HINSHAW

Privacy Law Essentials: New York City's Tenant Data Privacy Act

Privacy, Cyber & AI Decoded Alert | 5 min read
Jul 16, 2021

Hinshaw summer associate Jenny Li contributed to the research and drafting of this alert.

The New York City Tenant Data Privacy Act (TDPA) was passed on May 28, 2021. Scheduled to go into effect on July 29, 2021, the law addresses a number of perceived privacy-related issues concerning smart access systems in multifamily buildings.

To whom does it apply?

The law will affect three groups of people: owners of smart access buildings, tenants of smart access buildings and their guests, and third-party entities that install or operate the smart access system for such buildings. A smart access building is any Class A multifamily building—or any multifamily building occupied for permanent residence purposes—that uses a smart access system. A smart access system is any system that uses digital technology such as key cards, fobs, phones, and fingerprints to grant entry to the building, its common areas, or an individual unit in the building.

What types of information does it cover?

The law applies to authentication data and reference data. Authentication data is data generated or collected to grant entry into a smart access building. Such data excludes any data generated or collected by a video or camera system that monitors entrances but does not grant entry. Reference data is data against which authentication data is checked for identity verification.

What does the law require and prohibit?

Data Collection

Building owners and third-party entities must obtain express consent from tenants and their guests before collecting their data. Even after obtaining express consent, building owners and third-party entities are limited to collecting or using the following information:

- The name of the tenant or guest;
- The unit number and areas in the building that the tenant or guest has access to with the smart access system;
- The tenant or guest's preferred method of contact;
- The tenant or guest's biometric identifier information—if the smart access system uses any physiological, biological, or behavioral characteristics to identify an individual;
- Passcodes or identifiers associated with the physical hardware used to gain entry;
- Lease information, including move-in and move-out dates; and
- The time and method of entry, to be used for security purposes only.

Prohibitions

Building owners and third-party entities are prohibited from:

- Collecting any information about a tenant's use of internet service, unless the building owner provides internet service directly to the tenant and the information is aggregated and anonymized or necessary for billing purposes;
- Selling, leasing, or disclosing the data to another person, with some exceptions;
- Using a smart access system to track the location of any tenant or guest when they are outside the building;
- Using a smart access system to capture data of any minor, unless the minor's parent or legal guardian has given written authorization;
- Using a smart access system to deliberately collect information on or track the relationship status of tenants and their guests, unless required by law;
- Using a smart access system to collect information on or track the frequency and time that tenants and their guests use the system to harass or evict the tenant;
- Using a smart access system to collect data from an individual who is not a tenant and who has not given express consent, in writing or through a mobile application, except if the individual is an employee or agent of the building owner; and
- Sharing any data about a minor collected from a smart access system unless the minor's parent or legal guardian has given written authorization.

Furthermore, building owners are prohibited from:

- Using data collected through a smart access system for any purpose other than granting entry;

- Using a smart access system to limit the time that any tenant or guest can enter the building unless requested by a tenant;
- Requiring a tenant to use a smart access system for entry; and
- Using any information collected through a smart access system to harass or evict a tenant.

What obligations will it impose?

Data Destruction and Retention

If building owners or third-party entities violate the prohibition on collecting unauthorized data about an individual, deliberately collecting information on the relationship status of their tenants and guests, or tracking the frequency that tenants or guests use the smart access system, the building owner or third-party entity must immediately destroy the data.

Building owners and third-party entities must also destroy data collected or generated by a smart access system with 90 days of collection or generation unless the data is anonymized.

Additionally, unless removing the tenant or guest's data makes the smart access system inoperable, their data must be removed within 90 days of the following events:

- Tenant permanently vacates the smart access building;
- Guests of tenants who permanently vacate the smart access building who are not also tenants of the smart access building;
- Tenant or guest withdraws consent previously given to collect their data; and
- Tenant withdraws request to grant a guest access to the smart access system.

However, if removing the data makes the smart access system inoperable, the tenant or guest's data must be anonymized.

Nevertheless, building owners and third-party entities can retain data beyond the 90-day time frame where:

- Data is necessary to detect and protect against security incidents and prosecute those responsible;
- Data is necessary to debug and repair errors that impair existing functionality;
- Data is necessary to comply with another law;
- Data is protected speech under the United States or New York State constitutions;
- Tenant or guest request, in writing or through a mobile application, that their data be retained; or
- Building owners or third-party entity needs the identifiers associated with the physical hardware used to gain entry to deactivate or activate the hardware, given that such data is retained separately from the smart access system.

Data Safeguards

To protect the security of individuals' data, the law requires stringent security measures and safeguards be implemented. At a minimum, security measures must include data encryption, regularly updated firmware, and the ability for the user to change the password if the smart access system uses a password.

Privacy Policy

Building owners must provide a written privacy policy to tenants. The policy must use plain language and include the following information:

- The data elements the smart access system will collect;
- The names and privacy policies of any entities that the owner will share the data elements with;
- The protocols and safeguards that the owner will use to protect the data elements;
- How long the data will be retained;
- The protocols the owner will follow for any suspected or actual unauthorized access to or disclosure of the data elements;
- The guidelines for permanently destroying or anonymizing the data or removing the data from the smart access system; and
- The process used to add and remove individuals who have provided temporary, written consent to the smart access system.

Furthermore, building owners must provide to tenants the written privacy policy of the entity who developed the smart access system or who currently operates the smart access system.

What remedies will the law provide?

Tenants can sue building owners or thirty-party entities for violating the prohibition against the sale of data to another person. Each tenant can recover damages of $200 to $1,000 for each unlawful sale of data, along with attorneys' fees and court costs.

When does it go into effect?

The TDPA will go into effect on July 29, 2021. Owners of existing smart access buildings have until January 1, 2023, to comply with the law. Owners of smart access buildings that are new or go online after the law takes effect must comply immediately.

Related Capabilities

Data Privacy, AI & Cybersecurity