THINK BIOMETRICS COMPROMISE PII SECURITY?

Think Again. The Case for Education in Building Public Trust.

Written by: Bobby Varma, CEO Princeton Identity

Return to office dates have been pushed back so many times we've lost count, but it seems like this spring will finally be the real deal. During the past two years, commercial property managers have had an opportunity to rethink and execute infrastructure upgrades, many of which evolved in response to COVID. In addition to tackling traditional physical security and health-safety concerns, building managers recognized that they must also address returning workers' strong preferences to interact with touchless technology. Certain biometric solutions provide an ideal tool for interfacing with security and facility management systems in a contact-free manner.

We're already starting to see the integration of biometric systems at single-tenant commercial buildings. Because a single entity employs all workers at these facilities, management is empowered to set the pace for how its organization engages with the technology. Access control is the most prevalent application, but some forward-thinking companies are testing the waters with visitor management, time-and-attendance, point-of-sale, and other solutions.

Multi-tenant properties wishing to explore biometric options face a higher hurdle: convincing a wide range of stakeholders that deploying the technology is in everyone's best interest. Despite biometrics' ubiquity in smartphones, there remains widespread skepticism of its safety and efficacy in other applications – primarily based on misconceptions over how such systems work.

The heart of most fears center on the safety of PII – or personally identifiable information. We've all felt the pain caused by malicious phishing, over-sharing on social media, sloppy storage or disposal of private communications, and data leaks. Anyone can perform an online search and uncover a history of our past addresses, phone numbers, the names of relatives, employers, political donations, court cases, and much more. We've also experienced the effects of PII shared by marketers, who seem to know all about our medical conditions, lifestyles, and spending habits without our permission.

The hassles of changing passwords, canceling credit cards, requesting a credit freeze, and taking other security precautions due to compromised PII are a constant source of stress. Therefore, it seems logical to be concerned about what would happen if a biometric database were to be breached. We can change a passwords and account numbers. We can't change our eyes, fingerprints, or other physiological traits. Many feel that the requirement to share biometric data with an employer or building management firm is a violation of privacy and a recipe for disaster.

Education can dispel these fears. The truth is that databases of PIN codes and passwords expose enrolled users to greater risk than ones containing encrypted biometric data. Here's why.

Biometric identity solutions do not store images or humanly discernable descriptions of subjects' biometric signatures. When a camera or reader processes an iris, face, palm, finger, or other modality, the system digitizes the measurements it perceives into a long, encrypted code using proprietary algorithms. The code is all that's recorded, and it cannot be reverse-engineered. If a hacker were to gain access to a database filled with these encrypted codes, he would be incapable of reconstructing a representation of the biometric features they represent. The code cannot reveal the information needed to replicate the patterns in an iris, the geometry of a face, or the ridges in a fingerprint. There is no PII to steal.

Another way to encourage biometric adoption is by deploying solutions in which system users maintain sole possession of their encrypted biometric data. Instead of a utilizing a centralized database, physical credentials like 13.56 MHz SmartCards or mobile credentials store each user's biometric data. To enter a secure area, users must present their physical credential plus verify it is their own by providing a biometric match to the data stored on it. This dual-authentication solution is less convenient than one relying solely on biometrics, but it is incredibly secure and eliminates the danger that an unauthorized individual could use a stolen or lost card.

Convenience and familiarity help breed acceptance of any new technology, but education is necessary too. When consumer-priced microwave ovens appeared on the market in the 1970s, their superior ability to heat leftovers and make popcorn was not enough to initially convince a significant subset of consumers that the ovens didn't cause cancer. When smart speakers like Amazon Echo and Google Home were introduced a few years back, initial sales were tempered by concerns over privacy – that voyeuristic tech workers were listening in on private conversations. In both instances, education about how the devices work – combined with convenience and familiarity – was key to expanding market penetration.

Biometrics offer convenience. They're also no longer an oddity, reserved for science fiction. In addition to unlocking our smartphones, we see biometric solutions in airports, sporting events, and when we check in at medical offices. Widespread adoption within commercial real estate is coming soon. Education must come first!

ABOUT PRINCETON IDENTITY

Princeton Identity is the identity management company powered by biometrics, making security more convenient, accurate, and reliable than ever before. Leading the revolution toward a more intuitive, efficient, and natural security experience that keeps people and businesses moving, Princeton Identity uses iris recognition, face recognition, and other biometric technology to enable businesses, governments, and global organizations to streamline identity management, resulting in improved safety and protection. Formerly a division within SRI International, Princeton Identity spun out as an independent venture in August 2016.