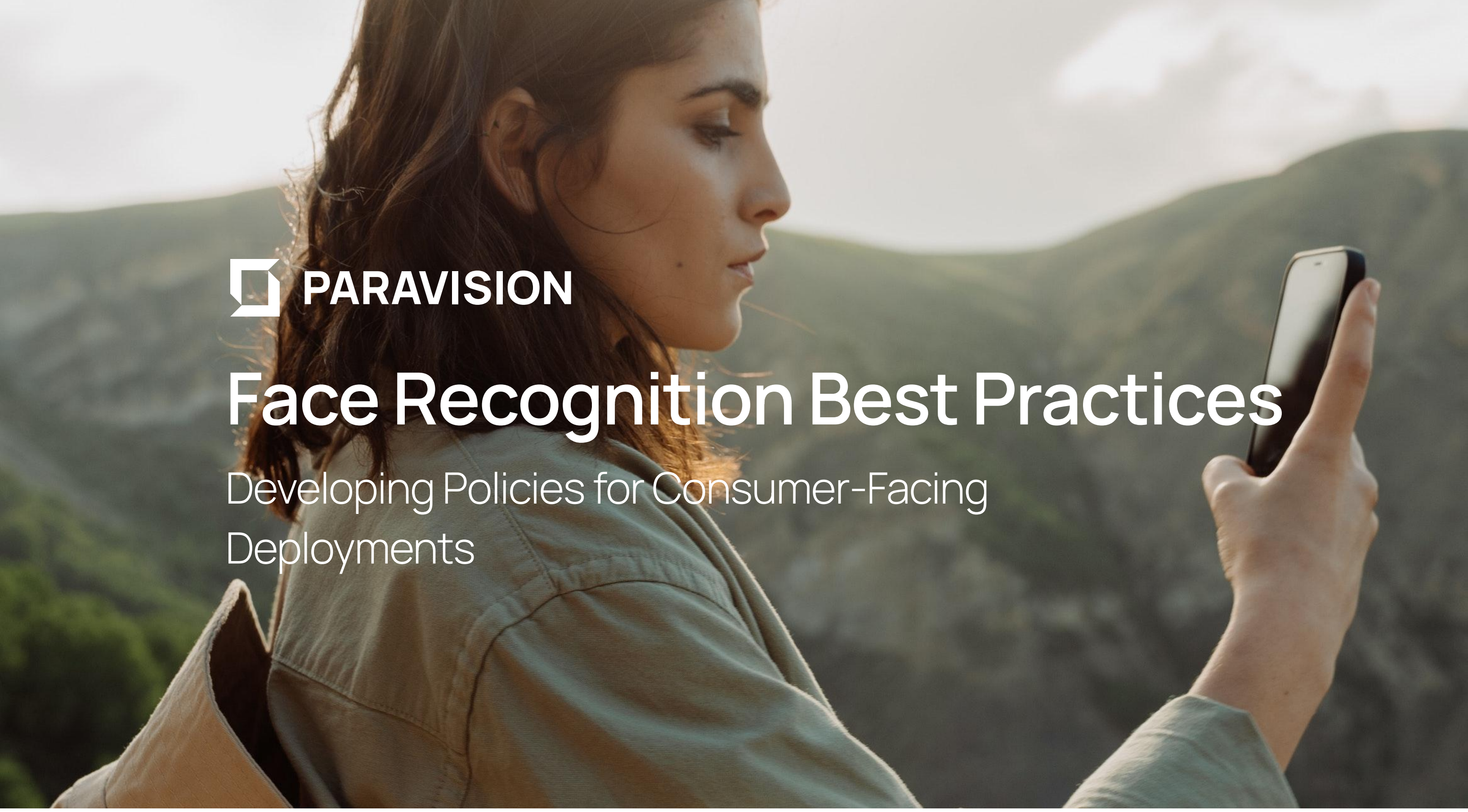

PARAVISION

Face Recognition Best Practices

Developing Policies for Consumer-Facing Deployments

Face recognition can be a powerful and effective tool for frictionless identification and authentication in consumer-facing applications. At the same time, the use of biometric identity demands careful consideration of its impact on privacy, trust, and general feelings of customer comfort. When deployed appropriately, face recognition can enhance the customer experience, improve security, and build deeper customer relationships. These best practices are intended to provide guidance developing policies to enable appropriate and successful deployment of face recognition in consumer-facing applications.

Note

This information is provided for reference only and should not be construed as legal advice. Organizations should consult internal, local, state, or national-level policies, as well as legal counsel, before deploying face recognition technology.

Focus on opt-in and consent-driven use

Opt-in / consent-driven use of face recognition not only puts the service provider on the most stable legal and ethical ground, but it can create a highly effective connection with consumers. Given a choice to engage, a clear articulation of the policies noted below, and an easy-to-understand benefits statement (e.g., "Touchless" or "No wait times"), consumers have shown a real interest in using face recognition for improved services.

Consent to participate should not be passive, but rather express. Wherever possible, consent should be provided in written form, and associated directly with clear delineation of the security, privacy, data use, and data retention policies. In addition, consumers should be aware of the specific uses of their biometric information, and if those uses change over time. Consent should be given both at the time of registration as well as verification / authentication / identification, although in the latter case, written consent may not be feasible or appropriate.

Clearly communicate a security, privacy, data use and data retention policy

Both at the time of enrollment / registration, as well as any time in the future, the security, privacy, data use, and data retention policies should be explicitly articulated.

- *Security* - What measures are being taken to ensure the data being captured will be safe and secure?
- *Privacy and Data Use* - How is personal data being used or shared?
- *Data Retention* - How long is data saved for? If a profile is deleted, what is the process for deleting the biometric data as well?

Provide clear signage around the use of face recognition technology

Although users may have already explicitly opted-in to a program at the time of registration, provide clear signage at the time of authentication / identification that face recognition is being used. This is important both for those who want to use the system and those who have not opted-in or are not aware of the use of face recognition technology. To the extent possible, signage should utilize graphics and imagery as well as text to facilitate understanding regardless of literacy or language barriers.

Provide an effective process for opted-out users and exception handling

The use of face recognition in a consumer setting will typically be driven by a compelling user experience and very likely other benefits such as short wait times and touchless processing. Customers who opt out of the biometric process should be given a reasonable and effective alternative so that they do not feel they are being penalized. In other words, while the face recognition-enabled process may offer a superior experience related to the norm, the non-biometric alternative should be no worse than the norm.

In addition, prepare for ready “human in-the-loop” support for exceptions that may arise due to technology limitations, usability or accessibility challenges, or otherwise.

Provide an easily accessible portal for detailed information about the program and the items listed above

Consumers should be guided toward easy-to-understand documentation regarding the program, including (i) Program benefits; (ii) How to enroll or delete a biometric profile; (iii) The security, privacy, data use, and data retention policy; (iv) Contact information in case of further questions.

Due to the pervasive use of smartphones, a URL with associated QR code is an example of an effective method to guide consumers to this information.

More resources

- https://www.ftc.gov/sites/default/files/documents/reports/facing-facts-best-practices-common-uses-facial-recognition-technologies/121022facialtechrpt.pdf
- http://www3.weforum.org/docs/WEF_Framework_for_action_Facial_recognition_2020.pdf
- https://www.biometricsinstitute.org/biometrics-institute-good-practice-framework/
- https://airc.nist.gov/

For more information, please contact us at info@paravision.ai.