THE USE OF FACE BIOMETRICS IN COMMERCIAL SETTINGS

Security technologies are coming to market so quickly that the industry sometimes resembles a runaway train. A solution seems like a good idea, investors take note, and suddenly manufacturers are clamoring for market share before the kinks are worked out.

Commercial applications for face biometrics and facial recognition solutions are perfect examples. Globally, the facial recognition market is projected to grow 21.71% annually through 2026, from $3.72 billion in 2020 up to $11.62 billion[1] just six years later. In the U.S., a projected CAGR of 14.3% for the same period is slightly lower but still impressive.[2] While much of the demand is being driven by government opportunities related to Homeland Security and law enforcement, the commercial market is also exploding. Businesses are integrating face biometrics with access control systems to increase the security of their most sensitive assets: vaults, data centers, research facilities, controlled substances, critical infrastructure, and more.

As the Founder and President of a company that manufacturers biometric identity solutions that use the iris, face, or both, I have every reason to encourage these trends. However, I have experienced noticeable pushback against facial recently, and I sense a widening disconnect between the enthusiasm of manufacturers and the receptivity of the commercial market. Privacy concerns, fear of lawsuits, and changing regulations are making the face-based solutions less desirable than other biometric modalities, like the iris or palm.

The fraught status of facial recognition as a surveillance tool made headlines in 2018 when a feature in Google's popular Nest doorbells was challenged and found to violate Illinois' Biometric Information Privacy Act.[3] Nest doorbells record a short video clip whenever a visitor approaches. The "familiar face feature" spurring the lawsuit allows homeowners to identify specific individuals as "regular visitors" so that the Nest device recognizes them in future visits. What's the problem? There is no formal mechanism by which visitors are given the opportunity to agree – or decline – to be identified as a familiar face and thereby have their behavior essentially tracked. Video clips of familiar faces are aggregated by the Nest software and shared with homeowners as a series of related events. For Nest doorbells in use in Illinois, Google has since disabled the feature.

There is still no federal law regulating the use of facial recognition technology, but state legislatures beyond Illinois are taking action. Maine has banned the use of the technology for surveillance purposes, including by most areas of government,

[1] https://www.smarthomepoint.com/nest-device-illnois-eu/

[2] https://www.ipwatchdog.com/2020/01/28/varying-laws-governing-facial-recognition-technology/id=118240/

[3] https://www.smarthomepoint.com/nest-device-illnois-eu/

and strictly regulates its use by law enforcement. Laws in Texas and Washington state both take aim at businesses who collect and use biometric identifiers for commercial purposes, although the Washington law allows this to occur without notice and consent if the information is used to prevent shoplifting, fraud, and theft.[4] Without federal guidance, other states will surely follow suit. What does this mean for commercial real estate, where biometrics can clearly help strengthen security measures?

Facial recognition systems still have a place in commercial spaces, but stakeholders need to understand how they can and cannot be used. The two concepts to focus on are "subject consent" and "surveillance."

Face-based systems are in the spotlight because the face can be captured without a user's knowledge or consent and matched against readily available public databases. By contrast, users must willingly agree to have their iris or palm veins read and recorded. It would nearly impossible to gather this data surreptitiously. However, once individuals consent to share their faces for use by a biometric solution, businesses can use them for a wide range of purposes. Facial recognition can add convenience to access control, visitor management, time and attendance, point-of-sale, and other systems and processes with which workers interact daily.

For high-security areas, dual authentication requirements that include the presentation of a physical credential – whether card or mobile – combined with a biometric match such as the face, can eliminate the possibility of cards being used by anyone other than their owner.

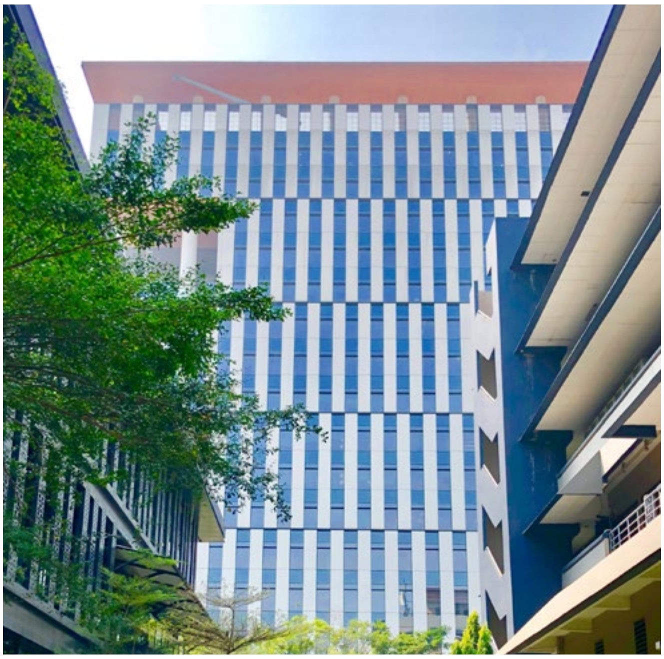
The use of facial recognition technology for surveillance purposes is becoming illegal in an increasing number of environments and applications. The bans apply to using software to automatically identify and track the movement of individuals within live or recorded surveillance video without their consent. However, this does not mean that corporate operations and commercial property stakeholders should completely shy away from facial analytics as a surveillance tool. There are still ways it can be helpful, using it only with subjects who have granted permission.

Paul Benne, PSP, CPOI, and President of Sentinel Consulting, has provided security guidance to some of the most high-profile commercial properties in the U.S. Assume that employees have registered their faces for use with the company's access control system and security operations. He says that facial recognition software integrated with surveillance cameras can alert security teams when the CEO or other high-ranking executives are onsite, or that a former employee who is now banned from the property has entered the building and may pose a threat. Such knowledge allows security teams to change their security posture immediately.

There's no question that facial biometrics and facial recognition technology have more than their fair share of critics. The public perceives face-based solutions as posing a greater risk for misuse and privacy violations than the iris, palm, or fingerprint. Therefore, companies wishing to implement operational and security technologies that leverage integrated biometric identity solutions will find an easier path to adoption using a modality other than the face.

However, solutions that include face as a secondary option should not be categorically dismissed. For systems that bundle facial and iris within the same reader, face identification can be disabled for employees who wish to opt-out. Keeping face as an option gives businesses added capabilities to enhance security while respecting legal limitations and workers' privacy. Faces can be identified from a greater distance and more seamlessly than other biometric markers and often do not require specialized readers. Facial identification also lends itself to surveillance applications, when permissible by law as previously discussed, in a way that other modalities don't.

No technology is perfect for all scenarios. When evaluating biometric solutions for commercial real estate, make sure that concerns over facial are rooted in fact, not fear. Maybe face-based systems shouldn't be the only biometric tool deployed onsite, but completely disregarding the category's potential may be a disservice to the facility itself and those working there.



[4] https://www.ipwatchdog.com/2020/01/28/varying-laws-governing-facial-recognition-technology/id=118240/