

# STATE OF NEW YORK

2078

2023-2024 Regular Sessions

## IN SENATE

January 18, 2023

Introduced by Sens. KAVANAGH, KRUEGER -- read twice and ordered printed,  
and when printed to be committed to the Committee on Housing,  
Construction and Community Development

AN ACT to amend the multiple dwelling law and the multiple residence  
law, in relation to the use of electronic or computerized entry  
systems and the information that may be gathered from such systems

The People of the State of New York, represented in Senate and Assem-  
bly, 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 an electronic and/or computerized entry system.

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

15 (c) "Critical security vulnerability" means a security vulnerability  
16 that has a significant risk of resulting in an unauthorized access to an  
17 area secured by an electronic and/or computerized entry system.

18 (d) "Reference data" means information against which authentication  
19 data is verified at a point of authentication by a smart access system  
20 in order to grant a user entry to a smart access building or common area  
21 of such building.

22 (e) "Security breach" means any incident that results in unauthorized  
23 access of data, applications, services, networks and/or devices by

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

LBD00692-01-3

1 bypassing underlying security mechanisms. A "security breach" occurs  
2 when an individual or an application illegitimately enters a private,  
3 confidential or unauthorized logical information technology perimeter.

4 2. Entry. a. Where a landlord installs or plans to install an elec-  
5 tronic or computerized entry system on any entrance from the street,  
6 passageway, court, yard, cellar, or other common area of a class A  
7 multiple dwelling, such system shall not rely solely on a web-based  
8 application to facilitate entrance but shall also include a key fob, key  
9 card, digital key or passcode for tenant use.

10 b. Landlords may provide various methods of entry into individual  
11 apartments including a mechanical key or an electronic or computerized  
12 entry system of a key fob, key card or digital key, provided, however  
13 that such electronic or computerized entry system shall not rely solely  
14 on a web-based application.

15 c. Notwithstanding paragraph a or b of this subdivision, landlords  
16 shall provide a non-electronic means of entry where requested by the  
17 tenant due to a religious preference.

18 d. All lawful tenants and occupants shall be provided with a key, key  
19 fob, digital key or key card at no cost to such tenants. The term "occu-  
20 pants" shall include children under the age of eighteen who shall be  
21 issued a key, key fob, digital key or key card if a parent or guardian  
22 requests such child be provided with one. Tenants may also receive up to  
23 four additional keys, key fobs, digital key or key cards at no cost to  
24 the tenant for employees or guests. The term "guests" shall include  
25 family members and friends who can reasonably be expected to visit on a  
26 regular basis or visit as needed to care for the tenant or the apartment  
27 if the tenant is away. Employees, including contractors, professional  
28 caregivers or other services providers, may have an expiration date  
29 placed on their key, key card, digital key or key fob, which may be  
30 extended upon the tenant's or occupant's request. Tenants may request a  
31 new or replacement key, key fob, digital key or key card at any time  
32 throughout the course of the tenancy. The landlord or his or her agent  
33 shall provide the first replacement key, key fob, digital key or key  
34 card to the tenant free of charge. The cost of second and subsequent  
35 replacement cards shall not be more than what the landlord paid for the  
36 replacement up to and not exceeding twenty-five dollars.

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

39 f. Any door that has an electronic or computerized entry system shall  
40 have backup power or an alternative means of entry to ensure that the  
41 entry system continues to operate during a power outage. A landlord, or  
42 his or her agent, shall routinely inspect the backup power and shall  
43 replace according to system specifications. Owners or their agents  
44 shall provide lawful tenants and occupants with information about whom  
45 to contact in the event that the tenant, occupant or the tenant's or  
46 occupant's children, guests or employees become locked out.

47 3. Notice. Landlords or their agents shall provide notice to a tenant  
48 at the time the tenant signs the lease, or when the electronic or  
49 computerized entry system is installed, of the provisions of subdivision  
50 two of this section.

51 4. Data collection. a. If an electronic and/or computerized entry  
52 system is utilized to gain entrance to a class A multiple dwelling, the  
53 only reference, authentication, and account information gathered by any  
54 electronic and/or computerized entry system shall be limited to account  
55 information used to grant a user entry or to access any online tools  
56 used to manage user accounts related to the electronic and/or computer-

1 ized entry system, or reference data, such as the lessee or tenant's  
2 name, apartment number, the preferred method of contact for such lessee  
3 or tenant, other doors or common areas to which the user has access,  
4 move-in and, if available move-out dates, and authentication data such  
5 as time and method of access for security purposes and a photograph of  
6 access events for security purposes. For electronic and computerized  
7 entry systems that rely on the collection of biometric data and which  
8 have already been installed at the time this section shall have become a  
9 law, a biometric identifier may be collected pursuant to this section in  
10 order to register a lessee or tenant for an electronic and/or computer-  
11 ized entry system. No new electronic and/or computerized entry systems  
12 that rely on the collection of biometric data shall be installed in  
13 class A multiple dwellings for three years after the effective date of  
14 this section.

15 (i) The owner of the multiple dwelling may collect only the minimum  
16 data required by the technology used in the electronic and/or computer-  
17 ized entry system to effectuate such entrance and protect the privacy  
18 and security of such tenants.

19 (ii) The owner or agent of the owner shall not request or retain, in  
20 any form, the social security number of any tenant or occupant as a  
21 condition of use of the electronic or computerized entry system.

22 (iii) The owner, agent of the owner, or the vendor of an electronic or  
23 computerized entry system on behalf of the owner may record each time a  
24 key fob, key card, digital key or passcode is used to enter the build-  
25 ing, but shall not record any departures.

26 (iv) A copy of such data may be retained for reference at the point of  
27 authentication by the electronic and/or computerized entry system. Such  
28 reference data may be retained only for tenants or those authorized by  
29 the tenant or owner of the multiple dwelling.

30 (v) The owner of the multiple dwelling shall destroy or anonymize  
31 authentication data within a reasonable time, but not later than ninety  
32 days after the date collected.

33 (vi) Reference data for a tenant or those authorized by a tenant shall  
34 be destroyed or anonymized within ninety days of (1) the tenant perma-  
35 nently vacating the dwelling, or (2) a request by the tenant to withdraw  
36 authorization for those previously authorized by the tenant.

37 b. (i) For the purposes of this section, "biometric identifier" means  
38 a retina or iris scan, fingerprint, voiceprint, or record of hand, face  
39 geometry or other similar feature.

40 (ii) An entity may not capture a biometric identifier of an individual  
41 to gain entrance to a class A multiple dwelling unless the person is a  
42 tenant or person authorized by the tenant, and informs the individual  
43 before capturing the biometric identifier; and receives their express  
44 consent to capture the biometric identifier.

45 (iii) Any entity that possesses a biometric identifier of an individ-  
46 ual that is captured to gain entrance to a class A multiple dwelling:

47 (1) May not sell, lease or otherwise disclose the biometric identifier  
48 to another person unless pursuant to a grand jury subpoena or court  
49 ordered warrant, subpoena, or other authorized court ordered process.

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

54 (3) Shall destroy the biometric identifier within a reasonable time,  
55 but not later than forty-eight hours after the date collected, except  
56 for reference data. If any prohibited information is collected, such as

1 the likeness of a minor or a non-tenant, the information shall be  
2 destroyed immediately.

3 c. The owner of the multiple dwelling, or the managing agent, must  
4 develop written procedures which describe the process used to add  
5 persons authorized by the tenant to electronic and/or computerized entry  
6 systems on a temporary or permanent basis, such as visitors, children,  
7 their employees, and caregivers to such building.

8 (i) The procedures must clearly establish the owner's retention sched-  
9 ule and guidelines for permanently destroying or anonymizing the data  
10 collected.

11 (ii) The procedures cannot limit time or place of entrance by such  
12 people authorized by the tenant except as requested by the tenant.

13 5. Prohibitions. a. No form of location tracking, including but not  
14 limited to satellite location based services, shall be included in any  
15 equipment, key, or software provided to tenants or guests as part of an  
16 electronic and/or computerized entry system.

17 b. It shall be prohibited to collect through an electronic and/or  
18 computerized entry system the likeness of a minor occupant, information  
19 on the relationship status of tenants, lessees and/or guests, or to use  
20 a smart access system to collect or track information about the frequen-  
21 cy and time of use of such system by a tenant and/or guests to harass or  
22 evict a tenant or for any other purpose not expressly related to the  
23 operation of the smart access system.

24 c. Information that is acquired via the use of an electronic and/or  
25 computerized entry system shall not be used for any purposes other than  
26 monitoring building entrances and shall not be used as the basis or  
27 support for an action to evict a lessee or tenant, or an administrative  
28 hearing seeking a change in regulatory coverage for an individual or  
29 unit. However, a tenant may authorize their information to be used by a  
30 third party, but such a request must clearly state who will have access  
31 to such information, for what purpose it will be used, and the privacy  
32 policies which will protect their information. Under no circumstances  
33 may a lease or a renewal be contingent upon authorizing such use. Elec-  
34 tronic and/or computerized systems may use third-party services to the  
35 extent required to maintain and operate system infrastructure, including  
36 cloud-based hosting and storage. The provider or providers of third-par-  
37 ty infrastructure services must meet or exceed the privacy protections  
38 set forth in this section and will be subject to the same liability for  
39 breach of any of the requirements of this section.

40 d. Information and data collected shall not be made available to any  
41 third party, unless authorized as described above, including but not  
42 limited to law enforcement, except upon a grand jury subpoena or a court  
43 ordered warrant, subpoena, or other authorized court ordered process.

44 6. Storage of information. Any information or data collected shall be  
45 stored in a secure manner to prevent unauthorized access by both employ-  
46 ees and contractors and those unaffiliated with the landlord or their  
47 agents, except as otherwise provided in this section. Future or continu-  
48 ing tenancy shall not be conditioned upon consenting to the use of an  
49 electronic and/or computerized entry system.

50 7. Software issues. Whenever a company that produces, makes available  
51 or installs electronic or computerized entry systems discovers a securi-  
52 ty breach or critical security vulnerability in their software, such  
53 company shall notify customers of such vulnerability within a reasonable  
54 time of discovery but no later than twenty-four hours after discovery  
55 and shall make software updates available and take any other action as  
56 may be necessary to repair the vulnerability within a reasonable time,

1 but not longer than thirty days after discovery. Smart access systems  
2 and vendors shall implement and maintain reasonable security procedures  
3 and practices appropriate to the nature of the information collected. In  
4 the event that a security breach or critical security vulnerability that  
5 pertains to the embedded software or firmware on the smart access  
6 systems is discovered, smart access systems and their vendors shall:

7 a. be able to create updates to the firmware to correct the vulner-  
8 abilities;

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

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

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

18 9. Penalties. (a) A person who violates this section is subject to a  
19 civil penalty of not more than five thousand dollars for each violation.  
20 The attorney general may bring an action to recover the civil penalty.  
21 An individual injured by a violation of this section may bring an action  
22 to recover damages. A court may also award attorneys' fees to a prevail-  
23 ing plaintiff.

24 (b) Where a landlord or his or her agent uses an electronic or comput-  
25 erized entry system to harass or otherwise deprive a tenant of any  
26 rights available under law, such landlord or agent shall be subject to a  
27 civil penalty of ten thousand dollars for each violation.

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

30 10. Rent regulated dwellings. Installation of an electronic or comput-  
31 erized entry system pursuant to this section in a rent regulated dwell-  
32 ing shall constitute a modification of services requiring the landlord  
33 of such dwelling or his or her agent to apply to the division of housing  
34 and community renewal for approval before performing such installation.  
35 Such installation shall not qualify as a basis for rent reduction.

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

39 b. Nothing in this section shall limit the authority of the division  
40 of housing and community renewal to impose additional requirements  
41 regarding electronic or computerized entry systems installed in multiple  
42 dwellings for which the division is required to approve substitutions or  
43 modifications of services.

44 § 2. The multiple residence law is amended by adding a new section  
45 130-a to read as follows:

46 § 130-a. Electronic or computerized entry systems. 1. Definitions. For  
47 the purposes of this section, the following terms shall have the follow-  
48 ing meanings:

49 (a) "Account information" means information that is used to grant a  
50 user entry or access to any online tools that are used to manage user  
51 accounts related to an electronic and/or computerized entry system.

52 (b) "Authentication data" means data generated or collected at a point  
53 of authentication in connection with granting a user entry to a class A  
54 multiple dwelling or common area with an electronic or computerized  
55 entry system, except that "authentication data" shall not include data



1 generated through or collected by a video or camera system that is used  
2 to monitor entrances but not to grant entry.

3 (c) "Critical security vulnerability" means a security vulnerability  
4 that has a significant risk of resulting in an unauthorized access to an  
5 area secured by an electronic and/or computerized entry system.

6 (d) "Reference data" means information against which authentication  
7 data is verified at a point of authentication by a smart access system  
8 in order to grant a user entry to a smart access building or common area  
9 of such building.

10 (e) "Security breach" means any incident that results in unauthorized  
11 access of data, applications, services, networks and/or devices by  
12 bypassing underlying security mechanisms. A "security breach" occurs  
13 when an individual or an application illegitimately enters a private,  
14 confidential or unauthorized logical information technology perimeter.

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

21 (b) Landlords may provide various methods of entry into individual  
22 apartments including a mechanical key or an electronic or computerized  
23 entry system of a key fob, key card or digital key, provided, however  
24 that such electronic or computerized entry system shall not rely solely  
25 on a web-based application.

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

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

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

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

1 contact in the event that the tenant, occupant or the tenant's or occu-  
2 pant's children, guests or employees become locked out.

3 3. Notice. Landlords or their agents shall provide notice to a tenant  
4 at the time the tenant signs the lease, or when the electronic or  
5 computerized entry system is installed, of the provisions of subdivision  
6 two of this section.

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

27 (i) The owner of the multiple dwelling may collect only the minimum  
28 data required by the technology used in the electronic and/or computer-  
29 ized entry system to effectuate such entrance and protect the privacy  
30 and security of such tenants.

31 (ii) The owner or agent of the owner shall not request or retain, in  
32 any form, the social security number of any tenant or occupant as a  
33 condition of use of the electronic or computerized entry system.

34 (iii) The owner, agent of the owner, or the vendor of an electronic or  
35 computerized entry system on behalf of the owner may record each time a  
36 key fob, key card, digital key or passcode is used to enter the build-  
37 ing, but shall not record any departures.

38 (iv) A copy of such data may be retained for reference at the point of  
39 authentication by the electronic and/or computerized entry system. Such  
40 reference data may be retained only for tenants or those authorized by  
41 the tenant or owner of the multiple dwelling.

42 (v) The owner of the multiple dwelling shall destroy or anonymize  
43 authentication data within a reasonable time, but not later than ninety  
44 days after the date collected.

45 (vi) Reference data for a tenant or those authorized by a tenant shall  
46 be destroyed or anonymized within ninety days of (1) the tenant perma-  
47 nently vacating the dwelling, or (2) a request by the tenant to withdraw  
48 authorization for those previously authorized by the tenant.

49 (b) (i) For the purposes of this section, "biometric identifier" means  
50 a retina or iris scan, fingerprint, voiceprint, or record of hand, face  
51 geometry or other similar feature.

52 (ii) An entity may not capture a biometric identifier of an individual  
53 to gain entrance to a class A multiple dwelling unless the person is a  
54 tenant or person authorized by the tenant, and informs the individual  
55 before capturing the biometric identifier; and receives their express  
56 consent to capture the biometric identifier.

1 (iii) Any entity that possesses a biometric identifier of an individ-  
2 ual that is captured to gain entrance to a class A multiple dwelling:

3 (1) May not sell, lease or otherwise disclose the biometric identifier  
4 to another person unless pursuant to a grand jury subpoena or court  
5 ordered warrant, subpoena, or other authorized court ordered process.

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

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

15 (c) The owner of the multiple dwelling, or the managing agent, must  
16 develop written procedures which describe the process used to add  
17 persons authorized by the tenant to electronic and/or computerized entry  
18 systems on a temporary or permanent basis, such as visitors, children,  
19 their employees, and caregivers to such building.

20 (i) The procedures must clearly establish the owner's retention sched-  
21 ule and guidelines for permanently destroying or anonymizing the data  
22 collected.

23 (ii) The procedures cannot limit time or place of entrance by such  
24 people authorized by the tenant except as requested by the tenant.

25 5. Prohibitions. (a) No form of location tracking, including but not  
26 limited to satellite location based services, shall be included in any  
27 equipment, key, or software provided to tenants or guests as part of an  
28 electronic and/or computerized entry system.

29 (b) It shall be prohibited to collect through an electronic and/or  
30 computerized entry system the likeness of a minor occupant, information  
31 on the relationship status of tenants, lessees and/or guests, or to use  
32 a smart access system to collect or track information about the frequen-  
33 cy and time of use of such system by a tenant and/or guests to harass or  
34 evict a tenant or for any other purpose not expressly related to the  
35 operation of the smart access system.

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

52 (d) Information and data collected shall not be made available to any  
53 third party, unless authorized as described above, including but not  
54 limited to law enforcement, except upon a grand jury subpoena or a court  
55 ordered warrant, subpoena, or other authorized court ordered process.



1 6. Storage of information. Any information or data collected shall be  
2 stored in a secure manner to prevent unauthorized access by both employ-  
3 ees and contractors and those unaffiliated with the landlord or their  
4 agents, except as otherwise provided in this section. Future or continu-  
5 ing tenancy shall not be conditioned upon consenting to the use of an  
6 electronic and/or computerized entry system.

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

20 (a) be able to create updates to the firmware to correct the vulner-  
21 abilities;

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

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

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

31 9. Penalties. (a) A person who violates this section is subject to a  
32 civil penalty of not more than five thousand dollars for each violation.  
33 The attorney general may bring an action to recover the civil penalty.  
34 An individual injured by a violation of this section may bring an action  
35 to recover damages. A court may also award attorneys' fees to a prevail-  
36 ing plaintiff.

37 (b) Where a landlord or his or her agent uses an electronic or comput-  
38 erized entry system to harass or otherwise deprive a tenant of any  
39 rights available under law, such landlord or agent shall be subject to a  
40 civil penalty of ten thousand dollars for each violation.

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

43 10. Rent regulated dwellings. Installation of an electronic or comput-  
44 erized entry system pursuant to this section in a rent regulated dwell-  
45 ing shall constitute a modification of services requiring the landlord  
46 of such dwelling or his or her agent to apply to the division of housing  
47 and community renewal for approval before performing such installation.  
48 Such installation shall not qualify as a basis for rent reduction.

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

52 (b) Nothing in this section shall limit the authority of the division  
53 of housing and community renewal to impose additional requirements  
54 regarding electronic or computerized entry systems installed in multiple  
55 dwellings for which the division is required to approve substitutions or  
56 modifications of services.

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

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