FindBiometrics Identity School:

FACIAL RECOGNITION CHEAT SHEET

Find the Biometric Solution for Your Security and Customer Experience Needs

Facial recognition has become a catchall term that is used to describe any application that analyzes someone's facial features in order to verify their identity. Unfortunately, that broad designation can make picking the right type of biometric solution for your organization difficult.

When it comes to facial recognition, distinctions matter. Privacy and security issues can vary widely depending on the nature of a facial recognition application—some applications can enhance and protect a user's personal identity data, while others run the risk of infringing on their privacy rights. And yet, biometrics remain the best way to enhance security and convenience, to enable fraud protection, to prove identity, and to enable compliance with Know Your Customer (KYC) regulations. Facial recognition can solve your authentication and identity challenges, but the question remains: *what type of facial recognition do I need?* FindBiometrics' Identity School has you covered: here are four of the most common types of facial recognition technology, what they're best suited for, and how to tell them apart.

Smartphone Authentication

What it's for: Password replacement, strong authentication, convenience

What it is: Facial recognition is versatile and can be deployed as software on any device with a digital camera, and it is so convenient for end users that it ships prepackaged in many flagship smartphones. In practice these systems allow you to use a built-in camera or a special infrared sensor to unlock a phone, tablet, or other consumer mobile device with your face, or to replace passwords on apps This is perhaps the most common form of facial recognition, and the one that you are most likely to encounter on a daily basis when unlocking your smartphone, logging into your banking app, or authenticating on your password manager.

How it works: The most common phone unlock systems are entirely self-contained. The biometric template is stored on a secure element on the phone itself, and is never sent to the cloud or stored on an external database. In that regard, the template functions much like a PIN, since the phone is simply matching a new image to that existing template each time a registered owner unlocks the device. This on-device matching is the underlying facial recognition technology for most consumer sparthone applications, including mobile wallet payments and biometric app login.

Don’t forget: Smartphone biometrics do not require a user to verify their identity during the setup process. This means that while they enable high levels of convenience and personal security, they have no attachment to your personal information. A person who can unlock a smartphone with biometrics is only asserting that they are the person who enrolled their biometric in the first place, they are not verifying their identity. **If you want to provide a high level of convenience and security to your users, this type of facial recognition is for you.** But if you need more identity assurance you will need…

Mobile Identity Verification

What it's for: Opening accounts, complying with KYC regulations, deduplicating accounts, creating a trusted digital identity

What it is: Commonly referred to as remote enrollment or digital onboarding technologies, identity verification solutions are similar to device unlock systems insofar as they take advantage of a smartphone’s built-in cameras. However, they differ in the sense that they require an exchange of information, generally requiring the user to upload multiple images to a third party. Identity verification technologies typically appear in mobile apps, and are increasingly being used for financial applications like opening a bank account online.

How it works: The process begins with enrollment, where a facial recognition system will match a selfie of the user to the image on a photo ID to verify their identity. The technology allows for biometric identity verification in cases in which an organization does not yet have a record for an individual.

It also allows an organization to collect a template that can be used for subsequent authentication. The next time the user wants to log into their account, the system will match a new image of the user to that original template, building on the foundation of trust gained from the identity document match during the onboarding process. In some cases, the app asking for proof-of-identity may store the template on a remote server. In others, the match may be carried out locally on the phone.

Regardless of the setup, identity verification and any subsequent authentication thereafter relies on a one-to-one match, checking to see whether or not the person logging in is authorized to access a given account. In doing so, the system can replace a password with a biometric identifier that cannot be guessed or cracked by a cybercriminal, while also proving to another party (a bank, the government, or a service provider) that you are who you say you are.

Don't forget: Identity verification systems do not cross-reference images to match faces and names in a larger database. They instead perform a discrete match at a time and place of the user's choosing, with a device that remains in its owner's possession. **An identity verification solution is the best way for a user to prove they are who they claim to be, and for you to trust that claim.**

Authentication at Work

What it's for: Opening doors and turnstiles for authorized users, unlocking on-premises workstations, automating tracking time and attendance tracking

What it is: Many businesses are now using facial recognition for access control, scanning the faces of employees and other individuals when they try to enter a building; and for time and attendance tracking, enabling staff to punch in and clock out efficiently without having to touch shared surfaces. These systems are similar to online authentication systems, since they ask users to register their biometric credentials in advance, before presenting their faces at a point of entry to confirm who they are. The difference is that the end users are no longer in control of the authentication hardware, or in possession of their biometric templates.

How it works: Businesses install cameras and facial recognition software, integrated into their access control or time and attendance system. After enrolling their biometrics in the system, workers can approach a door or turnstyle equipped with a camera, sit at their workstation, or present their face to a time clock, to have their face scanned. A match of their face to the template in the biometric database will grant them access or clock them in/out. The hardware, software, and the biometric templates all remain in the possession of the organizations that set up and run the entire system, providing the end user with a seamless experience.

These systems are performing authentication procedures, matching a consenting individual to pre-enrolled biometric templates at a specific place and time. The cameras themselves can be deployed in a wide range of devices, from kiosks to tablets to security cameras, and do not force employees to carry around a physical badge while at work.

Don’t forget: This type of contactless facial recognition can be used for authentication purposes beyond the workplace, though the actual experience and technology will be similar regardless of the intended application. For example, retailers are now deploying facial recognition at checkout counters to enable face-based payments and loyalty rewards for shoppers. **Whenever you are collecting or storing biometric data, you are subject to privacy regulations—save yourself from a lawsuit by learning about biometrics privacy best practices.**

Identification via Biometric Surveillance

What it's for: Law enforcement, video-based security, border control, military applications

What it is: Biometric surveillance is the facial recognition most concerning to privacy advocates. Modern surveillance systems can apply facial recognition software to video feeds in real time, giving operators the ability to identify and track people as long as they are in view of a connected camera. These systems run continuously (instead of limiting scans to one point in time), and do not require any active participation from the people being monitored. As a result, those people will often not know that they are being watched, or that biometric matching is taking place. In security and law enforcement scenarios in which a user may not want to be identified, this type of facial recognition can be used to match against watch lists of known offenders.

How it works: The scope of a surveillance system can vary, depending on the organization and use case. The common element between biometric surveillance systems is their passive identification of subjects. A person who enters the range of a biometric surveillance system will have their face scanned and compared to templates in a database. Private businesses can use a relatively contained system to protect a facility like a warehouse or a factory, where facial recognition will alert security to the presence of any unfamiliar individuals. Public-facing establishments like casinos often use the tech to spot people like known cheats or problem gamblers on a maintained watchlist.

There is virtually no limit on the scale of a surveillance system if the government gets involved. Law enforcement departments have installed tens and even hundreds of thousands of cameras in some of the biggest cities all over the world. Such a system allows the government to potentially track and find almost any citizen in real-time, no matter where they happen to be. In many cases, the government can use driver’s licenses and other documents to generate a positive match.

Don’t forget: The scale, use case, and privacy protections vary on a situational basis when it comes to face-based surveillance. In certain jurisdictions, a private sector deployment of this kind is at high risk of running afoul of privacy regulations, while in others it can be implemented for security purposes with proper notice and transparency efforts. Unchecked and secret surveillance, however, is the token of authoritarian states. **Remember: facial recognition is a powerful technology and should be used responsibly.**

If you are aiming to improve security, trust, and the user experience at your organization—whether you are enhancing customer journeys through digital channels or physically protecting your facilities—you can deploy facial recognition today and start to see immediate results. Visit the FindBiometrics facial recognition vendor list to get started.

These four types of facial recognition technology are distinct, with their own implications for privacy, security, and convenience. If your organization is aiming to deploy facial recognition, or any biometrics for that matter, make sure you are on the right side of emerging privacy regulations by asking your self Identity School's Seven Questions That Can Save You From a Biometrics Lawsuit.

About FindBiometrics and Mobile ID World

FindBiometrics and Mobile ID World are your leading industry resources for all information on biometric identification and identity verification systems and solutions. We have the latest daily news from the global biometric and identity management business community, a comprehensive vendor list, informative articles, interviews with industry leaders, exclusive videos, links to biometric associations and a calendar for the most important and current industry events and conferences, including our lauded webinar series and virtual Identity Summit events. FindBiometrics is also a proud member and longtime supporter of the International Biometric and Identification Association (IBIA).

FindBiometrics and Mobile ID World are part of the ChannelPro Network, a division of EH Media LLC, a leading U.S. business-to-business media company and conference producer.

This resource is being provided as a starting point to understanding the best practices regarding biometric data collection and user privacy. It does not constitute actual legal advice. Before deploying any biometric technology it is wise to seek professional legal counsel regarding local, national, and international privacy laws.

For more educational resources on biometrics and digital identity, visit: FindBiometrics.com.