TECHNOLOGY ON YOUR RADAR? BE CAREFUL.

by Justin Klein

Question: Can private businesses use facial recognition technology for commercial purposes – for example, to capture customer demographic information?

Answer: Yes, depending on the location of the business, a private business can use facial recognition technology for commercial purposes. In doing so, a business may be required to obtain consent and follow other rules while collecting, using and/or sharing information gained from the utilization of facial recognition technology.

Currently, there are no federal laws that apply to facial recognition technology (FRT). While there has been federal legislation introduced that would impact FRT (i.e., Facial Recognition Act of 2022 and The Facial Recognition and Biometric Technology Moratorium Act of 2023), commercial use of FRT is regulated by a patchwork of state and local laws. Most state and local laws concerning FRT focus its application in government settings, where the government is collecting FRT and other biometric data to use in the investigation and prosecution of criminal matters.

There are a few states and local municipalities that do have laws surrounding commercial use of FRT. So far, every law requires operators to gain subjects' consent before collecting their biometric data. Some legislation requires consent to be opt-in (usually referred to as "affirmative," "written" or "unambiguous" consent), as well as freely given, specific and informed. Others do not specify what is meant by consent.

One approach that indirectly regulates commercial FRT use is to regulate the collection and use of biometric data. Illinois' Biometric Information Privacy Act (BIPA) provides that private entities seeking to use consumers' biometric information, including facial recognition, must first notify them of the collection. Disclosure of collected biometric data is prohibited without consent, and entities cannot profit from the data. By affording consumers a private right of action, BIPA allows them to hold companies like Clearview AI and Facebook accountable.

Both Texas and Washington have biometric privacy laws with similar requirements to BIPA, but consumers in these states are not entitled to a private right of action. Laws like BIPA have various requirements for businesses to be compliant such as providing notices related to the type of biometric data, specific purpose of the collection and time period of collection and storage of the data. Businesses may also be required to: have a written retention and destruction policy for biometric information; include restrictions on obtaining biometric information; prohibit profiteering from biometric information; restrict sharing of biometric information (which can impact the franchisor/franchisee relationship); and maintain a security program to ensure the safe collection and storage of biometric identifier data.

In 2009, Texas passed the "Capture or Use of Biometric Identifier Act," or CUBI. CUBI imposes a penalty of "not more than" $25,000 for each violation. However, unlike Illinois, there is no private right of action. In February 2022, Texas Attorney General Ken Paxton acted under the CUBI legislation and filed suit against Facebook, claiming that Facebook owed billions to the state for violating CUBI for not obtaining user consent when collecting the biometric data of more than 20 million Texas residents.

Another indirect approach can be seen in the handful of comprehensive data privacy laws recently passed that include facial recognition data in their scope. The only law currently in effect is the California Consumer Privacy Act (CCPA). It provides consumers certain rights related to their facial recognition data, such as the right to access, opt-out of the sale of and delete their data. Supplementing the CCPA, the California Privacy Rights Act (effective January 2023) allows consumers to limit a business' use and disclosure of their collected data. Colorado's privacy law (effective July 2023) requires businesses to obtain consent prior to processing consumers' facial recognition data, which falls under the law's definition of "sensitive data."

Currently, only a few jurisdictions directly regulate the commercial use of FRT. For example, Portland, Oregon, prohibits private entities from using FRT in "places of public accommodation." Other states or municipalities have legislation pending as well.

In July 2021, also by way of example, New York City passed a

biometric identifier information law prohibiting NYC businesses that "collect, retain, convert, store, or share biometric identifier information of customers" from profiting off the information; businesses must also disclose their FRT use to customers with a "clear and conspicuous sign." The law provides a private right of action for customers, but it also includes a cure provision for businesses to remedy certain violations. For instance, if a business violates the law's disclosure requirement, customers can notify the business of the alleged violation. The business then has 30 days to "cure" the violation before the customer can take legal action.

Additionally, early this year, New York City Council members have introduced two bills that would ban businesses and residential buildings from using facial recognition technology to identify customers or tenants without their consent. And, New York City has had some controversy around the use of FRT for commercial purposes. Specifically, the world-famous Madison Square Garden (and its owners) are alleged, without denial, to have used FRT to prohibit certain individuals from attending events being held at the venue. That is, Madison Square Garden has used this technology to identify lawyers from law firms who have filed lawsuits against the company from entering the facility despite their lawful purchase of tickets for an event. It will be interesting to see how this plays out in the courts and whether the justice system will concur that this is a legitimate use of FTR.

No different than Madison Square Garden, FRT creates many possibilities to gather information that can be used for numerous purposes for businesses such as Planet Fitness®. If this is a strategy that is used, operators will need to be sensitive to not only laws directly related to FRT but also other laws such as privacy laws or laws against discrimination that may also be implicated by this rapidly advancing technology. Indeed, the Planet Fitness franchise agreement addresses complying with all laws, requires approval for implementing processes in connection with operations and put the onus on franchisees to protect certain data, but maintains control over the "ownership" of said data. As such, there are significant considerations that should be taken into account if FRT is a potential data-gathering strategy for any purpose in connection with the operation of your business.

Additionally, there remains significant risk from consumers of potential lawsuits against business owners for collecting data wrongfully or mishandling the data that has been collected. Indeed, companies such as Amazon, Kroger and Walgreens have all been sued over the last several years for claims related to collecting customer data related to FRT and other biometric data.

The laws in this area are going to continue to evolve at a dramatic pace, and so is the use of these types of technology, especially as it relates to gathering marketing data. As such, it is critical to be mindful of both local and national laws that impact the use of FRT or similar types of technology. Moreover, and assuming the law permits it, this type of technology will likely soon be common if not standard in the marketplace, so educating yourself on the benefits, risks and how it works may be critical to your future success.

Justin M. Klein *is a franchise and business attorney and a partner with the nationally recognized franchise law firm of Marks & Klein, which represents Planet Fitness franchise operators throughout the United States and internationally. You can contact Klein at justin@marksklein.com.*