

STATE OF NEW YORK

156

2025-2026 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 8, 2025

Introduced by M. of A. ROSENTHAL, DINOWITZ, GLICK, SIMON, EPSTEIN, McMAHON, COLTON, WEPRIN, TAYLOR, RAGA -- read once and referred to the Committee on Housing

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

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

LBD00912-01-5

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

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

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

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

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

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

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

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

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

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

1 or their agent shall provide the first replacement key, key fob, digital
2 key or key card to the tenant or lawful occupant free of charge. The
3 cost of second and subsequent replacement cards shall not be more than
4 what the owner paid for the replacement up to and not exceeding twenty-
5 five dollars.

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

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

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

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

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

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

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

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

54 (v) The owner of the multiple dwelling or any third party shall
55 destroy or anonymize authentication data collected from or generated by

1 such smart access system within a reasonable time, but not later than
2 ninety days after the date collected.

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

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

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

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

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

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

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

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

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

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

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

54 c. Information that is acquired via the use of a smart access system
55 shall not be used for any purposes other than granting access to and
56 monitoring building entrances and shall not be used as the basis or

1 support for an action to evict a lessee, tenant, or lawful occupant, or
2 an administrative hearing seeking a change in regulatory coverage for an
3 individual or unit. However, a tenant or lawful occupant may authorize
4 their information to be used by a third party, but such a request shall
5 clearly state who will have access to such information, for what purpose
6 it will be used, and the privacy policies which will protect their
7 information. Under no circumstances shall a lease or a renewal be
8 contingent upon authorizing such use. Smart access systems may use
9 third-party services to the extent required to maintain and operate
10 system infrastructure, including cloud-based hosting and storage. The
11 provider or providers of third-party infrastructure services shall meet
12 or exceed the privacy protections set forth in this section and shall be
13 subject to the same liability for breach of any of the requirements of
14 this section.

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

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

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

39 a. be able to create updates to the firmware to correct the vulner-
40 abilities;

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

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

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

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

54 b. Where an owner or their agent uses a smart access system to harass
55 or otherwise deprive a tenant or lawful occupant of any rights available

1 under law, such owner or agent shall be subject to a civil penalty of
2 not more than ten thousand dollars for each violation.

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

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

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

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

23 § 2. The multiple residence law is amended by adding a new section
24 130-a to read as follows:

25 § 130-a. Electronic or computerized entry systems. 1. Definitions. For
26 the purposes of this section, the following terms shall have the follow-
27 ing meanings:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1 tenant, lawful occupant or the tenant's or lawful occupant's children,
2 guests or employees become locked out.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

25 (a) be able to create updates to the firmware to correct the vulner-
26 abilities;

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

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

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

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

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

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

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

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

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

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

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