

2023-2024 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 4, 2023

Introduced by M. of A. L. ROSENTHAL, DINOWITZ, GLICK, SIMON, EPSTEIN, McMAHON, COLTON, WEPRIN -- read once and referred to the Committee on Housing -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- reported and referred to the Committee on Codes -- 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:

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
18 or iris scan, (ii) a fingerprint, (iii) a voiceprint, (iv) a scan or
19 record of a palm, hand, or face geometry, (v) gait or movement patterns,

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

LBD00692-06-3

1 or (vi) any other similar identifying characteristic that can be used
2 alone or in combination with each other, or with other information, to
3 establish individual identity.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

42 a. be able to create updates to the firmware to correct the vulner-
43 abilities;

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

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

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

53 9. Penalties. a. A person who violates this section shall be subject
54 to a civil penalty of not more than five thousand dollars for each
55 violation. The attorney general may bring an action to recover the civil
56 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-

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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