How to Protect Privacy in Face-Based Access Control

A StoneLock White Paper

STONELOCK

We See People Differently

INTRODUCTION

Cutting Through the Controversy

Biometric technology has become increasingly popular over the last few years, finding its way into everything from smartphones to airport screening to door locks. And of the different biometric modalities – fingerprints, irises, and so on – facial recognition has emerged as the most familiar to consumers and citizens, in both positive and negative ways.

Regarding the latter, there has been a great deal of controversy in the mainstream news over government and police use of facial recognition. Authoritarian governments like China's have used the technology in oppressive surveillance systems, while in America, civil rights groups have raised alarm over police agencies' use of biometric surveillance on law-abiding citizens, with some municipal and state governments seeking to ban such practices.

At the same time, a growing number of consumers have started using their faces to unlock their smartphones, enjoying the convenience and security of sophisticated new facial recognition systems being adopted by top brands. The technology is also finding its way into computers and operating systems like Windows 10, with tech companies seeing great benefits in improving the user experience while boosting security.

In other words: it's complicated. Facial recognition is both hugely popular and quite controversial, depending on how it's being used. This paper will zero in on one of the most impactful applications of facial recognition technology – access control. It will look at the unique benefits that facial recognition brings to this area, and will parse through the controversy surrounding this technology, proceeding to detail how facial recognition can actually enhance privacy when used the right way. With so much to gain from embracing this technology, and so much to lose by doing it wrong, the paper aims to deliver critical insights for organizations looking to implement or enhance access control frameworks.

PART 1

Why Face is the Modality For Access

Inherently more secure and convenient than keys, cards, and PIN codes, biometrics are emerging as the security solution of the digital age, especially in the workplace. And, perhaps more than any other biometric modality, face recognition is best suited for physical access control: unlocking doors, safes, and turnstiles for authorized personnel.

Contactless and Clean

Public health is a major concern, and contact-based security can lead to the spread of harmful bacteria and viruses. Face biometrics is a completely contactless authentication modality, enabling facilities to stay secure and users to stay healthy.

Learn more about the hygienic benefits of face biometrics in the StoneLock white paper, **"Entering the Age of Contactless, Convenient and Clean Biometric Access."**

The Benefits of Face

What makes face recognition for authentication stand out? Its contactless convenience, for a start. Today's best facial recognition security technology can detect an enrolled user's face in less than a second from a convenient and safe distance, so that when an authorized person arrives at the door they want to enter, it's unlocked for them. This contactless nature makes facial recognition ideal for high-throughput deployments serving a diverse range of people in a safe and sanitary manner.

Face authentication also boasts a high level of accessibility and nuance. Properly deployed face readers can capture and match face biometrics from personnel of various heights and characteristics, authenticate users with gloves and safety gear or otherwise occupied hands, and still provide the best protection of critical spaces and assets. Furthermore, face recognition is the most natural mode of authentication – intuitive, easy to use and understand.

Match Game

There are two biometric matching methods for authentication:

1:1 (one-to-one) matching is when a biometric system is looking for a single authorized user based on an individual biometric template. For StoneLock, that allows an individual to present a verification card to confirm that person is present. In general, that template can be stored on a security card, in a mobile device's secure element, or in a biometric edge reader itself. For ultimate security and privacy measures, **StoneLock only stores templates on the StoneLock GO edge reader and enterprise Gateway.**

1:N (one-to-many) matching is similar—it matches users to stored templates for authentication—but eliminates the need for dual-factor authentication with a card reader and searches across multiple templates for the match. Authorized users have biometric templates stored securely on a device or access control server, and when approaching a door, their face biometrics are captured and compared to the various stored templates. A match to any template will verify the user, allowing the access control system to assert their granted permissions.

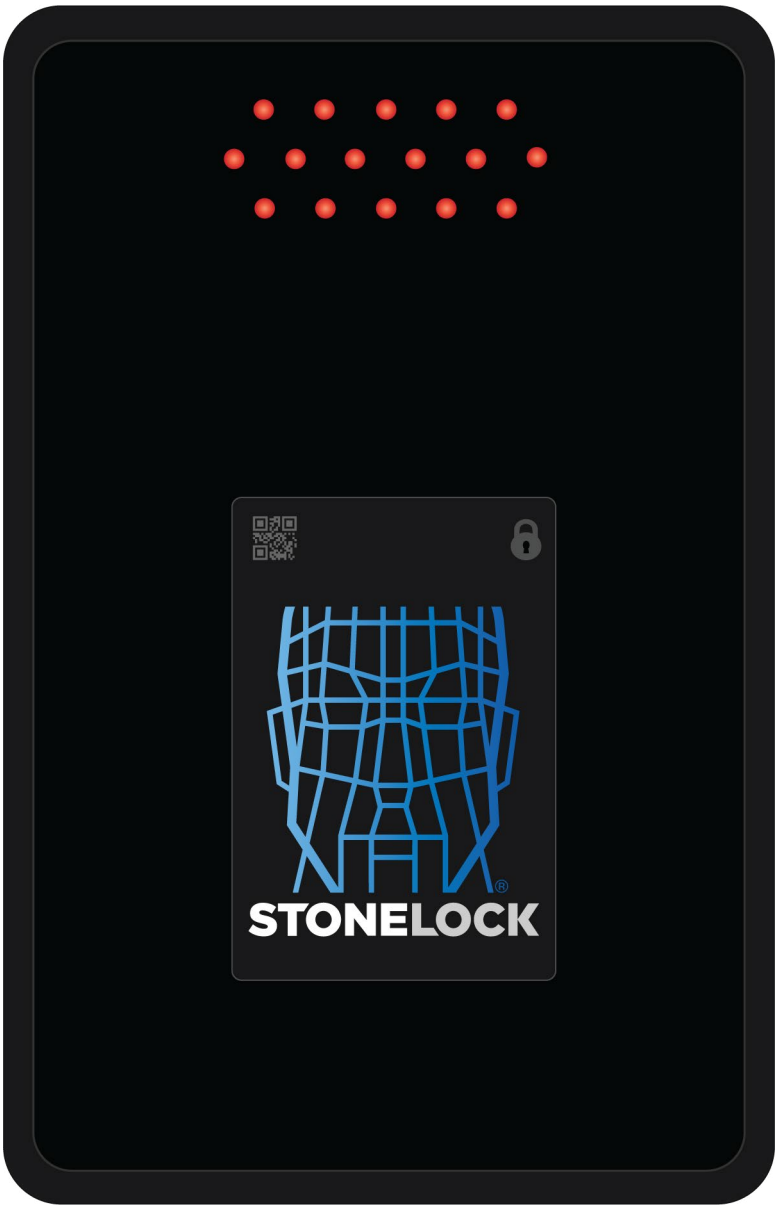
Both matching paradigms are suited for their own ideal access scenarios, but importantly: they are both secure, convenient, and privacy-enhancing. 1:1 matching is great for limited personal use, particularly when authenticating online or on a personal device like a smartphone or home computer. 1:N matching is ideal for shared spaces. The two can even be used in tandem, allowing for a flexible security system.

As an example: the StoneLock GO face authentication solution supports both 1:1 and 1:N matching. If an office entrance is protected by StoneLock GO, 1:N matching can authenticate permanent employees. It also works for short term contract workers. Instead of having to onboard a temporary employee onto the authentication server for 1:N matching, the temp can be issued a QR code, enabling StoneLock GO to use 1:N matching

First Read Enrollment™

StoneLock's new First Read Enrollment™ feature simplifies the user onboarding process. When a user presents a credential to a card reader – or a QR code in a 1:N scenario – the user triggers the StoneLock self-enrollment prompts on the device's display. By following the prompts, the user can enroll their biometrics in seconds from any designated reader in the access control system.

between a transient user's face and the template to be stored on the edge reader and Gateway.



The StoneLock GO edge reader, shown to scale.

PART 2

Why is face recognition so controversial?

While there are clear benefits to using facial recognition for access control, the broader controversy over this technology demands that administrators be able to dispel some of the misconceptions around face biometrics. Employees and visitors who are unfamiliar with the nuances of this technology will naturally have some questions, and many of the most common misconceptions can be grouped into two batches of concerns.

"What if my biometrics get stolen?"

The first batch revolves around the idea that biometric data can be stolen or otherwise violated. Biometrics *cannot be stolen* (short of amputation), but they can be mimicked, or "spoofed." Fortunately, sophisticated *liveness detection systems* have emerged that are designed to look for subtle clues – such as the micro-movement of hair, for example – to verify that an authorized user is truly present during a biometric scan, and that it isn't a photograph, video, or even an elaborate mask. Your face is public information, after all; anyone can see it when you're out in public, or even on your social media profile. What's important is making sure that this publicly available information isn't of any use to a fraudster, hacker, or other malefactor trying to fool a biometric system. A sophisticated biometric system featuring anti-spoofing capabilities (such as near-infrared imaging and subdural data) will do just that.

Authentication is Not Surveillance

The other batch of concerns is more directly tied to the controversy over biometric surveillance and potential privacy violations. This is a serious issue when it comes to government authorities' use of facial recognition technology, but a private organization's use of biometrics for access control is something very different. It

Templates are the Key to Privacy

To ensure the utmost privacy, a biometric authentication system should store templates representing an authorized user's biometric data rather than images of their face, fingerprints, or eyes. That way, in the case that a server is breached, bad actors only receive mathematical representations of their authorized users, not personal data. While it's true that modern biometric systems are incredibly difficult to trick (or "spoof") using pictures and videos, compromised images can still be used to violate user privacy through the malicious use of identification software that can match photographs and videos containing faces to social media profiles, in turn empowering fraudsters with personally identifiable information (PII).

1:N Authentication versus Identification

The difference between privacy enhancement and privacy violation hinges on consent. Biometric identification relies on 1:N matching, similar to some authentication scenarios. But identification technology is indiscriminate, scanning subjects and matching them to a dataset composed of face images. In a template-based authentication system, a biometric scanner is used only to match a consensually onboarded user to a mathematical representation of their biometrics.

comes down to *identification* versus *authentication*.

Identification is tied up in surveillance. These biometric systems are designed to identify individuals who aren't volunteering to be identified; indeed, they may not even know they are being scanned. *Authentication*, on the other hand, is the opposite: an individual knowingly consents to being authenticated by a biometric edge reader in order to confirm that they are who they say they are. This is what is happening in biometric access control, where employees trying to get to work – or visitors at a different kind of restricted facility – will volunteer some amount of personal data to gain access. Traditionally, this has been done at a security gate with a live guard, or with an access card at an automated door. In either scenario, a face scan can make the process easier, and is no more intrusive. Moreover, if done correctly, face-based authentication only enhances privacy protection.

Protecting Privacy

Face biometrics can actually help to protect privacy in authentication scenarios. That's because biometrics can identify an individual without any reference to biographical data like date of birth, address, or even name.

In the world of access control, traditional systems have tended to involve at least some disclosure of subjects' personal data. This might involve the provision of name and contact information at a sign-in desk, or using an access card that features identifying biographical data. Face biometrics offer an alternative. With an initial registration linking an individual to their employee records, there is no need for them to present any personal information during an authentication process: a simple face scan will open the door. And with no need for administrators to handle the paperwork associated with more data-driven access systems, organizations are better able to comply with privacy and data protection regulations.

PART 3

Security and Privacy in Practice

Face biometrics for authentication can offer the highest grade of security and the best user experience, while enhancing the privacy of users. Deployed using consent-based best practices, and used as a physical access control, face recognition can transform the working world for the better.

Face Authentication in the Enterprise

In the enterprise, biometrics save time and administrative costs. With biometrics at the door, you no longer have to worry about lost or stolen keys. When employees are authenticated by their faces, access is easier. Beyond the front door, face-based authentication can be used for accurate payroll, allowing employees to clock-in with ease and ensuring administrators have accurate records.

The StoneLock privacy difference: StoneLock GO face authentication technology is an easy-to-use enterprise management system that utilizes near-infrared technology without capturing – let alone storing – photos or images of faces. This means short-term staff and long-term staff alike can rest assured that their physical facial profile is never stored, and can never be compromised. The biometric profile is completely unrecognizable outside of the SonteLock GO edge reader or Gateway, meaning the data captured will never inadvertently expose personal information about the user. In many ways, this could be called "faceless" recognition given the technology does not rely on any identifying facial features.

Face Authentication at the Bank

At the bank, face biometrics are up to the task of protecting the most valuable assets, while keeping operations running smoothly. Cash drawers, vaults, financial records, even banking data centers and check processing: these are all high-risk access scenarios vulnerable to shared or

stolen passwords and keys. Face biometrics improve on even multi-factor security methods, reducing friction and administrative costs associated with credential replacement and reset procedures, while keeping an accurate audit log. As in the enterprise, face biometrics can also be used for keyless entry and attendance management in financial institutions.

The StoneLock privacy difference: Because StoneLock GO uses biometric template matching for security, even high-risk access control scenarios that depend on authentication-proofing processes don't require biographical or contextual PII to be connected to employee credentials. With StoneLock, the vetting process and onboarding process are separate, so your credentials aren't a liability for your employee's privacy.

Face Authentication in the Clinic

The wave of digitization in the healthcare sector has made patient records more vulnerable, while the ongoing opioid crisis has spurred an increased need for professional accountability and best-in-class security. Access control and audit trails are essential in ensuring said accountability in clinics. Face-based biometric security on drug cabinets ensures only registered clinicians can access restricted substances, which in turn helps keep an easy-to-follow audit trail in case anything goes missing.

The StoneLock privacy difference: In healthcare, privacy extends beyond biometric matching. Patient health records contain highly personal information, and it's important it doesn't fall into the wrong hands. By using the StoneLock GO edge reader to control health record access, clinics ensure sensitive data is only shared between patients and registered StoneLock GO keeps healthcare providers HIPAA compliant, while providing contactless and clean physical access security, preventing the spread of contagions.

Whether it's for a high throughput entrance, a bank vault, a drug cabinet, or anything else that needs the best security on the market, face biometrics that remove the use of photographs are the privacy-enhancing answer. Your face is the key to a frictionless user experience, and in a privacy-first authentication model, facial recognition for authentication will ensure your privacy remains as safe as your most valuable assets.

CONCLUSION

The StoneLock Difference

StoneLock GO is the answer to your privacy-enhancing security needs.

StoneLock GO is easy to deploy as a biometric authentication solution that enhances your existing physical access system. With intuitive and flexible onboarding, and the ability to detect user faces in total darkness, thanks to its near infrared technology, StoneLock's solution is versatile enough to bring convenience, security, and privacy peace-of-mind to your organization. That's the StoneLock difference.

Learn more about the StoneLock difference today at stonelock.com

Contact information: sales@stonelock.com

About StoneLock

A woman-owned business enterprise (WBE), StoneLock® is a global leader in the design and manufacturing of biometric access control reader technology. Providing a best-in-class solution for both security and privacy, StoneLock offers rapid, reliable authentication of users while providing ease of use for both users and administrators of the system. Together with the StoneLock® Gateway, a biometric-centric authentication solution, the StoneLock® GO delivers a contactless and utterly secure and private experience for users. More than 40 percent of Fortune 100 companies as well as government entities rely on StoneLock®, a privately held company, for the seamless protection of their most critical assets. For more information, visit www.stonelock.com