Published on *The National Law Review* https://natlawreview.com

New York City Enacts Tenant Data Privacy Act

Article By:

John L. Mascialino

Stephen L. Rabinowitz

David A. Zetoony

Daniel Friedman

Ellen M. Gustafson

On May 28, 2021, New York City enacted privacy legislation that specifically targets owners of multifamily dwellings. The Tenant Data Privacy Act (TDPA) addresses perceived privacy issues surrounding the use of smart access systems in multi-family dwellings and is modeled, in part, after broader European and California privacy legislation. Among other things, it requires that all owners of Class A multiple dwellings that use smart-access systems (e.g., key cards, phone access, fingerprint) take the following steps:

- Provide tenants with a privacy notice.
- Obtain consent for the use of smart access systems.
- Establish data retention periods for collected data.
- Ensure that collected data is not sold or shared.
- Create parameters surrounding the tracking of tenants.
- Protect data that they collect.

The law goes into effect in 60 days, but multifamily residential landlords in New York City who own existing smart access buildings have been given an 18-month grace period, until Jan. 1, 2023, to come into compliance with the new requirements. Should a smart access building go online for the first time in, for example, August 2021 (after the law takes effect but before the grace period for existing smart access buildings ends), the statute will apply immediately.

The TDPA is one of the first statutes nationwide to regulate the collection and retention of data from residential multifamily “smart access” buildings. While some residential landlords in other jurisdictions, such as California, have been impacted by broad privacy legislation like the California Consumer Privacy Act, the TDPA is one of the first attempts by any jurisdiction to specifically mandate that residential landlords take steps to protect tenant privacy. As a result, it is likely to have an impact on both commercial and residential landlords, as well as landlords outside of New York City, that are concerned about best practices or similar legislation being enacted in other jurisdictions.

Key Provisions of the Bill

Scope

- The TDPA only applies to Class A multifamily dwellings in New York City.
- The TDPA applies to buildings with “smart access systems,” which include “any system that uses electronic or computerized technology, a radio frequency identification card, a mobile phone application, biometric identifier information, or any other digital technology in order to grant entry,” including the ubiquitous key fobs.
- The bill applies not only to building entry but to any restricted space using the smart access system, such as gyms, laundry rooms, mail rooms and lounges.
- The bill applies to both reference data and authentication data. Reference data is the data against which authentication data is checked to confirm the identity of the tenant.
- The TDPA does not apply to data gathered through a video system that is not used to grant entry.
- Under the TDPA, landlords cannot collect information on a tenant’s use of gas, electricity, or other utilities beyond the tenant’s monthly usage, unless otherwise required to by law.
- Landlords may not collect any information about a tenant’s internet usage except when internet is provided directly from a landlord to tenant (such as in common areas of a building).

Privacy Policy

- Landlords must provide a “plain language” privacy policy that includes, at minimum:

– the data elements to be collected;

– the names of any entities or third parties the owner will share such data elements with, and the privacy policies of any such entities or third parties;

– the protocols and safeguards the owner will provide for protecting such data elements;

– the owner’s data retention schedule;

– the protocols the owner will follow to address any suspected or actual unauthorized access to or

disclosure of such data elements;

– guidelines for destruction or anonymization; and

– the process used to add and remove persons who have provided written consent on a temporary basis to the smart access system.

Data Collection

- The TDPA requires express consent for a building's owner to collect reference data from tenants.

- Landlords may only collect the following information as part of a smart access system (and only to the extent the information is necessary for the operation of the system):

– the tenant's name;

– apartment number and other amenities to which that tenant has access;

– preferred method of contact;

– biometric information, but only if the smart access system works on biometric data;

– identification numbers or passcodes used to gain entry;

– lease information; and

– time and method of building access; however, such information may only be used for security purposes.

Data Restrictions

- The TDPA generally prohibits landlords from:

– using data collected through a smart access system for any purpose other than to grant or monitor access;

– using a smart access system to limit the time of entry for any user, unless requested by a tenant;

– requiring a tenant to use a smart access system to access their apartment; or

– using any information gained through a smart access system to harass or evict a tenant.

- Landlords may not sell, lease, or disclose reference or authentication data, except:

– pursuant to a law, subpoena, or court order;

– to a disclosed third party that facilitates the operation of a smart access system, where the tenant has given express, informed consent in writing or through a mobile application;

– for utility data, to an entity employed or retained to improve the energy efficiency of the building; or

– to a guest of the tenant, as authorized by the tenant.

- Landlords may not track tenants or other users of smart access systems outside of the apartment building.
- Landlords also may not track minors, unless authorized by the minor's guardian, or use smart access systems to monitor the relationship status of a tenant.

Data Safeguards

- Smart access systems must implement "stringent security measures and safeguards to protect the security and data of tenants, guests, and other individuals in smart access buildings," including, at a minimum, data encryption, the ability of a user to change their password (if passwords are used), and firmware that is regularly updated to remediate security vulnerabilities.

Data Retention and Destruction

- Landlords must destroy or anonymize authentication data collected from or generated by smart access systems within 90 days after collection or generation.
- Reference data must be destroyed or anonymized within 90 days after a tenant permanently vacates the apartment building or withdraws their consent.
- The same timeframe for destruction of data applies to users of the apartment building.
- Data collected without consent must be destroyed immediately.
- Landlords do not need to destroy data that is necessary to protect against security incidents or is needed to debug the smart access system.

Private Right of Action

- The TDPA allows a "lawful occupant of a dwelling unit," either individually or in a class, to sue if a landlord violates the TDPA by selling information.
- Successful litigants can seek compensatory and punitive damages or statutory damages ranging from $200 to $1,000, plus attorney's fees.
- The private right of action does not replace other common law rights a tenant may have or relieve a tenant of their duty to pay rent.

Landlords should use the grace period to ensure they are in compliance with the TDPA before Jan. 1, 2023, and work with experienced counsel to draft or update privacy notices, review consents, or confirm that contracts with smart access system providers sufficiently protect owners of multifamily buildings.

National Law Review, Volumess XI, Number 148