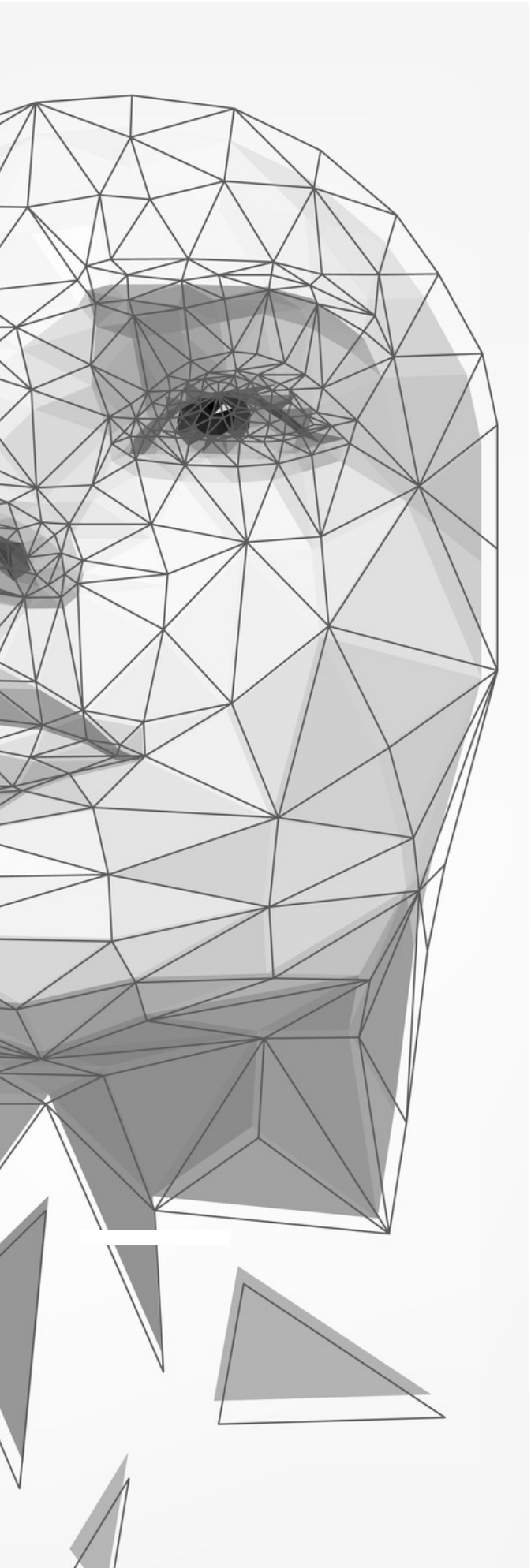
iPROOV

CLEARING UP THE FACIAL RECOGNITION DEBATE

IDENTIFICATION VS AUTHENTICATION

KENDEL RUPPERT, OCTOBER 2019



SUMMARY

Face biometric technology is commonly grouped under the catchall phrase of 'Face Recognition.' However, there is a critical distinction between 'Identification' and 'Authentication.'

Facial Identification technology aims to increase human efficiency, often utilised in surveillance settings to aid in identifying a face in a database or a watchlist of individuals. This is known as a one-to-many search. This use of Face Recognition for surveillance has sparked huge privacy and human rights debates due to a lack of legal regulation and grey areas of consent. Facial Identification is often undertaken without meaningful consent and provides no direct benefit to an individual; instead, aiming to promote a safer society overall.

Face Authentication refers to the process of determining if two samples of biometric data match and therefore come from the same person. This is known as a one-to-one match and is often used to allow individuals to voluntarily assert their identity. Examples include: passing through e-gates at airports or setting up bank accounts online remotely.

The use of Face Authentication aims to increase simplicity and usability with human:digital transactions, removing the need for human:human interactions to verify identity.

It is important to note that Authentication is dependent on individuals' consent and exists to provide direct and immediate benefit. However, as Facial Identification and Face Authentication are often both grouped under the same umbrella of 'Face Recognition'... the latter is commonly and unjustly associated with the controversy surrounding Facial Identification.

Here we will illustrate the distinction between Facial Identification and Face Authentication. This article will also demonstrate why the controversy surrounding Identification should not be leveraged against all Face Recognition technology.

INTRODUCTION

'Facial Identification' and 'Face Authentication' certainly sound very similar. Despite having two entirely different applications, the phrases are used interchangeably, and often dubbed as 'Face Recognition' in the press as well as in the biometrics industry. This lack of distinction creates confusion and unnecessary difficulty for businesses looking to implement Face Authentication. In some cases, leading businesses to overlook the benefits of Face Authentication altogether.

To put it simply:Facial Identification asks the question
"Who are you?"

While Face Authentication asks
"Are you who you say you are?"

FACE IDENTIFICATION

WHAT IS IT?

Facial Identification refers to the use of Facial Recognition technology for surveillance in public environments. The aim of this use is to find individuals that have been watch-listed by the Police. Faces in existing Police photos are mapped to create a 'biometric template' which is unique to every individual. Cameras in public spaces scan the faces of civilians and flag possible matches to Police Officers. The purpose of this is to speed up existing human processes. Facial Identification aims to increase officer efficiency, allowing a quicker identification of watch-listed individuals.

Recently, San Francisco legislators banned Facial Identification technology, becoming the first state to do so. (1) But, in the UK, The South Wales Police, Metropolitan Police and Leicestershire Police have used Facial Identification in public spaces since June 2015 (2) with the aim of increasing arrests of wanted individuals. So why is there such huge disagreement and debate around the use of Facial Identification?

UNREGULATED AND UNCHECKED

One worrying point to consider is that there is currently no legal framework for the use of Facial Identification in place, described as a "legal vacuum" by criminal law experts (3).

In the UK, police forces currently govern the use of Facial Identification with so-called "self-restraint." While they claim that data is only retained for those on a police watch-list, there is no legal requirement for the data of innocent individuals to be deleted (4). There is a distinct lack of clarity and inconsistency surrounding the legal limitations of Facial Identification. Begging questions such as:'In which public setting is Facial Identification appropriate?' 'Who controls my captured data?'

"FRT TRIALS HAVE BEEN OPERATING IN A LEGAL VACUUM. THERE IS CURRENTLY NO LEGAL FRAMEWORK SPECIFICALLY REGULATING THE POLICE USE OF FRT."

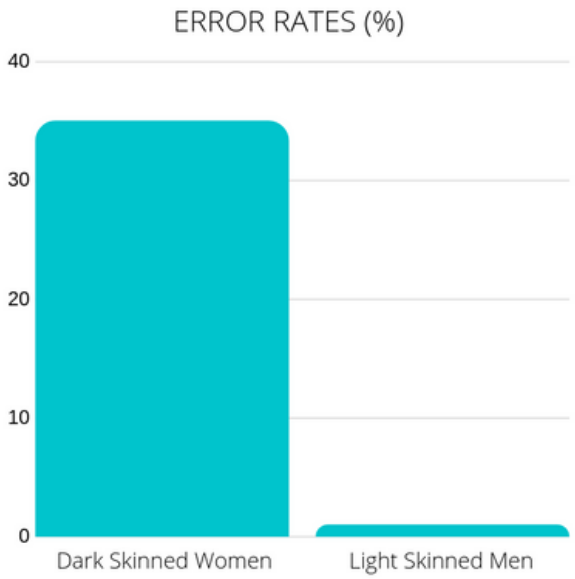
DR JOE PURSHOUSE, UEA SCHOOL OF LAW

PREJUDICED TECHNOLOGY

As Facial Identification matches one image to many (one face from surveillance footage to many faces in a database) there is more room for error than a one to one match. In addition, Facial Identification notoriously experiences problems of gender and racial bias.

Dark skinned women are the most misclassified group, with errors rates of 34.7%, while the maximum error rate for white males is less than 1%. (5)

According to a study by AIES, Facial Identification systems also commonly mistake women for men, in up to 19% of cases. (6) Therefore these groups are much more likely to be wrongly stopped and interrogated. Technology that promotes ethnic and gender bias can lead to unjustified over-policing in some areas as well as the potential to change the nature of public spaces.



THE GREY AREA OF CONSENT

Privacy and consent are two words at the forefront of the Facial Identification debate. Data is captured and utilised without the consent of the individual. This use simply involves the claiming of an identity, without the option for the individual to assert that this is, in fact, their identity (traditionally done with passwords, security questions etc).

A report by *The Human Rights, Big Data and Technology Project* highlights that consenting to Facial Identification "could only be called meaningful if an opportunity existed to make an alternative choice." (7) The report goes on to deem that sufficient alternative choice is not currently provided. Furthermore, the capturing of biometric data in this context also has no direct benefit to the average person.

However, there are cases in which Facial Identification has undeniably positive effects. This is clear when Facial Identification is leveraged to attempt to identify missing persons. One case that received a lot of attention in 2018 was New Delhi Police identifying "nearly 3,000 missing children" (8) within four days of deployment of Facial Identification technology. In this case, the fact that these children did not consent to the use of Facial Identification seems an arbitrary argument.

FACE AUTHENTICATION

WHAT IS IT?

Face Authentication refers to technology that allows an individual to assert a claimed identity. The technology performs one to one matching against an enrolment image and an authentication attempt to deliver a pass or fail result. Critically, the purpose of Face Authentication is not to make a human process more efficient (as it is with Facial Identification), but to remove the need for human process entirely.

One common example of Face Authentication is e-gates at airports that have reduced and will ultimately remove the need for border guards. You scan your passport “I am x” and a face scan takes place “Here is proof.” However, unlike Identification, Face Authentication does not always take place in a public setting such as an airport. Biometrics offer both security and usability and is, therefore, being increasingly adopted for remote, online authentication processes. For example, setting up a new bank account online at home.

CONSENT AND BENEFIT

Face Authentication is a process that is initiated with a user's consent, without consent no biometric data is captured. Further, Authentication delivers direct and immediate benefit to an individual by allowing convenient access to a service. Face Authentication allows you to assert your identity quickly and easily, without the need for in-person checks or reliance on traditional, less secure methods of authentication (e.g. passwords, security questions etc.)

However, although Authentication relies on meaningful consent, this does not mean every individual is comfortable consenting to an authentication process. Many privacy concerned users feel uncomfortable with images of their face being captured at all, whether for Identification or Authentication purposes. Providing alternative biometric modalities to users is therefore vital to promote maximum user comfort. Increasingly, organisations are seeing the value in biometrics as a secure and effortless authentication method for remote online journeys. The mobile biometric authentication industry brought in over 20 billion USD in 2018 alone. (9)

RELIABILITY & REGULATION

To be used commercially, Face Authentication must comply with regulation standards (e.g. GDPR.) Contrastingly to Identification, rather than creating a regulatory uproar, one major use of Face Authentication is regulatory compliance. For example, within the Financial Sector, Face Authentication is increasingly used to comply with KYC, AML and PSD2 standards.

Errors when using highly accurate Facial Recognition algorithms are also far less significant in an Authentication use case. A single Authentication process will attempt to match one image to another, meaning that potential error can

occur in only one instance. A single Identification process matches one image to potentially millions of images. This means there are millions of instances in which an error could occur. Therefore, Face Authentication poses a far less significant risk of misidentification and inconsistency.

THE RISK OF IDENTITY THEFT

Mobile biometrics allows a user to assert their identity any time, anywhere. This convenience is one of the major advantages of biometric authentication. But, it creates a huge issue of trust, especially when dealing with the face. Faces are not an anonymous biometric, most peoples faces are easily searchable on the internet. Faces are arguably the easiest biometric to generate copies, or 'spoofs' of. One recent example of this issue in practice is the Samsung Galaxy S10. The inbuilt Face Authentication is easily spoofed by holding up photos of the phone's owner (10).

Organisations must be sure that not only the **right person** is interacting with their service online...but that they are a **real person** and that they are interacting with a service **right now**.

This is certainly not a problem that Facial Identification experiences. In a public setting, it is obvious if someone is holding a photo over their face. So while liveness and checks that a user is 'genuinely present' is not necessary for Identification, it is absolutely paramount when dealing with Authentication. And it's not just photos that systems must be able to defend against, but the likes of well-engineered masks, DeepFake video and replay attacks.

(11)

ABOUT IPROOV

iProov creates digital trust with biometric authentication. We ensure that online users are genuinely present in uncontrolled environments, combining face biometrics and anti-spoofing. Our unique approach to spoof prevention (covered by 12 granted patents), world-class deep learning technologies and focus on sustainable security have given us an unrivalled global reputation.

We detect and prevent all known identity spoof attack vectors including masks, replay attacks, compromised devices, and - critically - the emerging threat of Deep Fake artificial video.

Customers in Financial services and Enterprise markets have adopted our systems for online logon, step-up authentication, and for remote identity verification based on trusted ID documents. iProov is running in production with a number of major global banks, including ING and Rabobank. iProov is also working with Government organisations including the US Department of Homeland Security and the UK Government.

REFERENCES

(1) Lee, Dave. (2019) “San Francisco is first US city to ban facial recognition” BBC News. [News Article] <https://www.bbc.co.uk/news/technology-48276660>.

(2) Coleman, Clive. (2019) “Police facial recognition surveillance court case starts.” BBC News. [News Article] <https://www.bbc.co.uk/news/uk-48315979>.

(3) University of East Angila (2019) “New legislation needed to regulate police facial recognition technology.” University of East Anglia Press Release. [Press Release] <https://www.uea.ac.uk/about/-/new-legislation-needed-to-regulate-police-facial-recognition-technology>.

(4) Dearden, Lizzie. (2019) “Police free to set own limits on use of facial recognition because law has not caught up, court told.” The Independent [News Article] <https://www.independent.co.uk/news/uk/home-news/facial-recognition-uk-police-legal-challenge-court-human-rights-a8927696.html>.

(5) O'Brien, Matt. (2019) “MIT Researcher Exposing Bias in Facial Recognition Tech Triggers Amazon’s Wrath.” Insurance Journal [News Article] <https://www.insurancejournal.com/news/national/2019/04/08/523153.htm>.

(6) Deborah Raji, Inioluwa. Buolamwini, Joy. “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products.” AIES [Report] <http://www.aies-conference.com/wp-content/uploads/2019/01/AIES-19_paper_223.pdf>.

(7) Fussey, Pete. Murray, Daragh. “Independent Report on the London Metropolitan Police Service’s Trial of Live Facial Recognition Technology.” The Human Rights, Big Data and Technology Project, page 100 [Report] <https://48ba3m4eh2bf2sksp43rq8kk-wpengine.netdna-ssl.com/wp-content/uploads/2019/07/London-Met-Police-Trial-of-Facial-Recognition-Tech-Report.pdf>.

(8) Cuthbetson, Anthony. (2018) “Indian Police Trace 3,000 missing children in just four days using facial recognition technology”. The Independent [News Article] <https://www.independent.co.uk/life-style/gadgets-and-tech/news/india-police-missing-children-facial-recognition-tech-trace-find-reunite-a8320406.html>.

(9) Liu, Shanhong. (2019) “Biometric technologies - Statistics & Facts.“statista, [Article] <https://www.statista.com/topics/4989/biometric-technologies/>.

(10) Gatlan, Sergiu. (2019) “Samsung Galaxy S10 Face Recognition Can Easily Be Bypassed” Bleeping Computer, [News Article] <https://www.bleepingcomputer.com/news/security/samsung-galaxy-s10-face-recognition-can-easily-be-bypassed/>.

(11) Image rights belong to <https://www.youtube.com/watch?time_continue=240&v=BGgQ9woZQOg>.