Updates
July 09, 2021
The City That Never Peeps? NY City’s Biometric Identifier Information Ordinance Goes Into Effect July 9, 2021

The nation's latest biometric privacy law will go into effect in New York City this week.

What Is the Ordinance?

New York City's new biometrics ordinance goes into effect today, Friday, July 9. The ordinance regulates the use of "biometric identifier information" in "commercial establishments." It is the first law of its kind in the State of New York.

- "Biometric identifier information" is broadly defined to mean "a physiological or biological characteristic," used "by or on behalf of" a "commercial establishment," to "identify, or assist in identifying, an individual." It includes, "without limitation," retina or iris scans, fingerprints or voiceprints, hand or face geometry scans, and any other identifying characteristic.
- "Commercial establishment" is broadly defined to include any place of entertainment, retail store, or food and drink establishment.
- A place of entertainment is "any privately or publicly owned and operated entertainment facility" and includes theaters, stadiums, arenas, racetracks, museums, amusement parks, observatories, and other venues where performances, concerts, exhibits, games, or contests are held. This definition is broad, and may sweep in venues as large as Madison Square Garden, and as small as an arthouse theater.
- Retail stores include any establishment where "consumer commodities are sold, displayed or offered for sale." The law will therefore apply to retailers as large as commercial grocery, clothing, or home goods chains and as small as corner bodegas and gas stations.
- Food and drink establishments include establishments of any kind that sell food or beverages, such as restaurants that serve food "on premises" as well as "pushcart[s], stand[s], or vehicle[s]." This definition captures the corner hot dog stands, neighborhood ice cream trucks, and popular artisanal food trucks parked up and down the midtown cross streets.

Why Does the Ordinance Matter?

Over the last several years, retailers, restaurants, and many other kinds of companies have increasingly used biometrics-based systems to control customer access, monitor for shoplifting, and learn more about how customers behave in their establishments. Fingerprint- and handprint-based entry to gyms, amusement parks, and entertainment and sports venues, as well as facial recognition systems at stores, are increasingly commonplace. The rapid advancement of this technology and the increasingly small size and popularity of recording devices and similar tools make such use more likely in the future. The New York City ordinance is likely to have an impact on those and other increasingly popular uses of biometric technology.

The broad definition of "commercial establishment" means that retailers, restaurants, and entertainment venues that use cameras to photograph or video consumers and then use software or other tools to analyze the captured individuals' features to specifically identify them appear to be subject to this ordinance.

What Does the Ordinance Require?

If you operate a "commercial establishment" that collects "biometric identifier information" in New York City, then you must comply with the new ordinance. Generally, the ordinance requires covered entities to:

- Disclose the collection, retention, sharing, and use of biometric identifier information to consumers by placing clear and conspicuous signage near all customer entrances and exits.
- Make sure that the required signage is written in plain, simple language. New York City's Commissioner of Consumer and Worker Protection may issue specific language or other guidance regarding the signage. Any such guidance, once published, will likely be posted here.
- Refrain from selling, leasing, trading, sharing in exchange for value, or "otherwise profit[ing]" from biometric identifier information. It is not clear what "otherwise profit" means in this context. Other privacy regulations, such as Illinois' Biometric Information Protection Act (BIPA) and the California Consumer Privacy Act (CCPA), have generated significant litigation and debate, particularly regarding the meaning of "sale" of data. Interpreting the language here will depend on the text and history of the statute at issue. Many have argued that "sale" or "profit" from data should mean some transfer of the data for value. Others have tried to argue that its scope should be broader and include the sale for profit of the devices that collect the data. The issue is not yet settled.

Are There Exceptions to the Ordinance?

Yes. The ordinance includes a number of important exceptions and exclusions. For example:

- Government agencies, government employees, and government agents are excluded from the ordinance.
- Financial institutions are also excluded. This means banks; savings and loan associations; credit unions; branches of foreign banks; public pension and retirement funds and systems; and securities brokers, dealers, and firms are all excluded from the ordinance. This exclusion does not include establishments that primarily sell goods and services and also issue credit cards or in-store financing. For example, a furniture chain that offers financing or a store credit card is not going to enjoy the financial institution exemption and will need to follow the requirements set out below if it uses biometrics to identify consumers.
- The ordinance expressly exempts video and photographic images if they are (1) not run through or analyzed by software or applications that identify or assist in identifying individuals based on physiological or biological characteristics; and (2) not shared, sold, or leased to third parties other than law enforcement agencies. This should mean that where a commercial establishment utilizes closed circuit television systems (CCTV) to monitor for shoplifting or consumer ingress and egress, but does not employ any identification tools or software on the images and does not sell or share the images with third parties other than law enforcement, that conduct is not regulated under the ordinance.
- Because the ordinance only covers the collection of biometric identifier information from customers, it does not extend to biometric time clocks and other collection of employee biometrics by employers.

Are There Penalties for Noncompliance?

Yes. The ordinance includes a private right of action, which means that individual consumers can sue for violations. More specifically, any consumer who is "aggrieved" by an alleged violation of the ordinance can file an action in a court of competent jurisdiction. The meaning of "aggrieved by" is not defined. (The ordinance does not explicitly state whether a New York City agency can bring its own action against a violating commercial establishment, but it states that the commissioner of Consumer and Worker Protection will issue rules pertaining to the ordinance and also instructs the city's chief privacy officer to facilitate outreach and education concerning the ordinance, in connection with any other "relevant agency.")

Damages range from $500 per "negligent violation" to $5,000 per "reckless violation." What constitutes a "violation" is not defined.

Prevailing plaintiffs may also recover reasonable attorneys' fees and costs, along with other relief that the court deems appropriate.

Importantly, the new ordinance also includes a "notice-and-cure" provision. Under that provision, a potential plaintiff may not file a lawsuit based on the alleged failure to post clear signage unless the plaintiff first provides the offending commercial establishment with written notice. After receiving the written notice, the establishment has 30 days to cure any defect or violation under the ordinance. This 30-day notice-and-cure period may take some of the sting out of the ordinance's private right of action for companies that are attempting compliance with the ordinance or are quick to respond to consumer complaints. No presuit notice is required for alleged violations of the prohibition on the sale, lease, trade, or sharing of the biometric identifier information for value.

What Should New York City Companies Do Now?

All companies that use facial recognition and other biometric identification tools and technology, and that have locations and establishments in New York City, should consult with experienced counsel to determine whether this ordinance applies to their businesses. If the ordinance applies, businesses can explore with counsel what changes to their practices, internal and external privacy policies, and consumer notices should be made to comply with the law's requirements.

Perkins Coie's experienced team of biometric law attorneys have deep experience advising clients on facial recognition technologies and litigating cases relating to biometric data and biometric privacy. Perkins Coie's lawyers also have experience advising clients on New York-specific privacy statutes and regulations, including the Stop Hacks and Improve Electronic Data Security (SHIELD) Act, which went into effect one year ago this month. For further information, do not hesitate to reach out to biometrics@perkinscoie.com or contact one of the authors.

Authors

Explore more in

Litigation Privacy & Security Retail & Consumer Products

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law