

STATE OF NEW YORK

48--D

Cal. No. 3

2023-2024 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 4, 2023

Introduced by M. of A. L. ROSENTHAL, DINOWITZ, GLICK, SIMON, EPSTEIN, McMAHON, COLTON, WEPRIN, TAYLOR, RAGA -- 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 -- ordered to a third reading, amended and ordered reprinted, retaining its place on the order of third reading -- again amended on third reading, ordered reprinted, retaining its place on 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.

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

LBD00692-10-4

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

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

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

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

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

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

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

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

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

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

48 d. All lawful tenants and lawful occupants shall be provided with a
49 key, key fob, digital key or key card at no cost to such tenants and
50 lawful occupants. The term "lawful occupants" shall include children
51 under the age of eighteen who shall be issued a key, key fob, digital
52 key or key card if a parent or guardian requests such child be provided
53 with one. Tenants and lawful occupants may also receive up to four addi-
54 tional keys, key fobs, digital keys or key cards at no cost to the
55 tenant or lawful occupant for employees or guests. The term "guests"
56 shall include family members and friends who can reasonably be expected

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

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

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

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

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

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

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

54 (iii) The owner, agent of the owner, or the vendor of a smart access
55 system on behalf of the owner may record each time a key fob, key card,

1 digital key or passcode is used to enter the building, but shall not
2 record any departures.

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

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

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

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

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

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

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

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

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

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

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

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

55 b. It shall be prohibited to collect through a smart access system the
56 likeness of a minor occupant, information on the relationship status of

1 tenants or lawful occupants and their guests, or to use a smart access
2 system to collect or track information about the frequency and time of
3 use of such system by a tenant or lawful occupant and their guests to
4 harass or evict a tenant or lawful occupant or for any other purpose not
5 expressly related to the operation of the smart access system.

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

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

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

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

47 a. be able to create updates to the firmware to correct the vulner-
48 abilities;

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

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

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

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

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

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

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

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

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

32 § 2. The multiple residence law is amended by adding a new section
33 130-a to read as follows:

34 § 130-a. Electronic or computerized entry systems. 1. Definitions. For
35 the purposes of this section, the following terms shall have the follow-
36 ing meanings:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

47 (c) Information that is acquired via the use of a smart access system
48 shall not be used for any purposes other than granting access to and
49 monitoring building entrances and shall not be used as the basis or
50 support for an action to evict a lessee, tenant, or lawful occupant, or
51 an administrative hearing seeking a change in regulatory coverage for an
52 individual or unit. However, a tenant or lawful occupant may authorize
53 their information to be used by a third party, but such a request shall
54 clearly state who will have access to such information, for what purpose
55 it will be used, and the privacy policies which will protect their
56 information. Under no circumstances shall a lease or a renewal be

1 contingent upon authorizing such use. Smart access systems may use
2 third-party services to the extent required to maintain and operate
3 system infrastructure, including cloud-based hosting and storage. The
4 provider or providers of third-party infrastructure services shall meet
5 or exceed the privacy protections set forth in this section and shall be
6 subject to the same liability for breach of any of the requirements of
7 this section.

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

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

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

32 (a) be able to create updates to the firmware to correct the vulner-
33 abilities;

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

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

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

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

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

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

55 10. Rent regulated dwellings. Installation of a smart access system
56 pursuant to this section in a dwelling subject to the emergency tenant

1 protection act of nineteen hundred seventy-four, the emergency housing
2 rent control law, the local emergency housing rent control act, or the
3 rent stabilization law of nineteen hundred sixty-nine shall constitute a
4 modification of services requiring the owner of such dwelling or their
5 agent to apply to the division of housing and community renewal for
6 approval before performing such installation. Such installation shall
7 not qualify as a basis for rent reduction.

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

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

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

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