PARAVISION

Key Considerations for Choosing a Face Recognition Partner

Choosing a technology partner for a new capability is a challenging, high-risk process for any business, and the complexity of the technology at hand can make the task overwhelming. Facial recognition is a new capability for many of our partners, and figuring out where to start when choosing a partner can be daunting. To help out, we've gathered some key considerations and criteria for solution providers searching for a partner for face recognition technology.

Is the partner highly trusted and ethical in their processes?

1. Does the partner have a clearly articulated ethics policy?

Because of the ways in which it can be deployed to establish or verify identity, face recognition technology must be handled very responsibly in both development and deployment. All vendors should have a clearly articulated ethics policy for this critical AI technology.

2. How does the partner limit the sale of its technology so that it is not used in problematic applications?

Face recognition vendors should set limits on how, where, and to whom their technology is sold. Vendors should be able to clearly articulate a policy for how they vet their customers and engage in a sale. They should also be able to articulate the technical training that happens along with access to the software to limit technical misuse.

3. Does the partner limit access to their technology or offer a public API?

Service providers should avoid vendors who distribute face recognition technology via public APIs. A public API is typically associated with unrestricted access to technology (with the exception of paying licensing fees) and therefore is inherently more prone to technical or ethical misuse. In addition, public APIs can allow bad actors to train GANs or other malicious AI tools that can be used to undermine deployment security.

4. Does the partner have access to end user data?

In order to best protect security, privacy, and intellectual property, face recognition technology vendors should not have direct access to end user data. Direct access to this data is often integrated with the terms of service of SaaS providers. Ensure that the terms of service does not allow the SaaS technology provider to use any submitted data to train on or otherwise develop new technology, especially if those terms are not explicitly articulated in any end user opt-in. In other words, end users should be made explicitly aware of how their data is used, and if their data can be used for training (which is not recommended) end users should be given an explicit opt-in / opt-out.

Does the partner build technology that performs at the highest level?

5. Is the partner benchmarked in NIST FRVT?

NIST FRVT is globally accepted as the gold standard benchmark for face recognition. Vendors from around the world regularly submit their latest algorithms, which are then tested across large, statistically significant datasets representing a variety of use cases.

Benchmarking in NIST FRVT is critical as it demonstrates the accuracy of submitted algorithms in a statistically significant way, including across types of images and a wide range of demographics. Being able to articulate this level of accuracy to end users is crucial in terms of operational performance and external communications alike. Service providers should be able to point to their face recognition partner with the confidence that they have been vetted.

Because of its unique position as a global test of AI technology, consistent NIST FRVT participation and top-tier performance is frequently a core requirement of RFPs in the public and private sector alike.

6. Does the partner deploy their NIST FRVT-submitted models to customers or are the NIST submissions for laboratory use only?

Some organizations submit algorithms to NIST that are not intended for production deployment. In this way, the published NIST results may suggest an algorithm that is more accurate than what is commercially deployable. Face recognition vendors should be able to commit to the fact that the NIST-tested algorithms are consistent with what is provided to their customers.

Does the partner provide deployment options that fit your tech stack?

7. Does the partner offer on-premises deployment options?

Service providers should have the option to deploy face recognition technology on their own Cloud instances or physical hardware. SaaS-only solutions do not permit the level of security, control, and data privacy that are rightly demanded by end user organizations.

8. Does the partner support all major processing platforms and operating systems?

Face recognition technology should be deployable not only in the Cloud or on-premises, but on leading desktop, mobile, and edge operating systems and chipsets. While the full face recognition solution may not be deployed on an edge platform, offering support for all of these allows service providers to optimize their system for speed, cost, security, flexibility, and user experience.

Is the partner's team easy to work with?

9. You should always feel comfortable and great about working with the partner's team.

Consider how transparent, honest, and flexible the people with whom you have interacted are, and how the company's values align with yours. Having a partner-focused team that's easy to work with helps tackle any future challenges together.

We hope these key considerations help when searching for the best partner for your company. If you'd like to explore a partnership with Paravision, please don't hesitate to reach out.