iProov

Facial Biometric Verification: Ensuring Equitable and Inclusive Access

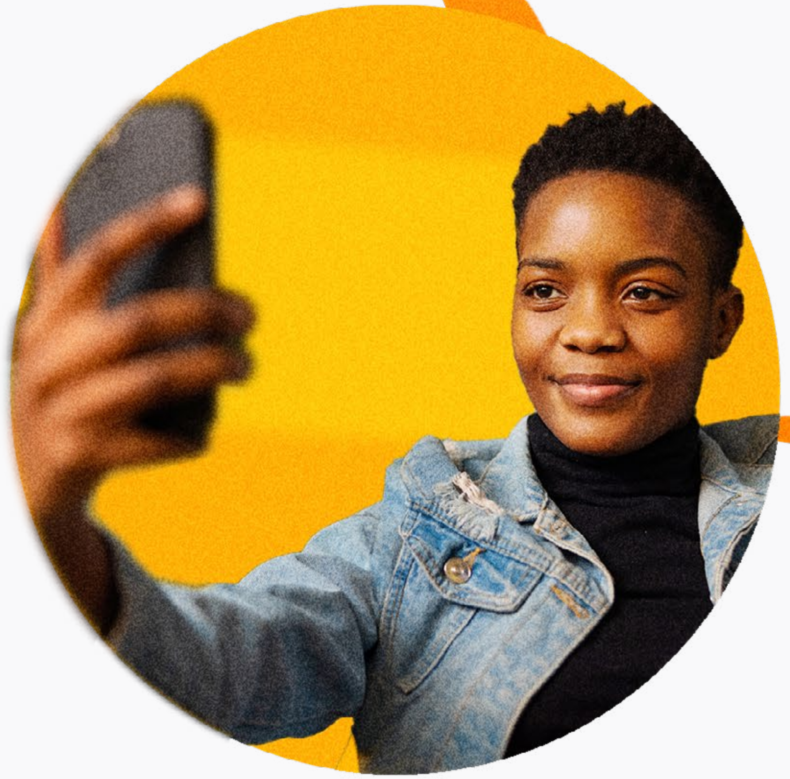
Contents

Introduction

Facial biometric systems are becoming a crucial part of our daily lives. They provide a convenient way to verify and authenticate our identity at home, at work, or on the go. As we continue to move more of our lives online, we have an incredible opportunity to create inclusive digital services. Offering remote access to government and financial services, as well as healthcare, can help not only speed up and enhance efficiency but also improve many people's lives, particularly those with accessibility challenges.

However, as an industry, we must ensure that our platforms are inclusive and accessible. Even a seemingly small 0.5% false reject rate can mean hundreds of thousands in the community are excluded from services. Rejection due to bias in devices, demographics, or cognitive ability leads to negative user experiences. The organization deploying the technology suffers ramifications, such as reputational loss, exclusion, low adoption rate, and even fines.

We must address bias concerns head-on to drive adoption and avoid generating public fear, uncertainty, and doubt. This is especially true for the financial sector and public services, which must make significant efforts to ensure access for everyone.



Web Content Accessibility Guidelines (WCAG) 2.2

The World Wide Web Consortium (W3C) recently published the Web Content Accessibility Guidelines (WCAG) 2.2, the latest standard for digital accessibility. This update introduces nine new success criteria, with the most significant change being the Accessible Authentication criteria (3.3.8). This new guideline prohibits the use of cognitive function tests, such as passwords or puzzles, during any step of the authentication process.

This change has far-reaching implications, as many traditional authentication methods rely on cognitive function tests and are now explicitly incompatible with WCAG 2.2 AA.

> The importance of WCAG compliance cannot be overstated. Approximately 1/5 of the population lives with a disability, and providing accessible digital content is not only a moral imperative but also a legal requirement for many public sector organizations.

Cognitive function tests refer to tasks that require users to remember, manipulate, or process information, such as:

- Remembering a password or PIN
- Performing mental calculations or interpreting patterns
- Solving a puzzle or answering a security question

This guideline’s rationale is that cognitive function tests can be too challenging or impossible for many users to follow, particularly those with cognitive disabilities, memory impairments, or learning difficulties. By prohibiting the reliance on these tests, WCAG 2.2 AA aims to ensure that authentication processes are accessible to a broader range of users.

To comply with the Accessible Authentication criteria, organizations must provide alternative authentication methods that do not rely on cognitive function tests. This could include:

- Biometric authentication, such as facial recognition or fingerprint scanning
- Physical tokens or devices, like smart cards or USB keys
- Third-party authentication services that do not require cognitive function tests

By implementing authentication methods that align with the Accessible Authentication criteria, organizations can create more inclusive digital experiences and ensure that their content and services are accessible to all users, regardless of their abilities or disabilities.

Biometric authentication

Physical tokens or devices, like smart cards or USB keys

Third-party authentication services that do not require cognitive function tests

Why Biometrics?

A Secure and Inclusive Solution for Authentication

Due to the significant amounts of money and personal information involved, bad actors frequently target financial services, the public sector, healthcare, immigration, and humanitarian efforts. Unfortunately, the desire to provide easy access to a wide range of users, coupled with high traffic volumes and the need for rapid decision-making, like in the case of pandemic relief funds, can lead to relaxed security measures and increased vulnerability to fraud.

President Biden's State of the Union address in March 2023 commented on the increased fraud in these sectors. Using biometrics correctly and responsibly can help prevent money from leaving the public purse and flowing to fraudsters. However, for this to be successful, biometric vendors must adhere to best practices throughout their technology's development, testing, and deployment phases to ensure that the system works fairly for all users, regardless of factors such as age, gender, skin tone, camera type, user behavior, or environmental conditions.

Facial biometric technology offers a compelling solution that balances security, accessibility, and inclusivity, surpassing traditional authentication methods like passwords or physical tokens. Moreover, providers that have achieved WCAG 2.2 Level AA conformance demonstrate that secure and inclusive authentication is achievable without relying on cognitive function tests.

The advantages of facial biometrics for remote verification and authentication are manifold:

01 Convenience: Users don't need to remember complex passwords or carry physical tokens, making the authentication process more user-friendly and accessible.

02 Security: Facial biometrics are unique to each individual and cannot be easily replicated or stolen, providing a higher level of security compared to passwords or possession-based methods.

03 Inclusivity: When designed and implemented correctly, facial biometric systems can be used by many individuals, regardless of their technical expertise or physical abilities.

04 Scalability: Facial biometric verification can be easily scaled to accommodate large numbers of users and transactions, making it suitable for applications in government services, financial institutions, and healthcare.

05 Remote access: Across devices with front-facing cameras - facial biometric verification enables secure remote access to services, which is particularly important given the increasing demand for digital services.

As we navigate the digital transformation of critical services, we must demand solutions that prioritize both security and accessibility without any trade-off. Facial biometric verification, when implemented responsibly and in compliance with WCAG 2.2 AA standards, offers a path forward while actively addressing bias and inclusivity concerns.

Organizations can create secure, convenient, and accessible digital services that benefit a wide range of users. This holistic approach is needed to foster trust, drive adoption, and ensure no one is left behind in the digital transformation of critical services.

Identity is a Human Right

“850 million people worldwide lack legal identity”

UN Sustainable Development Goal 16.9: Legal identity for all by 2030

The Impact of Generative AI:

Driving Urgency

There has been a sudden surge in the use of generative AI-based deepfakes and face swaps against remote identity verification methods, including video identification[1] (remote person-to-person call verification).

The evolving threat landscape has compelled organizations to reassess their security posture. Malicious actors, armed with easily accessed advanced technologies (and determination), have effectively redefined the boundaries of cybersecurity threats. This paradigm shift necessitates a heightened level of security measures and resilient defenses to safeguard against these novel adversaries and mitigate the risks they pose to organizational assets and operations.

According to iProov's threat intelligence[2], face swaps (a form of deepfake) increased by 704% in the second half of 2023. This form of synthetic media fed into a camera stream during a remote identification transaction has a higher success rate when the process is escalated to a human operator. Independent research has supported this, finding that human-operated video identification systems are easily overcome with basic everyday approaches.

Unsurprisingly, vendors are rapidly developing solutions claiming defensive capabilities that can analyze details imperceptible to humans. But what impact does this have on user experience?

If you tighten security, could the bar be set so high that genuine users find it difficult to access?

Vendors ramping up security without applying the same dedication to bias mitigation run the real risk that legitimate users, along with some bad actors, will be blocked out. Security professionals need to thoroughly vet vendor claims and implement facial biometric solutions that lock down security while proactively reducing bias. If they don't strike this balance, they could undermine the fundamental purpose of the technology, damage trust with their end users, and risk the organization's reputation.

As the threat landscape evolves, it's crucial that bias mitigation processing, algorithms, and testing are continually updated to ensure inclusivity while still remaining secure. Doing so can create a more inclusive and accessible world where technology empowers people rather than hinders them.

This report serves as a comprehensive guide to help organizations select facial biometric verification solutions that deliver robust security and seamless user experiences while proactively mitigating risks of bias to ensure equitable, inclusive access for all.

[1] *https://edition.cnn.com/2024/02/04/asia/deepfake-cfo-scam-hong-kong-intl-hnk/index.html*
[2] *https://www.iproov.com/press/new-threat-intelligence-report-exposes-impact-generative-ai-remote-identity-verification*

Use Cases Requiring Inclusive Biometrics

Deploying inclusive facial verification with active bias mitigation is critical for organizations to combat fraud, reduce costs, and maximize digital service accessibility.

01 Access to Financial Systems: In 2022, the World Bank reported that 76% of adults globally had access to some form of financial tools[3], such as a bank account or lending service. While access has improved significantly, bad actors can still target those excluded by using their identities to open fraudulent accounts online. Equitable facial verification helps expand financial inclusion securely.

02 Access to Public Sector Services: Government agencies have a statutory responsibility to deliver accessible services to all. They must be able to rapidly and reliably authenticate recipients to distribute funds, benefits, and services to those in need. Complex identity-proofing flows increase risks of discrimination or exclusion of vulnerable groups. Digital transformation failures lead to reverting back to expensive and error-prone manual remote verification.

03 Healthcare: Telehealth offers significant global benefits, improving access to care for billions in underserved areas. During the COVID-19 pandemic, telehealth usage surged worldwide, with some countries reporting increases of up to 154%[4]. Studies from various nations show that telehealth can reduce hospital admissions by 38%[5] and readmissions by 31%[6]. By optimizing provider resources, telehealth can improve the efficiency and cost-effectiveness of healthcare delivery globally.

[3] *https://www.worldbank.org/en/publication/globalfindex/Report*

[4] *https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2020.556720/full*

[5] *https://www.bristol.ac.uk/media-library/sites/primaryhealthcare/migrated/documents/unplannedadmissions.pdf*

[6] *https://doi.org/10.1371/journal.pone.0071238*

To remotely authenticate a user's identity, an organization needs a combination of three things: Knowledge (something they know), Possession (something they have), or Inherence (something they are). Biometric technology has become a popular authentication method, as it falls under the "something you are'' category - regarded as the most convenient and secure method. It is impossible to forget or lose your finger or face, unlike a password or a physical token, which can be easily:

- lost (physical key cards/phones)
- exploited (One-time passcodes)
- written down (complex passwords).

Facial Biometric Verification can be used alone during the identity proofing process or effectively as a multi-factor authentication (MFA) method in a step-up authentication environment.

However, it is essential to acknowledge that not all facial biometrics are created equal. They can vary significantly, not only in terms of the levels of assurance they provide but also in terms of their accessibility and ability to address bias.

The Cost of Not Getting It Right

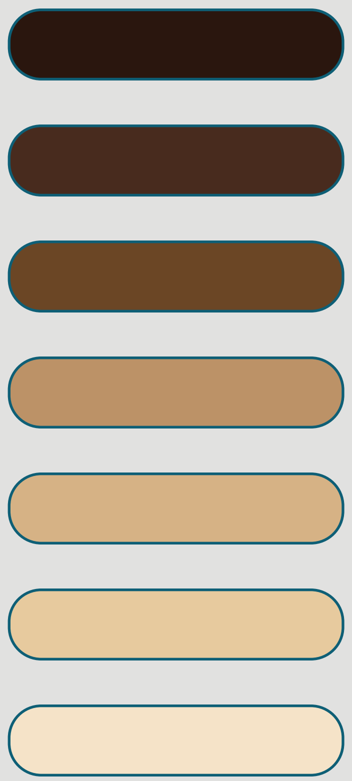
Organizations often find it challenging to determine how to assess whether a vendor is implementing bias mitigation best practices. While there are many certifications and standards to be met, it can be difficult to know which ones are relevant or even beneficial to mitigating bias in facial biometric systems.

Key studies have explored the potential bias that can be found in systems if they have not been designed, deployed, or maintained. Despite this, there are still instances where this guidance is not followed, and the ramifications are meted out:

Racial and Ethnic Bias:

In 2020, Uber faced a lawsuit alleging that its facial recognition system for driver identity verification discriminated against people of color, leading to the wrongful termination of drivers' accounts (Popa, 2020).[7]

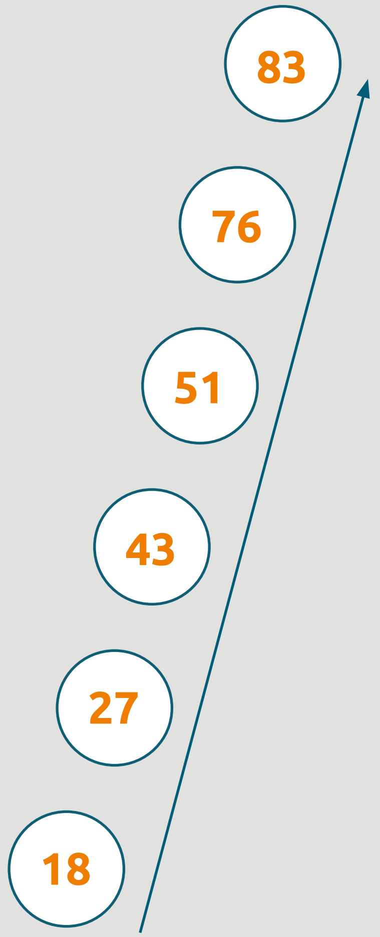
Repercussions: Legal challenges, public backlash, and damage to the organization's reputation. In addition to Facebook's $650 million settlement, companies like IBM, Amazon, and Microsoft have faced criticism and potential loss of contracts due to bias concerns in their facial recognition technologies (Heilweil, 2020).[8]



Age Bias:

In 2021, the Australian Human Rights Commission released a report highlighting the potential for age discrimination in the use of facial recognition technology, particularly in employment and access to services (AHRC, 2021).[9]

Repercussions: Customer complaints, regulatory scrutiny, and potential fines for violating age discrimination laws. Companies using biased facial recognition systems (including facial verification) could face legal action and financial penalties under laws such as the Age Discrimination in Employment Act (ADEA)[10] in the United States.

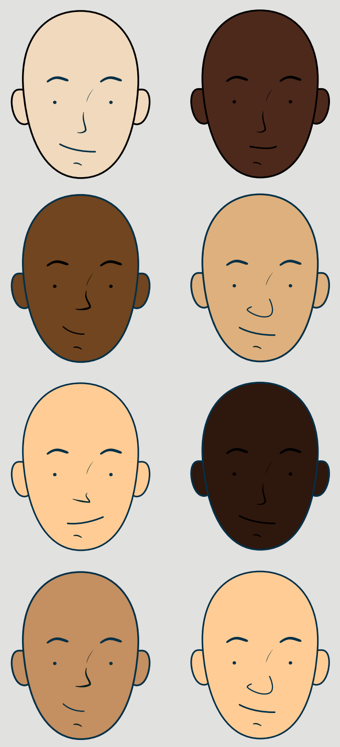


[7] https://www.autoevolution.com/news/uber-faces-lawsuit-over-facial-recognition-systems-used-to-identify-drivers-150846.html
[8] https://www.vox.com/recode/2020/6/10/21287194/amazon-microsoft-ibm-facial-recognition-moratorium-police
[9] https://tech.humanrights.gov.au/sites/default/files/2021-05/AHRC_RightsTech_2021_Final_Report.pdf
[10] https://www.eeoc.gov/age-discrimination

Bias in Training Data:

In 2019, a study by the National Institute of Standards and Technology (NIST) found that many facial recognition algorithms had higher error rates for people of color, particularly those with darker skin tones, due to biased training data (Grother et al., 2019).[11]

Repercussions: Increased scrutiny from civil rights organizations, potential legal challenges, and reputational damage. The Algorithmic Accountability Act, introduced in the U.S. Congress in 2019, aimed to address bias in algorithmic systems, including those used for facial recognition (U.S. Congress, 2019).[12]



Environmental and Lighting Bias:

Repercussions: Poor user experience, increased customer support calls, and potential loss of market share to competitors with more inclusive technology. Large corporations have faced criticism for the performance of their facial recognition systems for users with darker skin tones.[13]

These examples demonstrate the wide-ranging consequences of bias in facial recognition systems, from legal challenges and financial penalties to reputational damage and the erosion of public trust. As the use of this technology continues to grow, organizations must prioritize bias mitigation and partner with vendors committed to developing equitable and inclusive solutions. Failure to address bias not only harms individuals and communities but can also result in significant financial and legal repercussions for organizations.

[11] https://doi.org/10.6028/NIST.IR.8280
[12] https://www.congress.gov/bill/116th-congress/house-bill/2231
[13] https://proceedings.mlr.press/v81/buolamwini18a/buolamwini18a.pdf

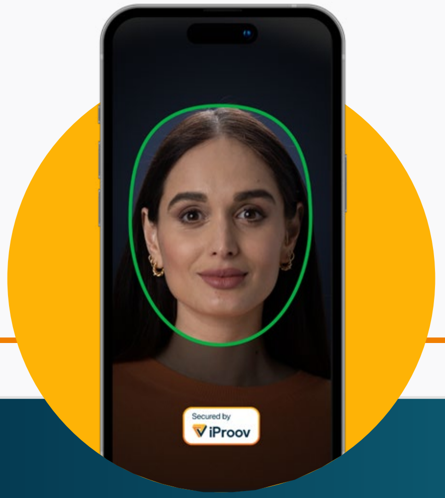
Recognition vs. Verification

Balancing Automation and Manual Processes for Optimized Bias Mitigation

Automated remote identity verification systems present compelling advantages, such as consistency, efficiency, and accuracy, mitigating the potential for human operator bias. Well-maintained systems offer standardized assessments and streamlined workflows, reducing the risk of errors associated with manual oversight or fatigue.

So, where do humans enter the equation? The Carnegie Council for Ethics in International Affairs[14] states that the ‘ human in the loop’ concept, which suggests that humans should supervise and make decisions alongside AI, is flawed. The article uses the example of Stanislav Petrov, who prevented a nuclear disaster, to highlight that humans may not have the technical skills needed to make the correct decisions in real-time. Specialized skills are required for these tasks.

When used responsibly and in conjunction with facial biometrics, automation with expert oversight presents opportunities to identify and mitigate human biases in a way no ‘human only’ environment would be able to measure, improving ongoing performance.



Face Verification:

Face verification is a process where the user:

- **KNOWS** the process is happening
- **COLLABORATES** with the process
- **BENEFITS** from the process
- Is assured of **PRIVACY** protection

Face Recognition:

Face recognition is a process where the user:

- **DOES NOT KNOW** the process is happening
- **DOES NOT COLLABORATE** with the process
- **DOES NOT DIRECTLY BENEFIT** from the process
- Has no control of **PRIVACY**

[14] *https://www.carnegiecouncil.org/media/article/7-myths-of-using-the-term-human-on-the-loop*

Key Considerations for Organizations

By prioritizing inclusivity by design, organizations can leverage facial verification's benefits while avoiding pitfalls. Achieving minimal bias levels in facial verification solutions requires a multifaceted strategy implemented by the vendor, spanning data practices, algorithms, testing processes, transparency, and human oversight.

The following are best practices for automated algorithms with expert human oversight.

01 Diversity in Training Data:

The issue of bias in algorithms often stems from the underlying data rather than the algorithms themselves. Researchers distinguish between the trainer algorithm, which can be biased by the data it is trained on, and the screener algorithm, which makes predictions based on the trainer.

Biases can be introduced through the data used for training, such as reflecting societal inequities or historical biases. Data collection methods, variable choices, and user-generated data can also contribute to bias in algorithms. It is crucial to understand and measure fairness in algorithmic decision-making processes to address and mitigate bias effectively.

Furthermore, diversity within training data helps to ensure that biometric systems do not exhibit significant bias. Training data that is biased towards a particular ethnicity or gender can result in inaccurate verification of individuals from underrepresented groups. The more diverse the data, the more accurately the system can authenticate and verify individuals from all demographic groups. A training group of one hundred, for example, will not yield the same results when live and being used by hundreds of thousands. That being said, it is not necessary to manipulate the data to achieve equal representation - for example, not all users in Thailand will have the same skin tone or features - but it is important that diversity exists naturally in a region where deployment will occur.

Organization key takeaway: Organizations should seek out vendors that use diverse datasets for training purposes, gathered via ethical data collection methods that respect privacy and consent. More recently, generative AI has played a positive role in enabling biometric technology to enhance inclusivity by generating larger, more diverse training datasets.

02 Testing for Equality:

Government agencies have a statutory responsibility to deliver accessible services to all. They must be able to rapidly and reliably authenticate recipients to distribute funds, benefits, and services to those in need. Complex identity-proofing flows increase risks of discrimination or exclusion of vulnerable groups. Digital transformation failures lead to reverting back to expensive and error-prone manual remote verification.

Organization key takeaway: Vendors should not infringe on personal information or use testing to discriminate against individuals or groups. If the testing reveals evidence of bias, vendors must take immediate action to refine algorithms, update training data, and implement changes across their technology.

03 Transparency and Vendor Accountability:

Organizations need to work with transparent facial biometric vendors who are open and honest about their testing procedures, how often they test, and how they measure and track biases. To help build trust, customers should have a clear understanding of how the process works and any potential biases.

Detailed records of testing methods, results, and any measures taken to address biases should be maintained and readily available to customers and relevant authorities. Furthermore, vendors should educate their customers about the significance of their testing, enabling customers to make informed decisions.

Biometric vendors vary in their approaches. While some rely on third-party face-matching providers, others depend on the National Institute of Standards and Technology (NIST) for guidance. Additionally, the presence of bias can introduce challenges in the facial matching and liveness detection components. For instance, a vendor could encounter biased data that differs from spoof detection datasets. This underscores the importance for organizations to diligently verify and cross-reference multiple sources of data to ensure accuracy and mitigate bias across the entire solution offering in their analyses.

Organization key takeaway: Request comprehensive bias performance reporting, including third-party audit reports, as well as industry certifications, such as WCAG 2.2 AA. These provide external validation of a vendor's commitment to inclusion and help verify their solutions meet accessibility requirements. Read more examples here.

04 Continuous Monitoring:

Continuous monitoring of biometric systems is crucial to identifying and mitigating biases. Given the ever-changing threat landscape and frequent defense updates, ensuring no new bias has crept in should be a regular practice. In addition, quarterly reports help prompt the identification and implementation of new training data built into algorithms.

The ability to continuously monitor performance enables vendors to be proactive in preventing any bias as soon as it manifests. Static systems simply do not have this capability. It is unacceptable for organizations striving to deliver equitable and accessible solutions to have to wait for the next scheduled update in order to improve performance.

Organization key takeaway: Request evidence of ongoing bias performance reports, which should carried out at least every three months, and what processes are in place to spot and address potential bias.

Transparent Performance Reporting: Organizations should insist on transparency around vendors' bias testing processes, methodologies, and results. Look for detailed performance reporting across demographic subgroups. In addition, look for vendors that collaborate with experts in the field, regulatory bodies, and advocacy groups to improve their processes and continuously address emerging bias-related challenges. Maintaining detailed records builds accountability.

Real-World Impacts of Equitable Facial Verification

The benefits of equitable, inclusive facial biometric verification are tangible across sectors:

Finance and Banking: **Major institutions like UBS have increased financial inclusion rates in underserved regions through secure, remote client onboarding that avoids demographic discrimination. In fact our Digital Identity Report found that: 64% of mobile banking customers either already use face authentication to access their account, or would do so if it was offered.**

Public Services: **Government agencies across Europe, the Americas, and APAC are enabling more equitable citizen access to telehealth, education, benefits programs, and other vital digital services regardless of demographics or abilities.**

Healthcare: **A 2021 study by PWC found that 72% of patients were comfortable using biometrics for telehealth[15]. Moreover, 82% of healthcare providers reported that biometric verification improved patient identification accuracy and reduced fraud risks[16]. By offering a robust and user-friendly authentication solution, facial biometric verification has become an essential tool in the rapidly growing telehealth market, which is expected to reach 455.3 billion by 2030, with a compound annual growth rate (CAGR) of 24.3% from 2024 to 2030[17].**

In a 2023 survey, two-thirds of organizations believe biometric solutions to be more inclusive than OTP systems, multi-factor authentication, and CAPTCHAs.[18]
As face biometric technology becomes a protector of digital accounts and services globally, organizations have an ethical obligation to prioritize inclusivity and equity in tandem with security and fraud prevention. By following the practices outlined, they can implement facial biometrics responsibly to empower and include all user groups.

[15] *https://www.pwc.com/us/en/industries/health-services/virtual-health.html*
[16] *https://healthtechmagazine.net/patient-centered-care/telehealth*
[17] *https://www.grandviewresearch.com/industry-analysis/telehealth-market-report*
[18] *Hanover Biometric Solutions Inclusivity Study 2023*

iProov’s Approach to Inclusive Facial Biometrics

iProov harnesses automated identity verification processes that are bolstered by real-time monitoring and analysis from cybersecurity and biometric science experts. By integrating science, policy, and compliance, iProov enhances operational practices and establishes ethical standards that reduce bias in systems and human decision-making. This human expertise encompasses dedicated in-house ethical hackers and threat intelligence teams, ensuring a mission-critical level of security. This approach empowers organizations to leverage secure, inclusive, and privacy-respecting biometric technology, reaping the full benefits while maintaining user trust.

While advanced machine learning underpins our facial verification, we judiciously integrate this human expertise through processes such as:

- Dedicated AI ethics review boards and councils
- Diverse “human-in-the-loop” edge case review workflows
- Continuous human monitoring for emerging biases or novel attacks
- Subject matter experts in science, threat intelligence, and penetration testing

This human-AI collaborative approach enhances accuracy while reinforcing responsible development practices in line with ethical AI principles. Our performance is optimized using advanced bias detection and mitigation techniques. Expert testing occurs quarterly at minimum to validate equitable performance across key demographics like age, gender, and skin tone. We maintain detailed records and are fully transparent with our customers about our methodologies and results.

Our facial biometric verification solutions prioritize inclusivity from the ground up, as validated by industry benchmarks like eIDAS certification and WCAG2.2 AA compliance. WCAG, or Web Content Accessibility Guidelines[19], is a set of recommendations for making web content more accessible to people with disabilities. WCAG 2.2 AA is the latest version of these guidelines, providing specific criteria for accessibility across various levels of conformance. Compliance with WCAG 2.2 AA is crucial for public sector organizations, as it ensures digital content accessibility for citizens with disabilities and meets legal requirements. The UK government and EU Web Accessibility Directive 2016 mandate WCAG compliance for public sector websites and applications, with the UK monitoring new WCAG 2.2 criteria starting October 2024. Read more about how this impacts some facial biometric technologies here.

[19] *https://www.w3.org/TR/WCAG22/#:~:text=Web%20Content%20Accessibility%20Guidelines%20(WCAG)%202.2%20defines%20how%20to%20make,%2C%20learning%2C%20and%20neurological%20disabilities.*

Conclusion

As industries depend on digital services globally, underlying identity verification technology should not exclude certain demographics. Therefore, it is critical that facial biometrics are implemented to empower everyone. Organizations should partner with vendors committed to achieving this vision.

We firmly believe that implementing inclusive facial verification not only aligns with ethical standards but also drives business success. By prioritizing equitable access, organizations can securely onboard more users, increase revenue, reduce overhead costs from manual reviews, minimize regulatory risks, and build further trust with their audiences.

Transparency is key; organizations need to be assured of the steps the vendor is taking to promote inclusivity and mitigate bias in their systems. Regular reporting and feedback from organizations can foster this two-way relationship.

Laws and regulations surrounding facial biometrics are changing quickly. It's crucial to check for the most up-to-date information in your specific jurisdiction. Mere vendor claims alone do not provide sufficient assurance of conformance or that the system is unbiased across diverse user groups.

Facial biometric technology can deliver high assurance against new and evolving threats, as well as support inclusivity. Ultimately, implementing inclusive facial biometric verification aligns with ethical standards and drives business success by enabling secure onboarding of a broader user base, reducing overhead costs, minimizing regulatory risks, and fostering a more equitable digital ecosystem.

Industry Perspectives

“As Africa’s leading provider of enterprise-grade Identity Verification (IDV), diversity and inclusivity has not only been a business priority for us but a non-negotiable aspect of our platform’s design. This is because accessible and secure identity is a powerful enabler to essential financial, government, and healthcare services. The World Bank’s Identity for Development (ID4D) report shows that the majority of the 850 million people without official identification live in low-income (LIC) and lower-middle-income (LMIC) economies in Sub-Saharan Africa and South Asia, so addressing this through accessible remote face identification is a priority for us.

iiDENTIFii’s facial recognition algorithm has been trained on over 50M African ethnicities, making it designed for inclusivity. The platform is available on a range of devices of varying sophistication, and users can switch between authenticating on a mobile to a desktop device. This makes it inclusive by design. Remote face verification as a technology is innately more inclusive, as it doesn’t require the physical abilities needed for technologies such as wink-and-blink or voice biometrics.

Leading with a focus on equity and accessibility has had a positive impact on our business outcomes, primarily because banks and governments in South Africa and beyond are working hard at bridging the gap between those with and those without identification.”

– Gur Geva, Founder and CEO at iiDENTIFii

“Biometrics are a key tool for businesses in fighting fraud and providing a frictionless user experience; it is the present and future of authentication. However, when designing biometric solutions it’s important to start with inclusivity at the forefront.

One aspect of this is designing the technology to be accessible for all from a UX perspective, taking into account groups such as the aged or those with physical disabilities. Biometrics solutions should also seek to reduce any negative impact based on race or gender. Some studies have shown that facial biometric technologies can be biased, for example, depending on the user’s skin tone.

Incorporating liveness capabilities further enhances the effectiveness of facial biometrics in combating emerging threats while helping to reduce bias or accessibility barriers. By adopting inclusivity in the design process, we can ensure we have systems in place that work for all users.”

– Jason Howard, CEO, caf.

iProov

Inclusive access is a priority:

Can facial biometrics work for everyone? Hanover Research, commissioned by iProov, examines accessibility challenges and privacy concerns.

HANOVER RESEARCH

BIOMETRIC SOLUTIONS INCLUSIVITY STUDY

Prepared for iProov

December 2023

Download Now