Should we ban facial recognition?

Introduction

The debates around the use of facial recognition and whether the technology should be banned show no signs of slowing. In May 2019, San Francisco became the first US city to ban its use for police and other agencies [1]. Later that year, Australian parliament's intelligence and security committee rejected laws to establish a national facial recognition database, recommending that the legislation be completely overhauled, with a focus on privacy, transparency and robust safeguards [2]. The European Union discussed the issue in January 2020 but ultimately decided against a ban, leaving the decision to individual member states [3]. Both democrats and republicans have introduced bills banning the use of facial recognition by federal agencies, with some calling for the formation of a commission to govern its use [4].

However, a one-size-fits-all approach to a ban would risk eliminating high value applications of facial recognition like national security at borders, finding lost children or uncovering identity fraud.

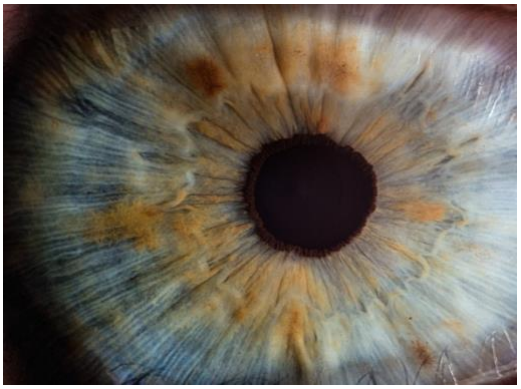
This paper aims to demystify some of the confusion regarding facial recognition technology and its different uses as well as to represent the views of some of our stakeholders on the subject of whether a ban or moratorium is what we need, right now.

Why this paper is important:

- The Biometrics Institute promotes the use of biometrics but only if used responsibly and ethically
- Biometrics are complex, different use cases present different levels of risk which need to be assessed, planned and managed carefully
- Using biometrics responsibly, requires informed decision-making. The institute provides unique tools like the *Three Laws of Biometrics*, its *Good Practice Framework* and *Privacy Guidelines* to work through the decision-making process
- The institute is well placed to provide these tools and accompanying guidance as the independent and impartial international membership organisation representing a diverse multi-stakeholder community

Background

Biometrics is the physiological measurement of fingerprints, face, iris, voice, gait and other distinguishing aspects of the human body.



Iris, fingerprints and voice are among the measurable, distinguishing biometrics

The explosive growth of biometrics in the United States began in response to the terrorist attacks on 11 September 2001 in New York and Washington DC. Although fingerprints had been used by law enforcement around the world for hundreds of years and have been considered very accurate, using biometrics for border control, passports, national identity registration and private sector applications generally started in the noughties. With the advent of Apple's use of the fingerprint to unlock its

iPhone in 2013 and the transition to facial recognition in 2017, the convenience of using biometrics became part of many people's everyday lives. Over the past two years facial recognition algorithms have improved so much that many algorithms are achieving similar levels of accuracy to fingerprints within the context of identity management.

Recent events

The New York Times reported disproportionate use, a lack of transparency, and security concerns at the beginning of 2020 [6]. It discovered a United States-based biometrics company, Clearview AI, had been scraping the facial images of billions of people from Facebook, YouTube and Twitter without permission. The searchable database it created and its facial recognition system has been sold to law enforcement agencies across America and other countries.

In January 2020, a Detroit man was falsely arrested and detained for over 30 hours due to an erroneous interpretation of a live facial recognition system [7]. The prosecutor apologised but said, 'This does not in any way make up for the hours that Mr Williams spent in jail.'

Several cities in the United States, including San Francisco, have banned the use of facial recognition technology. California, Oregon and New Hampshire have prohibited the use of police body-worn cameras state-wide [8]. And the US bill would temporarily restrict federal government use of the technology until legislation is passed to regulate it. Washington state has taken a more balanced view, being the first to implement new laws to curb facial recognition technology [9]. The new law demands government agencies obtain a warrant to use the technology and stipulates training and public reporting around its use.

Big names in the private sector are supporting calls for regulation of facial recognition technology too. In November 2020, Microsoft President Brad Smith congratulated President-Elect Biden, writing in his blog [10], 'When it comes to issues such as safeguards for facial recognition, we have no national law at all. We need new laws fit for the future.'

Whether police were lawful in using biometrics was debated in UK courts

In the UK, the lawfulness of police use of biometrics as a surveillance tool has been tested in court. The High Court initially ruled in favour of South Wales Police's use of live facial recognition technology in public spaces. But later in 2020, the ruling was overturned by the Court of Appeal in favour of Ed Bridges who argued his privacy had been violated [11]. Its verdict was that the use was unlawful and did not comply with the European Convention on Human Rights. However, the Court of Appeal did agree with the initial ruling that the use was proportionate interference with human rights and the potential benefits outweighed the impact. This case in particular demonstrates the importance of rigorous processes when using facial recognition technology.

In London, the Metropolitan Police has deployed live facial recognition to help officers identify both perpetrators and victims of gun and knife crimes, child sexual exploitation and other criminal acts. In 2020, Commissioner Cressida Dick defended the use saying, 'It is for the critics to justify to victims of crimes why police shouldn't use tech lawfully and proportionately to catch criminals.' [12]

In 2019, the independent London Policing Ethics Panel [13], set up to advise the London Mayor, said while there were 'important ethical issues to be addressed' these did not amount to reasons not to use the technology. It advised that the force 'proceed with caution' and to ensure robust internal governance was in place for every deployment.

Swedish Police asked the country's Data Protection Authority (DPA) if it could use facial recognition technology under existing laws. It was given the go ahead with the DPA saying the technology is 'far more effective' at identifying criminals but stipulated that the force should decide how long it needed to store data before it implemented the technology.

In October 2020, the French DPA, CNIL, provided guidance on the use of facial recognition at airports [14]. In 2019, it released a paper exploring the the different use cases and impacts of facial recognition [15] demonstrating an increased awareness of the opportunities and challenges with the technology in a country that had to address terror attacks in Paris in 2015.

The takeaways from these cases are that there are real privacy risks that require adequate controls. Biometric technology is probabilistic and is not always completely accurate. Errors can impact on personal rights and freedoms and need to be managed and addressed from the outset.

Humans also have difficulties identifying individuals and significant decisions should always be made by authorised and skilled individuals with the support of process controls and robust governance.

What has led to calls for a ban?

Facial recognition, just like fingerprint comparison, depends on algorithms – a mathematical model that varies with each individual system. There are about 200 different algorithms for facial recognition. Not all algorithms perform the same, and not all countries or suppliers use it in the same way.

Facial recognition depends on algorithms – not all algorithms perform the same

In December 2019, the National Institute of Standards and Technology (NIST) released a report on the demographic effects of facial biometrics [16], commonly referred to in the media as 'bias'. It found that not all facial recognition algorithms perform the same way [17] and that the best algorithms gave 'absolutely low' false non-match rates.

However, the report found that contemporary facial recognition algorithms exhibit demographic differentials of various magnitudes. False positive differentials – where a person is wrongly accepted – are much larger than false negative differentials – where a person is wrongly rejected. False positive differentials exist broadly, across many, but not all, algorithms tested. The report found that in the most accurate algorithms, variances were significantly smaller or negligible.

Patrick Grother, co-author of the report, said, 'While it is usually incorrect to make statements across algorithms, we found empirical evidence for the existence of demographic differentials in the majority of the face recognition algorithms we studied.'

Media articles focused on the differences in accuracy between ethnicities and genders. The report did find that women produce higher false non-match rates. However, this was described as a 'marginal effect' – with 98% of women still correctly verified. But when coupled with the word bias, this caused a great deal of concern. The focus on so-called bias, when associated with accuracy affecting gender and people of colour, overshadowed the other findings in the report.

The report also found that differing false negative rates existed because of varying degrees of image quality and lighting. With US domestic mugshots collected using a photographic setup specifically to produce high-quality images, false negatives were higher in Asian and American Indians. But using lower-quality US border crossing images, false negatives were higher in people born in Africa or the Caribbean.

UK media reporting of facial recognition trials at the Notting Hill Carnival and major football and rugby events of 2017 and 2018 caused significant confusion about matching capability, with journalists claiming false match rates of 90%. Critical, contextual considerations were not reflected in the reporting. For example that it is the number of checks performed against a watch list that determines overall matching accuracy.

Confusion over these different uses for different purposes has led to a lack of understanding of what facial recognition is, and a generalised fear of the technology without understanding how it works. The societal positives and the benefits – where the technology has helped catch criminals or helped identify patients in third world countries for example – are rarely discussed. Those opposed to its use often continue to cite inaccurate information, discredited media articles, and dated knowledge as to the technology's apparent accuracy and effectiveness.

Constantly-fixed cameras raise questions about proportionality

The concerns

Facial recognition has been generally well accepted by the public where there is a personal benefit in using it. Millions of people are happy using it to unlock their phone or use e-gates and kiosks to fast-track border control. Critics raise issues about using the technology when cameras are permanently fixed and constantly watching a public space, be it a street, railway station, tourist spot or shopping mall.

This raises the following questions:

- Is it proportionate that in seeking to identify one terror suspect or shoplifter, every person's face is collected and processed with the theoretical assumption they might be the wanted person?
- Is proportionality based on the use case? For example is identifying a terror suspect at an airport more important than identifying a shoplifter at a store?
- What does the database being matched against consist of? Does it include people whose misdemeanors are outside the target group? Is it up-to-date or does it include people whose cases were resolved?
- What happens to the match result? Is it immediately discarded if it is a miss, so that no human touches the data or remembers that a person was at location x with person y? Or is it kept and re-used at a later date for some other purpose?
- Is it true that the algorithms make lots of mistakes and that a lot of innocent people can be made suspect?
- What happens if there are no algorithms – does the system rely on people like security guards or border officers? Would these humans be more or less prone to making mistakes than technology?
- Is it true that someone with very dark skin is more likely to be made a suspect than someone with paler skin tones? And a woman more likely to be wrongly identified than a man?

As it has with everything in the world, COVID-19 has changed the dynamics of this conversation too and raised new questions:

Coronavirus has shown the fine balance between privacy and public health

- Is it reasonable that the use of facial recognition for COVID-19 contact tracing or vaccination status purposes is for a greater good than a particular individual's right to be ignored?
- Is there any difference between retrospectively using facial recognition for COVID-19 contact-tracing of an infected superspreader in a COVID-19-free community, and tracing a terrorist bomber back through the London underground by using facial recognition recorded videos to detect their movements?

Biometrics is a probabilistic technology and there can be serious consequences if errors are made in matching. Therefore the automated matching process can only be a tool supporting human decision-making.

Not all humans are equally capable of deciding whether two images are of the same person. Some human adjudicators are not trained to the stringent standards required for making the required decisions or presenting evidence in court.

Not all humans are equally capable of deciding whether two images are of the same person

This has caused tensions between law enforcement bodies and forensic and biometric regulators. This issue needs to be explored further and precise standards must be introduced to reassure the public and the judicial system that live – also known as automated – facial recognition can be used appropriately and legally.

Some law enforcement agencies refer to their use of *assisted* facial recognition, rather than *automated* facial recognition, drawing attention to the human in the loop – required so that any mistakes made technically or procedurally can be remedied by a qualified person.

A 2018 study [18] showed that face identification accuracy can be maximised by exploiting both the strengths of skilled humans and machines working collaboratively. It pointed to the best approach being to combine human and machine expertise. Fusing the most accurate machine with individual forensic facial examiners produced decisions that were more accurate than those arrived at by any pair of human and/or machine judges.

The Three Laws of Biometrics

In October 2020, the Biometrics Institute released its *Three Laws of Biometrics* to guide anyone working with biometrics in their implementations, and crucially in the order in which tasks should be carried out. Policy first, then process and only when robust review of those initial steps has taken place should the requisite technology be explored.

Statutory regulation and policy have not kept pace with the development and deployment of facial recognition technology. Most importantly, procedures guiding its use by law enforcement agencies are either non-existent or lacking transparency and oversight.

While there are generic risks related to sharing biometric data, there are also very different levels of severity associated with errors in specific use cases. Having to supply a code because your phone cannot detect your fingerprint may only be a minor inconvenience, but being detained and interrogated by law enforcement personnel is a different matter. At the same time, there are serious risks to community safety that can be mitigated through the use of biometric technology.

In the absence of trusted governance frameworks for the use of facial recognition, users of the technology including law enforcement agencies, border management agencies, private security companies and commercial outlets such as shopping malls, banks and casinos are each developing their own standards and approaches. This has left civil liberties groups and privacy advocates to use the courts to effectively formulate policy on behalf of the government resulting on the calls for outright bans on the use of facial recognition.

And because courts operate differently in different countries and jurisdictions there is now a patchwork of decisions across the globe, which inevitably adds to the confusion. Some countries, including the United States, are now developing legislation specifically for facial recognition, but this is a race to contain and control a technology that has been unregulated for over two decades in many regions of the world.

Is a ban or moratorium on facial recognition what we need right now?

At the Biometrics Institute's 2020 Congress, Wojciech Wiewiorowski – the European Data Protection Supervisor, said he supports the idea of a moratorium on the deployment of biometrics in public spaces in the EU, so that an informed and democratic debate can take place [19]. Other countries are also calling for a moratorium or even bans. The Australian Human Rights Commissioner for example has called for a moratorium until proper laws are put in place [20].

But it is also necessary to consider what a world without facial recognition technology would look like. Some worst-case scenarios could include:

- Citizen-benefiting government programmes no longer working
- Media criticism about huge queues at international airport arrivals
- Identity fraud out of control and the public complaining of the inconvenience of having to use pins to unlock phones
- Law enforcement agencies struggling with a return to a world before the technology and fearing a reduction in public safety, while terrorists exploit the scaled-back scrutiny
- Testing technology improvements on issues like demographic effects being impossible without an environment in which the industry could test

The Biometrics Institute asked a diverse group of its members and stakeholders whether they agree there should be a moratorium on the use of biometrics. Their responses have been amalgamated below.

YES, THERE SHOULD BE A BAN OR MORATORIUM…

> Pressing pause on the use of the technology may enable governments to work with biometrics experts as well as with law enforcement, border management, public authorities and with privacy advocates and the wider public, to build an appropriate legal framework which safeguards human rights.
>
> Following calls for a ban based on certain use cases of the technology which privacy campaigners say has infringed privacy, freedoms and democratic rights, such a pause may offer the opportunity for controlled trials and closer scrutiny.
>
> For uses that are deemed acceptable, standards and requirements would then need to be agreed.

Such a global methodology or legal agreement would need to address concerns about the risks of using facial recognition technology in decision-making that may result in a significant inconvenience or legally binding effects on members of the public. It would need to also address the concerns that impacts of demographic differences may affect certain sections of the population more than others."

NO, THERE SHOULD NOT BE A BAN OR MORATORIUM

It is much easier to call for a ban than to come up with a balanced position, so calls for bans have spread while the conversations continue about how to regulate the industry, guide users and protect privacy and data.

Would a ban have any exceptions? Or would the ban apply to particular use cases like untargeted surveillance in public areas in certain countries? Consideration must be given to use case and context and the different impacts of varying degrees of banning. No exceptions to a ban would mean the elimination of established, beneficial use cases of facial recognition such as verifying identity at a border, tackling passport and driver's licence identity fraud, tracking terrorist activity across a city, finding a kidnapped child or identifying a suspect when the only tool is an image.

Bans and moratoria in some countries will not affect the development and deployment of the technology in others. Some commercial providers may choose not to supply technology to some jurisdictions because of their history of public suppression or poor human rights compliance. However, there will always be firms that will be willing to supply technology to anyone who pays for it.

A ban will not solve the problem posed by new technology and techniques but only delay its introduction. In the months following a ban we could see a continuation in conflict and misunderstanding, leading onto safety concerns that could be mitigated through the sensible, controlled use of facial recognition. At some stage the competent authorities need to address the issues raised and legislate accordingly. Too much reliance is currently placed on the courts to provide retrospective rulings on these types of issues.

Bans and moratoria could stifle innovation and commercial competition. A ban in Europe, the UK or the United States would only allow other countries to develop, improve and deploy the technology. Long term, technology players halted under a ban may lose traction globally in favour of developers in the other parts of the world, and investment in technology in these countries could fall away. Once a ban was lifted – if in fact it was – we would be more likely to have to rely on foreign competitors to supply the technology we needed to keep our borders and streets safe.

Post COVID-19, government resources will be even tighter and facial recognition can be used to make many government processes more efficient, allowing officials to focus on misuse of the systems. This is true not just of automated border control, but also benefit fraud, organised crime and the new fight against coronavirus. Many organisations are currently working on biometric systems to detect sufferers in public spaces which could prove to be invaluable tools in the face of a historic crisis situation."

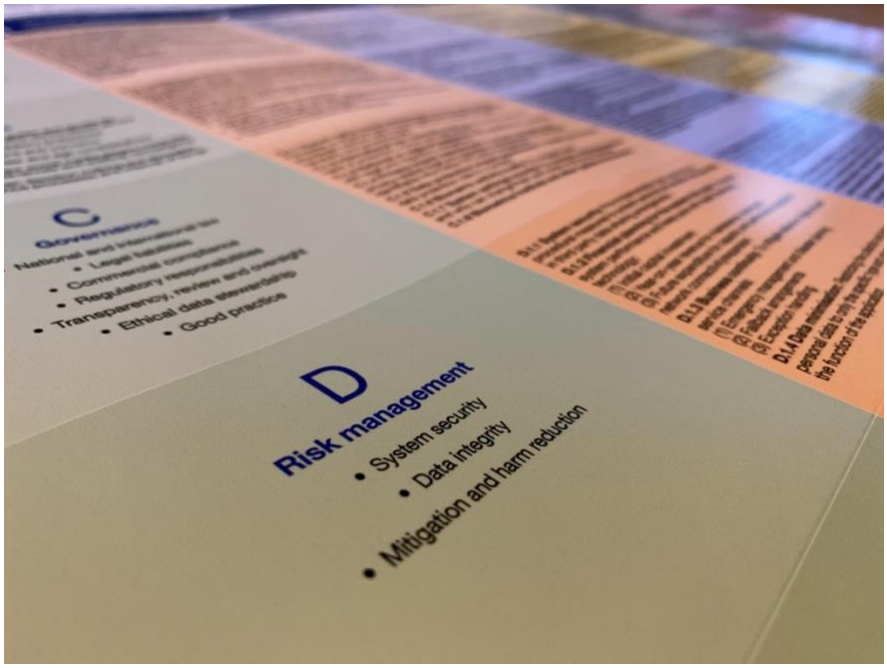
Conclusion

Like with any other technology, biometrics present risks – and those risks need to be carefully managed. There must be recognition that the current state of the technology is one of many security layers – just one indicator of authentication or identification. This technology can have limitations, depending on the use case and use environment.

Is it realistic that a pause on the use of the technology would bring a multi-stakeholder community together to draw up and agree on new regulatory or good practice measures? Is it likely that this global community would agree on a universal way forward?

Technological progress is unrelenting. Is banning facial recognition the answer? Or should we accept it exists, and work together to support, improve and create the necessary ecosystem for its success?

This moment in time is an opportunity for the biometrics community to use and advocate the use of the institute's *Three Laws of Biometrics*: policy first, then process, then technology. These concise guiding principles are a gateway to the in-depth *Good Practice Framework* [21] – a global methodology for assessing the impacts of the technology and how to manage and mitigate the risks.



The Good Practice Framework is a guide to mitigating the risks of using biometrics

There are significant responsibilities for users of the technology today. Things that should be done now regardless of regional legislative requirements. These are simply laid out in the *Three Laws of Biometrics* and explained in detail in the institute's *Good Practice Framework*. It is important to implement strong controls to prevent misuse of any technology including facial recognition, to identify and avoid the use of poorly performing algorithms and unscrupulous policies and procedures.

To gain public trust, openness and transparency are needed as to why and where and how the technology is being used, as well as independent scrutiny and oversight. It is important to follow existing good practices, and show you are adhering to legislation like the EU's General Data Protection Regulation (GDPR). The Biometrics Institute's *Privacy Guidelines* [22] are updated every two years to make sure they reflect global changes in technology or legislation which impact privacy. They are the result of extensive monitoring and consultation by our Privacy and Policy Expert Group, which comprises a broad spectrum of privacy specialists from around the globe. The guidelines include the significant international implications introduced by the GDPR, applied to biometrics.

The GDPR sets out a series of protections which anyone handling data should be aware of - whether or not you are affected by the territorial scope of the legislation. These include consent, transparency, accountability and the ability to seek redress where unfair.

So what next for biometric technology? It is likely that the two options are legislative frameworks or more bans and moratoria. Ultimately, a multi-stakeholder dialogue is crucial in arriving at any solution. The Biometrics Institute exists to create and educate our community on good practices, as well as to bring a diverse group of decision-makers together. By providing an independent forum for government, regulators, users, suppliers, and leaders in biometrics, privacy and research to debate, we have the best chance to bring about a way forward, together. Biometrics are a great solution for certain use cases. In order to assess whether biometrics are the right choice, policy and process need to be considered first. The *Good Practice Framework* provides a unique tool to plan and implement biometrics responsibly and ethically.

About the Biometrics Institute

The Biometrics Institute is the independent and impartial international membership organisation for biometric users and other interested parties. It was established in 2001 to promote the responsible use of biometrics and has offices in London and Sydney.

With more than a thousand members from 240 membership organisations spread across 30 countries, it represents a global and diverse multi-stakeholder community. This includes banks, airlines, government agencies, biometric experts, privacy experts, suppliers and academics.

The Biometrics Institute connects the global biometrics community. It shares knowledge with its members and key stakeholders and most importantly, develops good-practices and thought leadership for the responsible and ethical use of biometrics.

For more information, visit www.biometricsinstitute.org

References

[1] San Francisco Bans Facial Recognition Technology, 14 May 2019

[2] Committee led by Coalition rejects facial recognition database in surprise move, 24 October 2019

[3] EU seeks 'clear criteria' for use of biometric AI on mass scale, 30 January 2020

[4] Feds would be banned from using facial recognition under new bill, 25 June 2020

[5] The Three Laws of Biometrics, Biometrics Institute

[6] The secretive company that might end privacy as we know it, 18 January 2020

[7] Wrongfully accused by an algorithm, 24 June 2020

[8] Facial recognition laws are (literally) all over the map, 16 December 2019

[9] Washington State signs facial recognition curbs into law; critics want ban, 31 March 2020

[10] Building new bridges: Our thoughts on the U.S. election, 7 November 2020

[11] Facial recognition use by South Wales Police ruled unlawful, 11 August 2020

[12] Met police chief: facial recognition technology critics are ill-informed, 24 February 2020

[13] London Policing Ethics Panel final report on live facial recognition, May 2019

[14] France: CNIL outlines best practices for facial recognition in airports, 12 October 2020

[15] Facial recognition: For a debate living up to the challenges, 15 November 2019

[16] Face Recognition Vendor Test (FRVT) Part 3: Demographic Effects Report, December 2019

[17] NIST top 10 takeaways – demographic differences, Biometrics Institute

[18] NIST study shows face recognition experts perform better with AI as partner, 29 May 2019

[19] "The State of Biometrics" Update from the European Data Protection Supervisor, 7 October 2020

[20] Human Rights Commission wants moratorium on expanding facial recognition, December 2020

[21] Biometrics Institute Good Practice Framework

[22] Biometrics Institute Privacy Guidelines