WHITEPAPER

BIOMETRICS IN COMMERCIAL REAL ESTATE: Putting Possibilities into Practice

By Paul Benne, Sentinel Consulting & Bobby Varma, Princeton Identity

INTRODUCTION

In 2020, commercial real estate development and operations supported 8 million jobs and contributed more than $1 trillion to the US economy[1]. Entire cities depend on the health of this sector. Now, as we emerge from the worst of the pandemic, real estate developers find themselves facing unprecedented market challenges. Employees like working from home; three in 10 say they will seek another job if their employer discontinues the policy[2]. For more ambivalent employees, companies must make the prospect of returning to the office more desirable. Steps include creating buildings that feel safer and more welcoming.

To this end, commercial properties are increasingly incorporating biometric identity solutions as part of their technology infrastructure. By integrating biometrics with a number of security and operational applications, developers and management companies can offer a premium experience to tenants seeking state-of-the-art security, efficiency, automation, and convenience.

WHAT ARE BIOMETRICS AND BIOMETRIC IDENTITY SOLUTIONS?

A biometric identifies someone based on a unique biological or physiological characteristic they possess. It can be their arrangement of facial features, the patterns in their iris, the whorls in their fingerprints, or vein patterns in their palms. It can also be the motion and gate of a person's walk, or the unique sound and tenor of their voice.

A biometric identity solution uses a stored version of an individual's biometric data to verify that they are, in fact, who they claim to be. Each time a biometric reading matches a recorded, stored version, its owner's identity is authenticated and verified.

Actually, it's more complicated than that. Biometric identity solutions use sophisticated algorithms to digitize and then encrypt each biometric reading and convert it into a very long, indecipherable code. That unique code must match to validate a person's identity.

The code cannot be reverse-engineered. For example, if an iris, fingerprint, or palm biometric database were compromised, it would be impossible for hackers to determine what any of the enrolled individuals' features look like. With only the encrypted code to work from, they couldn't fabricate an image to replicate the stored biometric. Databases full of PIN codes and passwords expose enrolled subjects to far greater risk than ones populated with encrypted biometric data.

[1] https://www.naiop.org/Research-and-Publications/News/NAIOP-News/2021/Commercial-Real-Estate-Development-and-Operations
[2] https://news.gallup.com/poll/355907/remote-work-persisting-trending-permanent.aspx

GROWING PUBLIC ACCEPTANCE

For commercial properties, biometrics present an easier, more efficient, and secure way for employees to be identified and gain access to areas within the workplace. Touchless biometrics systems — like those that use the iris, or combined face and iris — are particularly secure, convenient, and desirable in today's pandemic-conscious environment.

However, as much as property owners seek to create a superior experience for tenants, their willingness to integrate biometrics into their security infrastructure has been tempered by concerns that tenants, and the greater public, may not yet be ready to embrace the technology wholeheartedly. Smartphones' integration of biometrics helped it make tremendous strides in public acceptance, but choosing to use the technology on one's phone is fundamentally different than having one's employer require and oversee its use.

Covid, and its emphasis on automated and hygienic solutions, may serve as a tipping point. In the past two years, commercial real estate stakeholders have demonstrated a greater willingness to introduce biometrics within their properties. For now, the trend is most evident in single-tenant buildings, where only one management team needs to endorse the system's use. Potential applications include physical access control, logical access control, time-and-attendance, visitor management, video surveillance, and point-of-sale.

Younger workers tend to be most receptive to interfacing with biometric solutions, as they highly value convenience and efficiency. Also, the younger generation's comfort level with posting personal information to apps and social media has desensitized them to privacy concerns. By contrast, older workers are more likely to fear that biometric data shared with an employer or facility manager might somehow become part of a larger ecosystem and then be used in unintended ways without their permission. They worry about losing control of their personally identifiable information (PII).

Manufacturers could allay many of these fears by doing a better job of educating the public on how their systems work. Much of the underlying distrust is based on misconceptions and misinformation – a problem that is easy to remedy with a little concentrated effort.

BIOMETRICS AND ACCESS CONTROL

Access control is the most common application for biometrics within a commercial office environment. When biometrics replace cards, fobs, or mobile credentials, employees become free to enter and move about without having to carry something with them at all times. There is nothing to forget, lose, share, or steal. For administrators, it is as fast to enroll subjects into a biometric system as any standard access control solution. Plus, the data is cleaner and easier to manage. Biometrics eliminates the possibility of duplicate entries or confusion between subjects with similar names. Reporting on facility use and traffic patterns can be trusted as highly accurate. Biometric solutions are also "green," reducing the use of consumables that end up in landfills.

Dual authentication can be achieved by screening for two separate biometric modalities or combining biometrics with physical credentials. An enrollee's biometric data may be stored on a 13.56 MHz access control SmartCard or a smartphone, eliminating the need for centralized storage of biometric data. To enter a secure area, a person must present a credential and match the biometrics stored on the card or phone.

Best practices dictate that employer identification cards be separate from access credentials; combining them on a single card is a mistake companies make too often. By keeping them separate, the finder of a lost card does not know where it can be used.

When developing a security plan, commercial properties should – at a minimum – consider biometrics for the exterior of the facility. Using biometrics alone, or in addition or a card or PIN, is the surest way to keep unauthorized persons from entering the building. Beyond that, biometrics are best deployed to secure mission-critical locations inside. Mission-critical assets are those that, if compromised, would potentially impact the building's ability to operate. Examples include the boiler room, main electrical feed, main telecommunications area, or data center.

From a security perspective, there's no reason not to use biometrics elsewhere. However, there is a cost factor associated with each secured access point. Therefore, employing biometrics for areas that require less protection may be an unnecessary expense.

BIOMETRICS AND VIDEO SURVEILLANCE

Facial recognition is a form of biometrics often used in conjunction with standard IP video surveillance cameras. Unlike most other modalities, many facial solutions do not require dedicated readers – just special software. This advantage makes the face one of the most affordable and flexible biometric modalities.

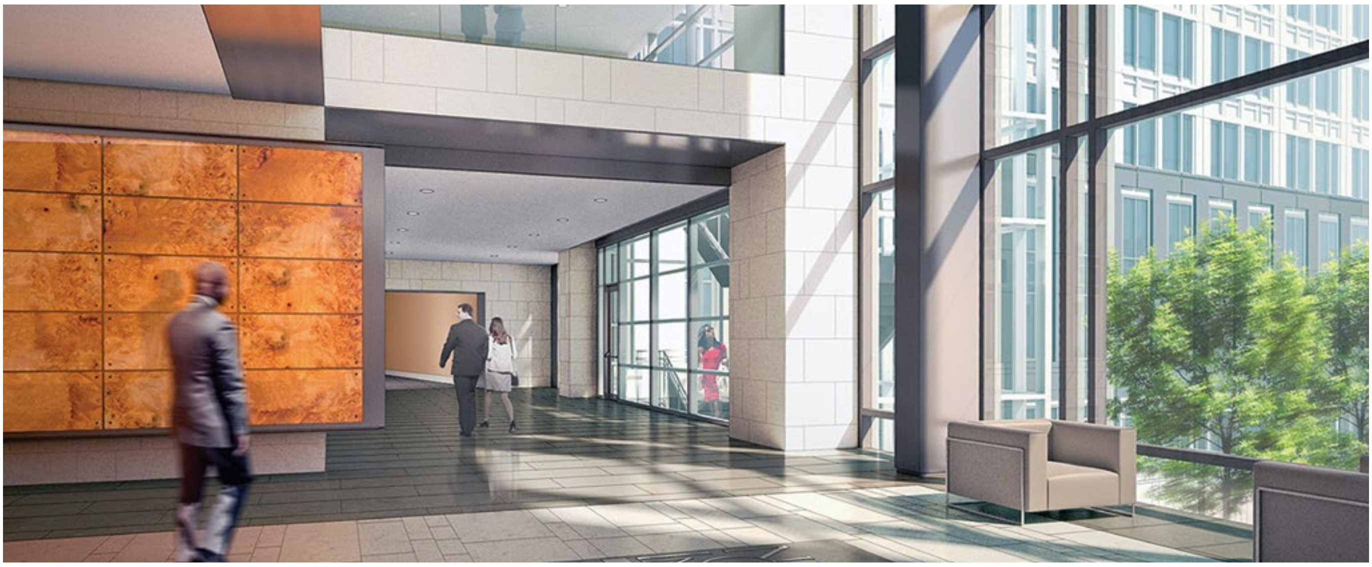
Especially in open environments, such as a commercial office lobby, customers are seeking a seamless experience. Here, biometrics integrated within video surveillance solutions are an attractive value-added application.

Strategically placed security cameras can scan the faces of people on the go. Identities can be verified against a list to quickly determine whether an individual should be granted access. Facial analytics also provide security management with an automated notification when certain conditions arise – not only from an access control standpoint but from an dentity perspective. For example, the software might alert system administrators that the company's CEO is on-premises, or that a former employee – now on a list of banned individuals – has entered the building and may pose a threat. The technology allows security teams to immediately change their security posture based on who enters the building.

However, of all the biometric modalities, facial has received the most pushback from the public. Studies have shown that facial recognition is less discerning with people-of-color, resulting in false matches and unequal treatment.[3] There is also widespread discomfort with public a nd private entities applying such technology without user consent.

Several states have moved to regulate facial recognition as a surveillance tool. The Security Industry Association asserted in July 2021 that it "is advocating nationwide for policies ensuring responsible use and sensible privacy protections, while urging rejection of blanket bans or unbalanced restrictions of these technologies that ignore the clear benefits of many applications and ultimately harm rather than protect Americans."[4]

Because of the controversial nature of facial biometrics and the headache of navigating a web of legal regulations, commercial real estate stakeholders may wish to explore alternative biometric modalities for use in their properties. Iris-based systems, for example, have not received any such backlash and are already well accepted in other public-facing applications, like travel screening.



[3] https://www.washingtonpost.com/technology/2019/12/19/federal-study-confirms-racial-bias-many-facial-recognition-systems-casts-doubt-their-expanding-use/
[4] https://www.securityindustry.org/2021/07/09/most-state-legislatures-have-rejected-bans-and-severe-restrictions-on-facial-recognition/

BIOMETRICS AND VISITOR MANAGEMENT

Visitor management is a relatively new application for biometrics. Management organizations with sizeable real estate portfolios are looking to create more customer-friendly experiences for visitors entering their buildings. They would like to eliminate the long lines of people waiting to have IDs validated and temporary credentials issued before they can pass through turnstiles and access elevators.

Suppose the identity of visitors can be validated before they arrive at the building. In that case, they can receive a temporary pass on their phone, allowing them entry for a designated window of time. Biometrics can serve as a valuable tool in this scenario. They may be used to validate visitors' identity remotely, in advance – like matching subjects' faces via webcam to their scanned driver's license image – before a mobile credential is issued. Upon arrival, a second facial match may be required in addition to presentation of the mobile visitor's pass. With these security precautions in place, visitors can bypass checking in at a visitor's desk.

Furthermore, if someone is a regular visitor, they can receive a credential that is valid for recurring appointments. Because the mobile credential cannot be shared with others, as a paper visitor's pass can, there's no need for rescreening and reissuing credentials for each separate visit.

CHOOSING THE RIGHT MODALITY

The success of any biometric solution is predicated on selecting a suitable modality for the application. If users find interacting with the system is burdensome, they do not trust its accuracy, or feel that it unduly infringes on their privacy, it is not a viable solution.

Stakeholders of commercial properties must clarify several issues before evaluating possibilities. How will the biometric identity system be used? How many people will be enrolled? How quickly must the system process users? What are the lighting and environmental conditions at locations where readers will be placed? Given COVID guidelines, are gloves, goggles, or masks likely to be in use?

In large lobbies, the face is the primary modality in use, although that may be changing. The iris is a better choice for applications that require more than a few hundred users or more secure settings. Unlike the face, it can accurately distinguish between an unlimited number of enrolled users. It is equally effective with people of all ethnicities and skin tones.

Highly discerning, touchless palm-based solutions are now available. However, while they are more hygienic than their predecessors, which required physical contact with a reader, the newer touchless systems are not hands-free. For settings where users are likely to be carrying objects or need their hands available for other purposes, the iris offers greater convenience.

Dual biometric authentication, such as iris and face, offers additional benefits. Such systems deliver a second layer of security. They also provide flexibility for processing the rare user for whom one of the modalities won't work.

WHAT'S NEXT?

There is enormous potential for biometrics in commercial real estate properties. We're just at the infancy of what biometrics can do to improve the modern workplace. The technology is uniquely suited to harden security while enhancing the user experience.

Imagine arriving at a facility, and your identity is already verified. You are then given instructions, via your smartphone, on which elevator bank to take and what floor to enter.

Or, in the lobby, security officers wear augmented reality glasses tied into the integrated biometrics and video surveillance system. The glasses allow them to see virtual green, amber, and red halos over people's heads, indicating who is verified and authenticated, who must be manually processed, and who is banned from the property. It happens seamlessly, all in real-time.

This is a future where security protocols don't slow us down – but power us forward. Biometrics can achieve that vision, but first, education must dispel misconceptions. As public acceptance of biometrics grows and forward-thinking developers prevail, today's fantasy of enhanced security, convenience, customer experience, and efficiency will become defining characteristics of tomorrow's most coveted commercial office space.

Mr. Paul Benne, PSP, CPOI, is the Founder and President of Sentinel Consulting, a full-service security consultancy that provides clients with technical and operational security expertise. Mr. Benne's professional career has included work in emergency management, law enforcement, firefighting, security management, crowd management, operations, training, and technical fluency in the design, implementation, and management of physical and electronic security systems, all of which form the basis for his uniquely broad and deep security perspective. His company offers risk assessment, security master planning, technical and architectural security design, operations, and training.

Ms. Bobby Varma is the co-founder and CEO of Princeton Identity (PI), a biometric solutions manufacturer recognized for its best-in-class technology. A visionary leader within the biometric arena, Ms. Varma is dedicated to expanding applications for biometrics through partnerships between PI and leading global entities in physical and logical security. She serves on the Security Industry Association (SIA) Identity and Biometric Advisory Board, an exclusive panel of experts who guide SIA's engagement with critical infrastructure operators and seeks to ensure biometric identity solutions are used in an ethical and non-discriminatory manner. Ms. Varma holds her MS in Biomedical Science from Drexel University and BS in Biochemistry from Rutgers.