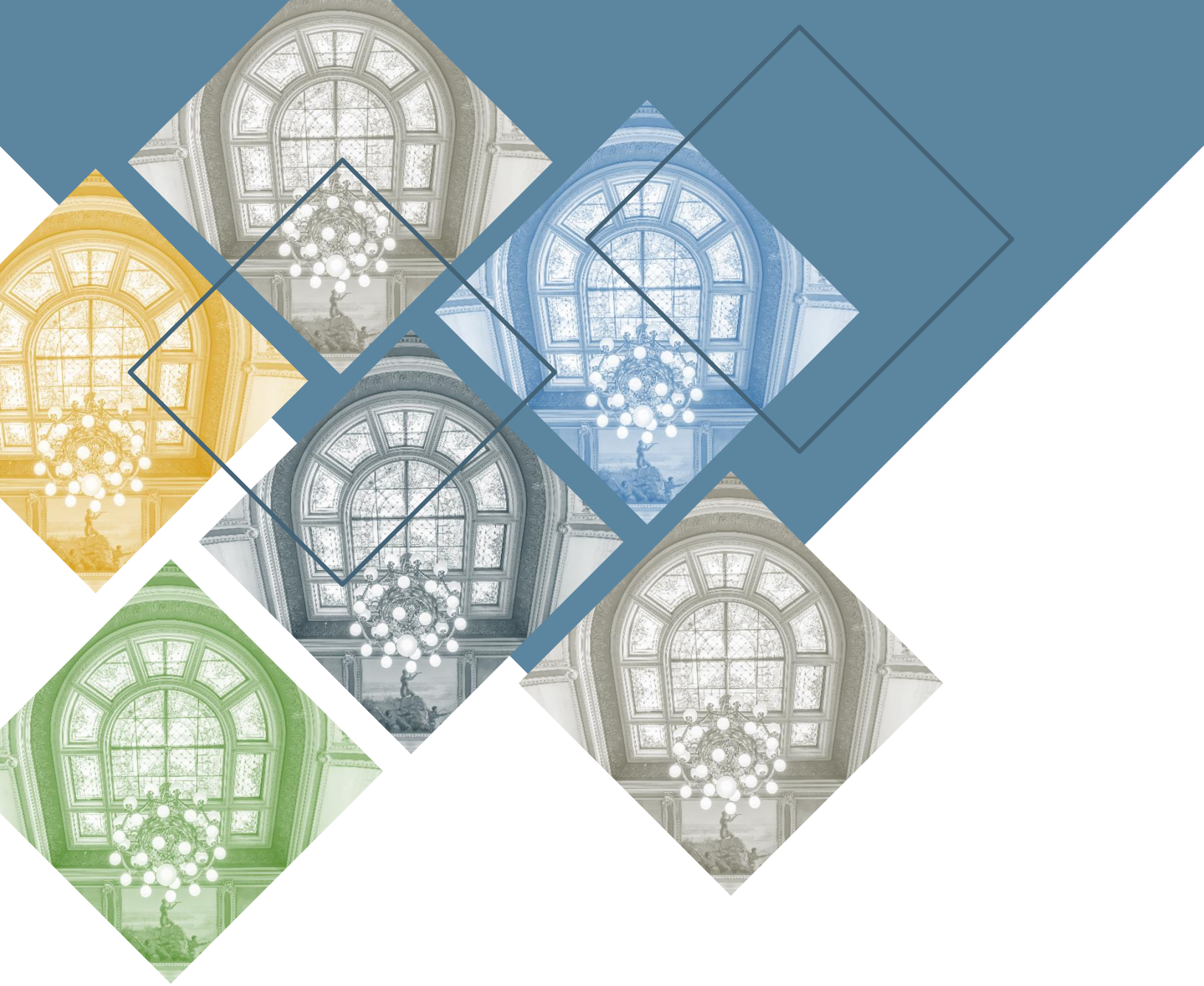

FACIAL RECOGNITION TECHNOLOGY: VERIFICATION VS. IDENTIFICATION

November 2021

Economic Affairs Interim Committee

Erin Sullivan, Legislative Research Analyst

MONTANA STATE LEGISLATURE

FACIAL VERIFICATION VS. FACIAL IDENTIFICATION

Facial recognition is the process of identifying or confirming an individual's identity through technology from photos, video, or real-time surveillance of their face. Generally speaking, facial recognition systems can be used to accomplish two types of tasks: verification or identification. The underlying technologies are different and designed for different uses. The primary difference between facial verification and facial identification is the type of matching the technology uses: one-to-one matching, or one-to-many.

FACIAL VERIFICATION

Facial verification is the process of determining whether someone is who they declare themselves to be. In this instance, for example, a user sets up a profile for an app or program, such as their smartphone or banking app, and as part of the profile setup, will upload a government-issued ID, take a selfie, and provide other identifying credentials. Then the technology uses a **one-to-one** matching system so when the user logs onto the app, the software takes a selfie of the user, from which a biometric template is created and compared with the stored image of the person. A proper match, based on an accuracy score, confirms the user's digital identity, completes the secure authentication process in the background, and opens the app for the user. Facial verification is typically used for personal applications, such as unlocking a smartphone or apps, boarding an airplane, authorizing purchases and other payments, and for facial recognition employee timeclocks.

FACIAL IDENTIFICATION

Facial identification, on the other hand, uses **one-to-many** matching technology and is more prevalent for use by law enforcement, retailers, schools, casinos, and other large crowd events or centers where there is need for surveillance for safety reasons. Facial identification software compares an unknown face taken from a photo, video, or surveillance camera and compares it to known faces in a database. A "match" or "no match" determination is made, depending on if the facial signature[1] of the individual matches one of the images stored in the database.

[1] A "facial signature" is a mathematical algorithm that is computed based on facial landmarks that distinguish one face from another. https://www.jumio.com/facial-recognition-vs-facial-authentication/

Facial Verification Use by Department of Corrections & Courts

One example of how facial verification is used in Montana is through the Department of Corrections' contract with Compliance Monitoring Systems, who provides alcohol monitoring systems to several counties within the state. According to Jake Henry, Program Manager for Compliance Monitoring Systems, the alcohol monitoring system uses Automated Facial Intelligence (AFI) software on two programs for their clients:

> The first is the Remote Breath alcohol monitoring device. This is [a] portable breath testing device clients blow into at fixed or random intervals as we set up at the direction of our referring agency. At test time a picture is taken of the client and the AFI attempts to match up the face to the enrollment photo of the client (we do all enrollment photos at our locations and we require identification so we know the client is who we are supposed to be enrolling.) If the photo does not match the enrollment photo it flags it in the system for our team to match up and/or review.
>
> Our other program which uses this is not a device but uses the same software. Our Touch Point Program is used in conjunction with some clients on electronic monitoring and/or as a stand alone program. It is an application the client downloads on their phone and "checks" in answering a set of designated questions we determine (i.e. have you changed phone numbers, any consumption of alcohol, etc.), and then they take a picture of themselves and it pulls a GPS point from their phone. The picture goes through the same process to be matched up as the remote breath. Again, anything that does not automatically match up we review.

The AFI software is an example of facial verification using one-to-one matching technology. Compliance Monitoring Systems has been providing services to a number of agencies, including the Department of Corrections, several courts, and child and family services, for at least 10 years. Currently between 150-200 clients in the state utilize the software. Mr. Henry stated that the technology allows for more convenience for program members, while giving them a new level of accountability. The remote monitoring device is less intrusive than an ankle bracelet and provides flexibility for the client to still attend work or school without having to physically check in to test at a testing location. It's automated matching technology reduces manual review of photos by 90-95%, resulting in efficiencies in the program, and allowing officers more time to spend on their caseloads and clients.

Sources:

- https://www.jumio.com/facial-recognition-vs-facial-authentication/
- https://www.csis.org/blogs/technology-policy-blog/how-accurate-are-facial-recognition-systems-%E2%80%93-and-why-does-it-matter
- https://partnershiponai.org/wp-content/uploads/2021/08/Understanding-Facial-Recognition-Paper_final.pdf
- https://www.compliancemonitoringsystems.com/services