Members' Viewpoints: The Relationship between Biometrics and Artificial Intelligence (AI)

The intersection between biometrics and AI

Version Final | 14 January 2025

Introduction

In 2024, the opportunities and challenges of AI and biometrics delivered many headlines and a need to clarify what policies and legislation would need to be put in place to ensure the responsible use of these technologies. The very first question the Institute members identified is whether all biometric uses are AI. Many believed that was not the case and the two should be separated. Therefore, an explanation (and definition) of the relationship of biometrics and AI was critical to understand how policy and legislation would apply to biometrics.

The Institute released a discussion paper early in 2024 untangling the issues and put them to its global membership for debate at three of its global conferences. The output is now this paper with key take aways and a new entry to the *Biometrics Institute Explanatory Dictionary* as well as briefings to members, policy makers and regulators on the findings and viewpoints.

During this consultation, we asked the following questions based on the discussion paper:

- How would you define the relationship between AI and biometrics: Are biometrics to be a subset of AI or is AI to be a subset of biometrics?
- Biometrics & AI: What are the corresponding issues?
- How does AI interact with biometrics: is there a relatively small overlap between the two or are they completely separate?

Key points

There are conflicting opinions among members of the Biometrics Institute regarding the relationship between AI and biometrics. Some say that biometrics are an adjunct to AI technology and, as a consequence, are always an integral part of it. Others point out that while biometrics and AI can be used together in a variety of applications it is also the case that some biometric applications exist quite separately from AI. The interpretation of this relationship relies heavily on the definition being used for both AI and biometrics.

Although there is an ISO definition for both biometrics and AI there are other important but sometimes non-aligned definitions that are probably better known in the public domain. These often emanate from national legislation and by governments across the world responding to the new and emerging AI technologies. Other key players such as major technology corporations, civil society organisations and the Biometrics Institute (dictionary on website) also seek to define AI from their own perspectives, knowledge base and experience.

Human operators working within biometric systems have also been cited as examples of non-AI processing but their continued existence depends heavily on their ability to match or exceed the performance of AI software in the future. There appears to be one set of views around humans making mistakes versus another set that are overly critical of errors, of any degree, made by machines.

This paper outlines the findings in detail and should be extremely valuable to those who shape policy and regulation around biometrics and around AI.

Headline Takeaways

Definitions of biometrics & AI

- There are *no universal definitions of biometrics or AI* and those put forward by ISO and some governments are either too technical, obtuse or are not fully aligned with one another or are hidden behind paywalls and not accessible to the majority of the general public

- The role of the *Biometrics Institute's Dictionary* is in capturing the shades of meaning and the different perspectives of key terms such as biometrics and AI - the definitive meaning and the general perceptions e.g. explaining the terms to a neighbour at a BBQ

- Therefore, what is the *public's perception of biometrics and AI*? Good, bad or ugly?

- The media (social and traditional) *struggle to define, explain and differentiate* between biometrics, in all its forms, and AI, in all its forms. A technological soup…

Impact and influence of AI on biometric processes

- *Which biometric applications 'have' AI*? What do we mean by that?

- There are *many ways that AI interacts with biometric technologies*, to aid processing, as a threat vector, as a protective measure or as an enhancement to general processes. Therefore, do they all present a serious risk, or just some?

- As AI becomes more pervasive in all technologies how will we *identify and assess the various risks*? Eventually, will we even be able to separate 'AI' components from any other element in a system?

Relationship between biometrics and AI

- There are *conflicting opinions* among members regarding the relationship between AI and biometrics.

- Some say that biometrics are an adjunct to AI technology and as a consequence are *always an integral part of it.*

- Others point out that while biometrics and AI can be used together, in a variety of applications, it is also the case that *some biometric applications exist quite separately from AI*.

- The inclusion of AI in any biometric process is dependent on the use case and not necessarily the biometric modality. Systems using the same biometric modality may or may not employ AI technology subject to the operating requirements.

- Human operators working within biometric systems have also been cited as examples of non-AI processing but their continued existence and contribution depends heavily on their ability to exceed or even match the future performance of AI software. There is a heavy dependence on legislative and liability treatment – the criteria appear to be different. There seem to be one set of views around humans making mistakes versus another that are overly

critical of mistakes made by machines

Regulatory oversight of biometrics and AI

- The terms *biometrics (*especially the use of live and remote biometric surveillance) *and AI have become conflated* in some regulation e.g. the EU AI Act

- '*Face recognition*' and '*AI*' are virtually interchangeable in some contexts. The blanket term "AI" is frequently used when "face recognition" would be the correct term. This might also be applied to other biometrics, especially *speaker authentication*

- Some regard all remote biometric techniques as restrictive of civil liberties and a threat to basic human rights

- Others consider some aspects of regulation to be excessive because it potentially constrains innovation, entrepreneurship and the ability to deploy cutting edge technological solutions to current societal problems and challenges

During the consultation we asked members: Do members agree with this graphic? There wasn't agreement on this question.

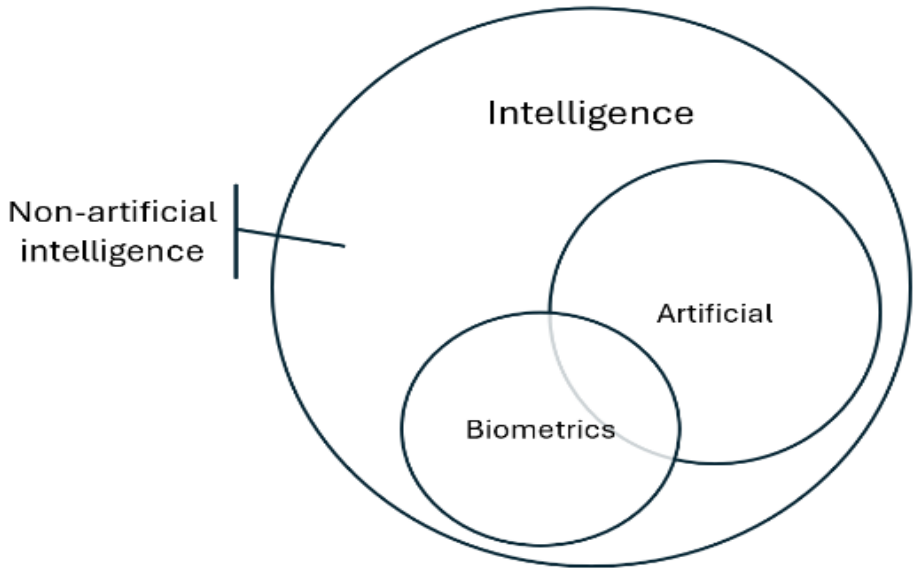

Figure 1: This graphic provoked discussion but not agreement among members

Members' viewpoints

1. Definitions of biometrics and AI

Summary of members' viewpoints

- We should align with the public viewpoint or at least take it into account
- There is no agreed definition of AI or biometrics
- The media, in general, contribute to public confusion
- ISO definition of biometrics
- ISO definition of AI (biometrics not specifically mentioned)

Context and dependencies

Although there is an ISO definition for both biometrics and AI there are other important but sometimes non-aligned definitions that are probably better known in the public domain. These often emanate from national legislation and by governments across the world responding to the new and emerging AI technologies. Other key players such as major technology corporations, civil society

organisations and the Biometrics institute (Dictionary on website) also seek to define AI from their own perspectives, knowledge base and experience. The sequestering of ISO material behind a paywall is not necessarily conducive to widespread engagement or the promulgation of good practice and a sound understanding of the subject matter to journalists, social media commentators and others involved in public discourse. Biometrics/face recognition is usually termed simply as AI in most media. Consequently, in general terms, the public's comprehension of both biometrics and AI is highly variable and often ill defined.

2. Impact and influence of AI on biometric processes

Summary of members' viewpoints

AI is used in biometrics in any of the following ways:

- Processing data from sensors
- Distilling a decision-making process from training data
- Segmentation and quality assurance
- Selecting the result to be presented in a fusion or vote process
- As an attack vector e.g. presentation or injection attacks
- As a countermeasure to protect against such attacks

AI also has a wider role in content authentication alongside biometric authentication for example:

- Used against threats such as those posed by the illegal dissemination of CSAM (Child Sexual Abuse Material) or NCII (Non-Consensual Intimate Images)
- GenAI threats e.g. asking GenAI to develop CBRN (Chemical, Biological, Radiological and Nuclear) and Cyber weaponry

AI can be employed to enhance biometric development:

- Supply chains
- Impact assessments
- Managing resources
- Incident Response
- Improving policy and governance procedures
- Data model training

Context and dependencies

This array of potential use cases in which AI and biometrics are used jointly in the same application raises the question about the perceived risk of employing biometric systems that 'have AI.' Does this just include systems that use AI as part of the matching process such as face recognition or does it also include PAD and other protective technologies or even applications, that are further removed from frontline performance, such as supply chain enhancement etc? As AI becomes increasingly pervasive in all technologies it will be important to identify specific risks because there could be many different AI components in any one system, including biometric applications, and not all AI components will carry the same level of risk or perhaps even be separable or easily identifiable from other 'non-AI' components.

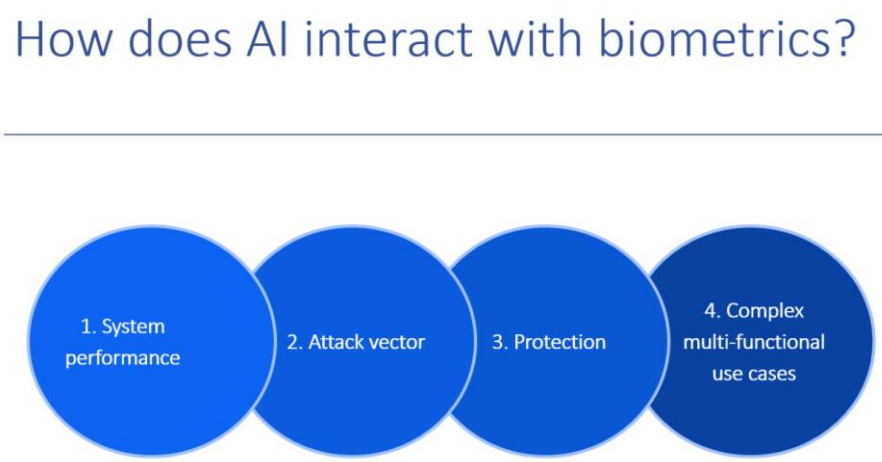

Figure 2: Presentation slide exploring how AI interacts with biometrics

3. Relationship between biometrics and AI

Summary of members' viewpoints

- AI is a critical technology for biometric success
- Not all biometric systems have an AI component
- Biometrics are one of many AI functions therefore all biometric systems are AI
- Biometric systems where decisions are presented using automated processes can be considered as AI
- AI is not a feature of biometrics when humans perform biometric searches and/or comparisons
- AI is not a feature of biometric systems that rely on simple comparison of patterns in or even the presence/absence of biological characteristics
- Several biometric modalities have more than one application (use), where one application (e.g. access) will use software that is AI-trained and another application (forensics or law enforcement) will use non-AI trained, human assisted software
- The original understanding of AI as artificial intelligence (i.e. something that is able to automate at scale a complex process of decision making etc.) would suggest that biometric processes performed by a machine are all AI but the advent of neural networks has altered the perception of AI and it could be considered just a tool in which case not all biometric systems currently use it
- AI is capable of generating (1) content, (2) forecasts, (3) recommendations and (4) decisions and therefore biometrics are compliant with and complementary to uses (2) to (4) but (1) is largely out of scope but could be relevant in the contexts of (a) artificially generated training material (the academic jury being split on this); and (b) biometric deepfakes. Many of the views above depend on how the term "AI" and its scope are defined

Context and dependencies

There are conflicting opinions among members regarding the relationship between AI and biometrics. Some say that biometrics are an adjunct to AI technology and as a consequence are always an integral part of it. Others point out that while biometrics and AI can be used together, in a variety of applications, it is also the case that some biometric applications exist quite separately from AI. Again, as at section 1 above, the interpretation of this relationship relies heavily on the definition being used for both AI and biometrics. The inclusion of AI in the biometric process is dependent on the use case and not necessarily the biometric modality. Systems using the same biometric modality may or may not employ AI technology subject to the operating requirements. Human operators working within biometric systems have also been cited as examples of non-AI processing but their continued existence depends heavily on their ability to exceed or match the future performance of AI software. There is a heavy dependence on legislative and liability treatment - the criteria appear to be different. There seem to be one set of views around humans making mistakes vs another that is overly critical of mistakes made by machines.

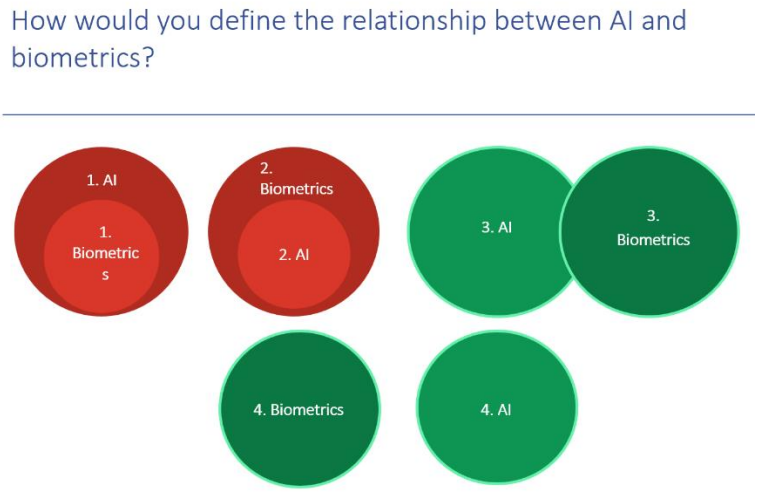

Figure 3: Presentation slide addressing the relationship between AI and biometrics

4. Regulatory oversight of biometrics and AI

Summary of members' viewpoints

- AI is a tool to enhance biometric performance and should not be convoluted with AI regulations
- Should biometrics be regulated with AI or as something else entirely?

Context and dependencies

AI and biometrics appear to have become conflated in some regulations e.g. EU AI Act and especially the use of live and remote biometric surveillance. As mentioned in 1 above, the terms '*face recognition*' and '*AI*' are virtually interchangeable and in this context the debate is centred around the requirement to protect the privacy and personal, sensitive data of innocent citizens while needing to identify criminals and terrorists before, during and after they have perpetrated offences. More generally, some regard all remote biometric techniques as restrictive of civil liberties and a threat to basic human rights whereas others consider some regulation to be excessive because it potentially constrains innovation and entrepreneurship e.g. in the case of the EU AI Act they would contend that the regulations interfere with independent law enforcement initiatives and thereby limit policing effectiveness and undermine their ability to protect citizens.

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 and ethical use of biometrics and has offices in London and Sydney.

The member register which represents a global and diverse multi-stakeholder community now lists over 200 membership organisations from 41 countries. It includes banks, airlines, government agencies, biometric experts, privacy experts, suppliers, academics and 18 Observers representing United Nations agencies, IGOs and European Union institutions.

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, ethical and effective use of biometrics.

For more information, visit www.biometricsinstitute.org

Contact:
Isabelle Moeller
Chief Executive
Biometrics Institute
isabelle@biometricsinstitute.org
Tel +44 7887 414 887

Dated: 15 December 2024

Annex 1: AI Definition as at December 2024

The Biometrics Institute Explanatory Dictionary can be accessed online. AI has been added to the list of terms in December 2024.

Artificial Intelligence (AI) 🚫

Biometrics usage

1. A machine, system etc. that performs intelligent functions or processes data using mechanisms believed to underpin intelligence (e.g., machine learning); or describing such a system.

   Many use AI to mean 'both performing intelligent function and containing intelligent data processing'. However, sometimes only one of these is intended; and sometimes systems with either function or processing are included (often when describing several such systems). Consequently, the meaning is often not obvious from the context; see examples 1, 2a and 2b below for illustration. Especially in formal use, ensure that the intended meaning is clear.

   This inconsistency confounds the relationship between biometrics and AI. Some view that all biometric systems are AI – applying to AI only an 'intelligence of function' requirement. Others argue that biometrics are only AI if they use intelligent data processing such as machine learning and neural networks.

2. AI has been increasingly employed in mainstream biometric processing in recent years, but it also features in other aspects of these applications:
   a) **AI attacks on biometric systems -** Threats from AI technologies that can seriously impact biometric applications are ever-present and growing. These include elements such as 'deep fakes' (where a person's face or voice is impersonated with AI techniques) and more general AI cyber attacks which result in the corruption or loss of data within the system.
   b) **AI protecting biometric systems -** AI can also play a crucial role in countering these threats by detecting incoming attacks and analysing and quality assuring data integrity.

More information is available in the paper *'The Relationship Between Biometrics and AI'* (see above) which explores this topic further.

Context and wider usage

In very general terms AI may be considered to be any form of an autonomous or partially autonomous computing system that is able to:

1. Simulate human thought, learning or behaviour.
2. Analyse large data sets to classify material, solve problems and make decisions, predictions or recommendations that previously would have required human intelligence.
3. Process data on a scale that exceeds human abilities.

However, it should be noted that many stakeholders observe the difficulty of drafting a solid definition for AI. Confounding factors include:

- Interest in AI from a wide array of governing bodies, commentators, and the public.
- Lack of clarity and shifting perspectives over time on what does and does not constitute 'intelligence' either in function or computation; and therefore what AI is when compared to non-intelligent machines.
- Reliance on comparisons with human intelligence. While analogy can aid understanding, it can lead to 'things that previously required human intelligence'. 50 years ago, that was true of calculators – yet

we do not now consider calculators to contain AI technology.
- Different stakeholders desire different entities to be considered, or not considered, as AI and even these predilections sometimes change over time.

Examples

1.

- The AI technology in the cameras recognised people passing in the street and presented them with tailored advertising on the electronic hoardings.
- Regulators are concerned about the non-consensual public capture and processing of face images using artificial intelligence facial recognition technology.

(NB these examples may well use techniques such as convolutional neural networks, but do not need to; and the actions and concerns described do not depend on this.)

- Face recognition system performance improved circa 2018 by adding AI (implying that prior to that time, non-AI algorithms were used).
- The legislators sought to impose controls on all types of AI systems (NB how would the scope of this intended action be defined?).

2a. Audio presented to the voice recognition system was actually an artificial intelligence-generated 'deep fake'. (NB that 'deep fake' usually implies generation by neural network techniques.)

2b. The attempt to enrol an altered, imposter's face image into the biometric system was prevented by artificial intelligence software that detected spurious artefacts and small distortions in the features. (NB a good example of where the process described may refer to a specific AI technique or be open to a wider interpretation i.e. any such software would be AI, no matter how implemented?).

Definitions in technical use

Russell & Norvig – 'Systems that act/think like humans,' aligned with the function/processing split noted in definition 1.
Google – Alternative - either intelligent in both function and processing as in definition 1; or using data analysis beyond human scale (Wider usage no.3).
US Presidential order – Intelligence in both function and processing.
EU AI Act (and OECD) – Intelligence in both function and processing.
ISO – Intelligence in either function or processing.
NIST CSRC – Intelligence in processing only.