

STATE OF NEW YORK

706--B

2021-2022 Regular Sessions

IN ASSEMBLY

(Prefiled)

January 6, 2021

Introduced by M. of A. L. ROSENTHAL, DINOWITZ, EPSTEIN, SIMON, GLICK, GALEF, J. RIVERA, McMAHON, GOTTFRIED, FRONTUS, ABINANTI, COLTON, WEPRIN -- read once and referred to the Committee on Housing -- committee discharged, bill amended, ordered reprinted as amended and recommitted to said committee -- again reported from said committee with amendments, ordered reprinted as amended and recommitted to said committee

AN ACT to amend the multiple dwelling 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 Assembly, do enact as follows:

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

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

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

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

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

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

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

LBD00549-04-1

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

55 (3) Shall destroy the biometric identifier within a reasonable time,
56 but not later than forty-eight hours after the date collected, except

1 for reference data. If any prohibited information is collected, such as
2 the likeness of a minor or a non-tenant, the information shall be
3 destroyed immediately.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

45 § 2. Severability. If any provision of this act, or any application of
46 any provision of this act, is held to be invalid, that shall not affect
47 the validity or effectiveness of any other provision of this act, or of
48 any other application of any provision of this act, which can be given
49 effect without that provision or application; and to that end, the
50 provisions and applications of this act are severable.

51 § 3. This act shall take effect on the one hundred eightieth day after
52 it shall have become a law.