humanitech
Powered by Australian Red Cross

Biometrics Background Paper

Wendy Shang

Research Volunteer, Humanitech

October 2022

Disclaimer:

This paper presents insights from a review undertaken by a research volunteer, Wendy Shang. The paper was commissioned by Humanitech for internal Australian Red Cross audience with the intent to inform understanding of humanitarian issues emerging with the implementation and use of biometric technology. It draws on information, opinions and advice sourced from a variety of secondary sources. The paper is not intended to be exhaustive and Australian Red Cross does not accept responsibility for any omissions or errors of fact.

Foreword

Frontier technologies have the potential to make our lives easier. Though not new, biometric technology is increasingly being used to identify or verify people in Australia and overseas. Due to its unique features and lack of passwords, biometrics promise to make authentication more secure and convenient, and to improve access to services. However, there is also the potential for misuse, mistakes, malfunction, discrimination, and violations of privacy and data security. It is important, therefore, to consider the foreseen and unforeseen risks of developing and using biometric technologies and mitigate them, as best we can.

Humanitech, an initiative of Australian Red Cross, is committed to ensuring data and technology is used in ways that serves humanity for the better. Our focus is on leveraging the opportunities of frontier technologies to benefit all people and communities, while addressing its risks to society. Humanitech proposes using a 'humanity first' approach to the design, development, and use of frontier technologies, such as biometrics. We have drawn on five (of nine) Humanity First principles to show *how* we might be able to ensure biometrics do not create or exacerbate vulnerability in our society.

This Biometrics Background Paper by Wendy Shang provides an excellent overview of some of the legal considerations around the development and use of biometrics in Australia. It highlights the need for strong legislative, regulatory, policy guidelines, and protections around inclusion, privacy, consent, and security of individuals' sensitive information. Our intention, through this paper, is to share best practices when it comes to engaging with biometric technologies. We hope it is a useful and practical guide for policymakers, technologists and practitioners to draw on, when they consider developing and using biometric technologies. In short, we hope this paper helps create an ethical, responsible and inclusive approach to biometric technologies in Australia and beyond.

Amal Varghese

Amal Varghese
Advocacy and Research Manager, Humanitech, Australian Red Cross

Introduction

The use of biometric information for the purpose of identifying or verifying the identity of a person is becoming more prevalent in Australia and overseas. The sensitivities around collecting such data, and the associated security and privacy risks, have been widely recognised on a global scale and led to legislative and policy reforms in various countries. This is most evident in the development of the European Union's *General Data Protection Regulation (GDPR)*[1], which has prompted various jurisdictions to revise their own data protection laws. Protections around using biometric data have also been incorporated into the African Union *Convention on Cybersecurity and Personal Data Protection* and the Council of Europe *Convention on the Automatic Processing of Personal Data*.[2] Risks in digital security were recognised at an early stage by the International Conference of Privacy and Data Protection Commissioners (ICPDPC) in 2015 with the adoption of the *Resolution on Privacy and International Humanitarian Action*[3], which focused on the risks associated with biometric identification systems.

Most recently, in Australia the Government has commenced a review of the *Privacy Act 1988 (Cth)* to strengthen privacy protection laws to support the growth of the digital economy.[4] It is anticipated to lead to major privacy law reforms in the country. This paper considers the current legal and practical considerations when using, or seeking to use, biometric data for the purpose of identifying or verifying the identity of individuals. It also explores the impact of biometric technology in the context of the principles of Humanity-First, a prototype developed by Humanitech to support people and organisations working with technology to investigate the ethical considerations and unintended consequences of their product or service. Specifically, it is critical that the development and introduction of biometric technologies into new contexts or communities do not exacerbate, or create, new types of vulnerabilities. Such vulnerabilities could take the form of discrimination, social exclusion, inadequate access, misuse of data for surveillance, and other unintended consequences. Serious consideration must be given to the types of future(s) – including adverse effects – that might arise as a result of the technology.

This paper proposes five Humanity First principles that may be helpful in considering the development, design, and use of biometric technologies in Australia.

Executive summary

There are several factors and principles that should be taken into account when considering the design, development, and use of biometrics as part of a solution to a problem in a governmental, corporate, or societal context. Organisations, decision makers and system developers must consider the vulnerabilities of the people that might be affected by the technology and consider the privacy of the data, the safety and security of the technology, and the trust of communities when using biometrics for identification purposes.

This paper draws on five of the Humanity First principles and how they can guide the development, design and use of biometric technologies.

Humanity First principle: Understand the individual, social, and environmental context of the problem that the solution is targeting.

In determining whether to introduce biometric technology in the delivery of solution to a governmental, corporate, or societal problem, it is important to consider the individual, community, society and environmental context of the problem and potential solutions.

Biometrics is being used internationally in a range of contexts

Biometric technology is being used all around the globe for different purposes in a variety of governmental, corporate and social contexts. It is important to include civil societies in the consultation process when designing biometric technology to gain deep insight into the context of the problem and illustrate some of the risks and vulnerabilities in the communities amongst which the technology will be used.

Humanity First principle: Design with a clear purpose that is shared with stakeholders.

When designing guidelines and laws for the use of biometrics, it is important to design with a clear purpose and explicitly share the story of why you are doing your work with the community and stakeholders.

Compliance with privacy laws

Entities should assess their data handling procedures to ensure these comply with the requirements of the Privacy Act, including obtaining the person's informed consent, providing the person with a compliant collection notice, recording the purpose for which the information is collected and ensuring processes are in place to prevent function creep (where information is collected beyond the primary purpose), complying with requirements if data is to be sent overseas, implementing security systems to store biometric data, and to destroy or de-identify information that is no longer required.

The Australian Government's review of the Privacy Act in 2021

Entities should be aware of the Australian Government's review of the Privacy Act, which is likely to lead to further reforms. All organisations should prepare to adjust their procedures and security frameworks to comply with the potential reforms.

Humanity First principle: Prioritise people and communities at risk of harm within the design and decision-making process and provide the support needed to move at the speed of trust.

In designing biometric technology and systems for use in the community, it is important to centre existing and potential vulnerabilities in the design process and invite people and communities at risk of harm to be at the centre of design and decision-making. This can help to identify the 'blind spots' in the technology and systems.

The risk of inaccuracies in biometric systems

Entities should assess their biometric systems for the risk of inaccuracies that may arise from false positive or false negative results, enrolment, and recognition failure due to changes to a person's biometric traits over time, inherent racial biases within the system, and human and system errors that may arise from processing data and working with algorithms.

Humanity First principle: Maximise freedom of those affected to control and use technology.

In designing frameworks for the use of biometric technology in society, maximise the freedom of those affected by offering them safe and inclusive opportunities for decision making, control, and use. This includes whether participants can provide meaningful consent and ensuring there are genuine alternatives, if they choose not to use the technology.

Meaningful and voluntary consent

Entities are encouraged to review their consent and notice procedures to determine whether a person is truly able to provide voluntary, meaningful, and informed consent when their biometric data is being collected. Processes should be assessed for the ways in which information about data collection is conveyed, whether these methods account for the person's level of literacy, language barriers, and cultural sensitivities, and whether alternate options are available to identify the person if they do not wish to provide their biometric information.

Humanity First principle: Be transparent about intentions, capability and use of data and privacy.

In building security systems for biometrics, it is necessary to be transparent and realistic about the problems that come with the use of biometrics solutions. By doing so, this will build the dignity, safety and trust of communities using or impacted by the technology. The use of biometrics is particularly problematic in terms of data security, theft and fraud and determining whether it is being used legitimately and in a proportionate manner.

Adequate security frameworks

Given the increased risks in data security, entities should ensure that their systems have adequate controls and oversight in place to protect against the risk of privacy and security breaches. Consideration should be given as to how biometric templates are stored (e.g., preferably not as raw data) and the security measures that must be in place. Entities should also assess whether the biometric information is being used for a legitimate purpose and whether using such data is necessary and proportionate to achieving that purpose. These considerations must be weighed against the risk of a security breach and the potential interference to an individual's privacy.

The background on biometrics

Biometrics in identification

As biometric characteristics are unique to individuals, they can be more reliable at identifying or verifying an individual's identity than other methods. Biometric data of an individual includes any physical, behavioural, or psychological trait of the person that can be used to identify them or authenticate their identity. This can include: DNA matching, ear shape, eyes (iris or retina recognition), face recognition, fingerprint recognition, gait, finger or hand geometry recognition, odour, signature recognition, typing recognition, vein recognition, and voice or speaker recognition.[5]

Increasingly, biometric data is being used for the purpose of authenticating a person's identity (known as one-to-one matching) or to identify an individual (known as one-to-many matching).[6] In an authentication system based on one-to-one matching, biometric data of a person can be matched against an existing database that already holds existing biometric information of that person. For example, a person's voice biometric may be collected as they speak with someone over the phone and used for authentication purposes in future calls. In an identification system based on one-to many-matching, a person's biometric data is compared against a database of biometric data of unknown persons (e.g., fingerprint databases). The purpose is to find a potential match between the sample and database in order to identify the person, such as in a crime scene. Biometric systems can also be used for surveillance purposes. Once a person's biometric features have been identified, they can be tracked through CCTV cameras as they move around in public.

Biometrics systems

Biometric systems identify or authenticate the identity of a person in two stages: enrolment and recognition.

- **Enrolment:** At the enrolment stage, a person's biometric characteristic is collected and enrolled into the system.[7] This information can be recorded either as raw data, such as a photograph of a face or an image of a fingerprint, or as a digital template, where key features of the characteristic are extracted to create a template which is then stored in the database.[8]

- **Recognition:** The recognition stage occurs in the future when a person's biometric information is presented and matched against existing biometric images and templates in the database. It is at this stage that the person's biometrics is used to identify, or authenticate the identity of, the person.[9]

There are variations in the way biometric technologies operate. Some utilise facial recognition systems which detect colour, black or white, infrared, images, or two or three-dimensional images. [10] Many biometric systems store only the template and not the raw data of the biometric characteristic. There are risks associated with storing original images (e.g. fingerprint images), which operators need to be aware of.

Humanity First principle: Understand the individual, social, and environmental context of the problem that the solution is targeting.

In determining whether to introduce biometric technology in the delivery of solution to a governmental, corporate, or societal problem, it is important to consider the individual, community, society and environmental context of the problem and potential solutions.

How is biometrics being used in different contexts internationally?

India – Aadhaar Digital system

In 2009, India launched Aadhaar, a 12-digit unique identity number linked to a range of citizen beneficiary services. Today, 1.3 billion Indians are enrolled in this system.[11] Aadhaar was deployed for biometric-based authentication to be used in the distribution of food rations and essential commodities and services to those in need through a Public Distribution System. So far, Aadhaar has streamlined the delivery of services and payments to individuals through contactless means during the COVID-19 pandemic. Through the Aadhaar authentication system, Indian residents can access up-to-date information about their entitlements, request services, and lodge complaints from their mobile phones.

Nigeria – pensioner systems

The University of Lagos, in collaboration with Avas Technologies Ltd, has launched a device which collects voice and fingerprint biometrics that can be used by pensioners and others for personnel management, healthcare, and education applications. [12] The solution allows pensioners to stay in the comfort of their homes and get verified, eliminating the need for them to appear in person to validate themselves.

Uganda – healthcare and welfare

Uganda's national biometric ID system is intended to improve access to services for Ugandans and has been funded in part by international organisations and country donors, including the World Bank and UKaid.[13] It has been compulsory to have an Ndaga Muntu ID number or card to access government services, including healthcare and welfare payments.

Zimbabwe - payroll

In Zimbabwe, a World Bank-assisted exercise to bring order to the civil service payroll successfully used biometric verification to reveal 10,000 ghost workers on Zimbabwe's public payroll.[14] The use of biometrics to identify 'ghosts' receiving fraudulent payments in Africa continues.

Sri Lanka - aerial drone surveillance

The Australian Joint Task Force Operation Sovereign Borders supported the Sri Lankan Police to establish an aerial drone surveillance capability to support the fight against crime in Sri Lanka.[15] The drones are used to deter maritime people smuggling activities in Sri Lanka (through transnational crime investigations) and in other activities, including natural disaster scene assessment and recovery. The threat of maritime people smuggling continues as vulnerable people are continuing to be exploited.

Various locations - CCTV

CCTV is used in various countries across the world. CCTV cameras can be linked to biometric databases in real time. The 'smart CCTV' system detects the location of anyone in the database and can monitor and record their behaviour and movements. [16]

The humanitarian sector

Biometrics is being used by some parts of the humanitarian aid sector to verify the identity of individuals. This includes fingerprinting, iris scans, and facial recognition, which has streamlined identification and has made it easier to add ID processes to aid distribution. The sector is becoming increasingly active in the use of biometrics, as seen through the UNHCR's biometric authentication programs, the World Food Program's biometric-based food distributions and high-level projects, such as the Centre for Humanitarian Data and UNICEF's Innovation Labs. [17]

UNHCR

In 2015, the UNHCR launched its Biometric Identity Management System (BIMS) for the registration and verification of refugees and to provide assistance to forcibly displaced people around the world. Of the refugees registered by the UNHCR, more than 80% of those above five years of age have a biometrics record.[18]

IrisGuard in the COVID-19 pandemic

Technology firm IrisGuard, in partnership with the UNHCR, has been used to provide contactless processes during the COVID-19 pandemic. The system uses iris biometrics, which is not impacted by the widespread use of protective masks. Iris Guards developed EyeCloud, a company developed to support real-time transactions at ATMs, supermarkets, post offices, and mobile wallets, and support resettlements processes by UNHCR partners.[19] In Jordan, iris recognition is used by banks' mobile bank buses visiting locked-down areas to enable refugees to withdraw cash and camp supermarkets, which process payment with biometrics.

The Restoring Family Links program - International Committee of the Red Cross

The Restoring Family Links program implemented by the International Committee of the Red Cross (ICRC), working with National Red Cross and Red Crescent Societies, have been reuniting families for decades[20]. Now with the aid of biometric systems and refugee databases, the ICRC can reunite families even faster following a conflict.

Image: Marie is reunited with her uncle after being separated for several months. Paulin Bashengezi/ICRC

Humanity First principle: Design with a clear purpose that is shared with stakeholders.

When designing laws and guidelines for the use of biometrics, it is important to design systems and processes with a clear purpose and to explicitly share the story of why you are doing your work with stakeholders.

Privacy laws in Australia

Organisations that collect, use, or disclose biometric data in Australia must comply with the obligations under the Australia Privacy Principles (APPs), which are incorporated in the *Privacy Act 1988* (Cth).[21] This is the main legislation that applies to the handling of personal and sensitive information in Australia. Under the Privacy Act, biometric data or information will be deemed 'sensitive information' if it is used for verification or identification purposes. A person's biometric information must be collected directly from the individual, unless it is unreasonable or impracticable to do so. There are some cases where this may not be practicable or possible, such as in the case of missing persons where an exemption might apply.

To collect a person's biometric data within Australia, it is necessary to comply with the following:

- **Consent:** Under APP 3, a person's consent must be obtained prior to collecting their biometric information and the information must only be collected where it is reasonably necessary for, or directly related to, the organisation's functions or activities.[22]
  In practice, this means they must ensure: [23]
    - the individual is adequately informed before giving their consent;
    - the person has given their consent voluntarily;
    - the person's consent is current and specific; and
    - the individual has the capacity to understand and communicate their consent.

- **Collection notice:** Under APP 5, if an entity wants to collect a person's personal information, they must notify the individual of [24]:
    - the identity and contact details of the collecting entity;

  - the purposes for collecting the information;
  - the main consequences if the information is not collected;
  - any other entities to which the information may be disclosed;
  - details of the entity's privacy policy and how to access or change their information or complain about a breach of APPs; and
  - whether the information will be disclosed to overseas recipients and, if so, the countries in which the recipients are located.

If there is a change to the details in the collection notice, the person should be asked to re-confirm that they consent to the changes in the notice.

- **Purpose of collection and disclosure:** Under APP 6, when biometric information is collected, it should only be used or disclosed for the primary purpose for which it was collected. The information cannot be used or disclosed for a secondary purpose unless the individual has consented to that purpose, or if the secondary purpose is directly related to the primary purpose.

  Consideration should also be given to how consent to primary and secondary purposes is recorded, monitored, and actioned, and whether adequate processes are in place to ensure biometric information is handled according to the persons' wishes.

  Function Creep
  Function creep occurs when information is used for a different purpose than the purpose for which it was collected. [25] When using biometric information for identification and authentication purposes, it is important to be aware of the risk of function creep. This can occur when the secondary use has not been communicated to the individual, or the individual has not given their consent to the secondary purpose, at the time the information was collected.

  Function creep can also occur unintentionally where the biometric data reveals more information than intended by the primary purpose. For example, where facial recognition is used for identification purposes, it may be possible to extract other information about the person (e.g. age, ethnicity) which can be used for secondary purposes.[26] This may result in the individual being discriminated against, profiled or targeted.

  Where biometric data is collected for one purpose, it should not be retained or used for other purposes without the consent of the individual. If the biometric information is to be used for a secondary purpose, the entity should obtain the person's consent.

- **Cross-border disclosures:** Under APP 8, when sending a person's biometric information overseas, it is necessary to take reasonable steps to ensure that the overseas recipient does not breach Australian privacy laws. However, this obligation may not apply if the individual consents to the disclosure of their information overseas and is fully aware that steps have *not* been taken to compel the overseas recipient to comply with Australian privacy laws.

  The collection notice (to the individual) must specify the entities and the locations to which the person's data is to be sent. Before sending a person's information overseas, it would be prudent to conduct due diligence on how the information will be handled once it is overseas and whether disclosure of the information would pose a serious threat to the life, health or safety of the individual.

  Where information handling is likely to present risks to persons, a prior Data Protection Impact Assessment should be carried out to evaluate the benefits of collecting and using the data, assess the nature, likelihood and severity of the threat, and implement any measures that can be to be taken to minimise the risks.

- **Security of information**: Under APP 11, biometric information must be securely stored and reasonable steps must be taken to protect the information from misuse, interference and loss, and from unauthorised access, modification or disclosure. This entails reviewing existing data security systems to ensure that biometric information can be adequately protected or whether security measures need to be increased. It may also extend to investigating the security systems of any overseas recipients to which the biometric data is being transferred to assess whether their security measures are adequate.

  Destruction of sensitive information

  Once biometric information is no longer required for any purpose for which it was collected, the entity is required to destroy the information or ensure that it is de-identified. If a legitimate secondary purpose still exists to which the individual has given its consent, then the information can still be kept for that purpose. Adequate processes must be in place to record primary or secondary purposes and to track whether these purposes still exist or whether information must be destroyed or de-identified.

Australian Government's Review of the Privacy Act in 2021

In response to the 2019 Final Report from the Australian Competition and Consumer Commission (ACCC) on its *Digital Platforms Inquiry*, the Australian Government is conducting a review of the *Privacy Act 1988 (Cth)* to identify areas where privacy protection may be improved and protect consumers data to support the growth of the digital economy.[27]

The Privacy Act review published a public Discussion Paper in October 2021 seeking consultation on possible reform options.[28] It includes considerations for better privacy protections around the use of artificial intelligence in biometric technology and forms of facial recognition.

Issues with the collection, use, and disclosure of biometric or genetic data
The Discussion Paper raises some preliminary issues on the collection, use, and disclosure of biometric data. This includes:

- Whether the collection, use, or disclosure of biometric or genetic data, including the use of facial recognition software, should be a 'restricted practice' where entities are required to take reasonable steps to:
    1. Identify privacy risks, and
    2. Implement measures to mitigate those risks.[29]
- Greater clarity is needed on how biometric information and templates are treated under the act, specifically in the context of video surveillance and the use of facial recognition in public where individuals may not be 'reasonably identifiable'.[30]
- There is confusion as to how the term 'biometric information' may apply to recent technological changes, such as gait recognition, and mouse use, or typing recognition.[31]
- There are human rights implications of biometric technologies, particularly facial recognition, as identified by the Australian Human Rights Commission in its recent Human Rights and Technology project.[32]

Notice and consent requirements

Submissions in the paper recommend that the current notice and consent model should be tightened requiring entities to handle personal information in a 'fair and reasonable manner' or in accordance with a higher benchmark of protection such as the 'legitimate interest' test modelled on Europe's General Data Protection Regulation (GDPR).[33] It is also recommended that more stringent protections should be applied to entities handling personal information of children and vulnerable persons.[34]

Sending data overseas

The paper suggests the development of a Cross Border Privacy Rules system in Australia as a certification scheme which would facilitate the free flow of data overseas while protecting the privacy rights for individuals.[35] Entities that wish to send personal information (including biometric data) overseas would need to comply with the certification scheme and may also be restricted from sending data to countries that do not comply with the scheme.

Restricted practices on 'high risk' activities and Privacy Impact Assessments

The Office of the Australian Information Commissioner (OAIC) has recommended creating 'restricted practices' and 'proceed with caution' zones which would prohibit the collection, use and disclosure of information in relation to 'high risk personal information handling' activities. The OAIC submitted that high-risk activities should be subject to additional organisational accountability obligations requiring them to 'proceed with caution' to ensure that individuals are protected from harms arising from those practices. Such entities should be required to conduct a Privacy Impact Assessment (PIA).[36] This requirement is already in force in the UK, whereby a Data Protection Impact Assessment must be conducted if an entity uses profiling or special category data to decide on access to services, or if the entity uses biometric or genetic data in certain situations.[37] The Australian Human Rights Commission (AHRC) supports these protective measures and has called for stronger laws around the use of facial recognition and biometrics, even going as far as recommending a complete ban on the use of biometrics within 'high risk' areas.

Automated decision-making

The paper recommends that privacy policies may need to include information on whether personal information will be used in automated decision-making which has a legal, or similar significant effect on people's rights.[38]

Greater accountability to disclose and record secondary purposes

The paper suggests that, before using or disclosing personal information for a secondary purpose, there may be more stringent obligations to disclose each of the secondary purposes for which the information is to be used or disclosed and to record those purposes formally.[39]

Looking ahead

Submissions on the Discussion Paper closed on 10 January 2022, and it is anticipated that draft reforms to the *Privacy Act* will be released later in the year. In the interim, entities that are collecting and using, or looking to collect and use, biometric data should prepare for potential changes to Australian privacy laws.

Humanity First principle: Prioritise people and communities at risk of harm within the design and decision-making process and provide the support needed to move at the speed of trust.

When developing, designing, and introducing the use of biometric technologies, it is important to centre people at (or potential) risk of harm from the very start of the process. This can help identify the "blind spots" inherent within such technologies and systems.

Inaccuracies in biometrics – what can go wrong?

There are inherent weaknesses in biometric systems, which can affect the accuracy of matched results.

False positive and false negative results

The accuracy of biometric systems can be compromised if errors in the system create false positive or false negative results. A false positive occurs when the system incorrectly matches an input to a non-matching template on the database.[40] Conversely, a false negative occurs when the system fails to detect a match between an input and the matching template.[41] A system returning high rates of false results becomes unreliable and can lead to unfair outcomes for the person being identified or authenticated. For example, where access to services or benefits is dependent on the identification of an individual, false negative results will deny the person access to these services and benefits. False positives in the context of criminal investigation can lead to the wrong person becoming imprisoned and impinge on a person's right to a fair trial (Article 14, International Covenant on Civil and Political Rights; ICCPR). These outcomes can impact a range of human rights, civil and political rights, and economic and social rights of the individual.

Enrolment and recognition failure

Problems arise when there is enrolment failure, which occurs when a biometric template cannot be successfully created.[42] Enrolment failure can occur through various causes, including low quality reference information (e.g., poor environmental conditions or bad lighting), low quality sensors in the system, or if the person has a physical or medical condition affecting their ability to enrol their biometrics in the system. For example, manual workers who have lost fingers or injured their hand in an accident may not be able to use fingerprint matching technology. Older people that have aged may experience difficulties in using facial recognition technologies. Maintaining a high successful enrolment rate is critical to ensuring the accuracy of a biometrics system.

Errors can also occur at the recognition stage due to:

- changes to the person's biometric characteristics between the time of enrolment and recognition (e.g., facial or vocal changes due to ageing, injury, surgery, or medical conditions).[43]
- different individuals sharing similar biometric characteristics (e.g., identical twins would have similar facial biometrics).[44]
- differences in the individual's interaction with the system between the enrolment and recognition stages may be different (e.g., the user poses differently or different lighting).[45]

Changes to an individual's biometric traits over time can render the biometric data on the system out of date, leading to recognition failure.

Case Study: inequality of access to welfare services in India

Where access to welfare is reliant on biometric systems, there is a risk that people will be denied access due to a disability or medical condition. In the case of the biometrics system being used in India, Aadhaar, it has been reported that a 68-year-old disabled woman with missing fingers was denied from enrolling for the system, which resulted in their receiving no food rations for 11 months.[46] Since the introduction of the system, there have been reported instances of people being denied social services and food rations due to missing digits or medical conditions, which prevent the person from being identified through the centralised system. This includes leprosy sufferers with no fingers or eyes. There are also reports that homeless and transgender people have been excluded from accessing services.[47]

Biases in the system

There are studies that show that there can be racial and gender biases inherent within systems. A test of American faces conducted by the US National Institute of Standards Technology demonstrated that women were less likely to be recognised by facial recognition than men.[48] This was even more pronounced for women of colour, as it was reported that "the highest false positives [were] in American Indians, with elevated rates in African American and Asian populations".[49] If a group of a particular race or gender tended to return false positive or false negative results, because the system found it difficult to verify persons in such cohorts, the use of biometric systems for law enforcement activities without the support of secondary materials would have the potential to impede on the right to a fair trial (Article 14, ICCPR). Additionally, it would impede the right to non-discrimination (Article 3, ICCPR) in respect of persons within that cohort. For this reason, it is necessary to carefully consider the level of inherent bias within a system when using it for identification purposes. It may be necessary to assess whether the underlying algorithms are trained on diverse and representative datasets to ensure minimal racial biases. System biases can arise if the current algorithms used for facial recognition have predominantly been tested with a certain cohort (e.g., white men). Default camera settings should also be assessed, as some settings may not be optimal for people with darker skin tones, resulting in lower-quality database images.

Human and system errors

Biometric systems are based on probabilistic calculations[50] and results must be reviewed by experts trained in facial recognition to reduce the possibility of false matches. Mistakes can still occur within this human review process. In addition, although the accuracy of facial recognition technology is continuing to improve, there is still a small chance of error. According to testing by the US National Institute of Standards and Technology (NIST), the accuracy of facial recognition algorithms improved by 20 times between 2014 and 2018.[51] After testing 127 algorithms from 39 leading developers, the combined failure rate was 0.2 percent. This means the systems were 99.8 percent accurate compared to 96 percent in 2014.[52] As observed by the Australian Human Rights Commission, biometrics are based on what are considered unique characteristics and "there is a risk that biometric identification may be perceived to be more accurate than may be the case".[53] It is important to be aware of the risks of inaccuracy when using biometric systems.

Humanity First principle: Maximise freedom of those affected to control and use technology.

In designing frameworks for the use of biometric technology in society, it is important to maximise the freedom of those affected by providing them with safe and inclusive opportunities for decision making, control, and use of the technology. This includes whether participants are able to provide meaningful consent and whether alternatives are available if they choose not to.

Consent – is it meaningful?

When obtaining a person's consent to collect their biometric information, it is important that their consent and participation in the enrolment process is truly voluntary and meaningful.

Cultural insensitivities and language barriers

There are many factors that can prevent a person from being able to participate in the enrolment of their biometric information, including cultural or religious considerations where it may not be inappropriate to collect facial images or other types of bodily information. The operators of biometric systems need to be sensitive and accommodating to these factors when requesting persons to provide their biometric information. In the case of veiled Muslim women in Bangladesh, women and girls reported they were not consulted on biometric identification systems and said they felt disrespected and violated when their headwear was adjusted during the registration.[54] Both operators and system designers need to cater for this diversity when planning to implement biometric systems.[55] Cultural insensitivities and language barriers can also lead to a lack of informed consent.

Many agencies reported that migrants had little or no understanding of the implications of sharing data, confidentiality or data privacy. In a report of the International Federation of the Red Cross (IFRC), it was identified that an agency using iris biometrics reported it spends 15 to 20 minutes with each person to explain the process.[56] The report states that: "There is a growing concern that informed consent is neither really consensual, nor properly informed, particularly in the case of digital identifies, creating a risk of misunderstanding or lack of knowledge on behalf of the end user".[57] When it came to consent, many non-government organisations asked migrants to sign or tick a box to indicate their consent. Therefore, it is important to be aware of the language and literacy barriers and cultural sensitivities when producing literacy to inform operators and participants in the biometric process.

A lack of alternatives

Organisations need to provide alternative options to using biometric systems if there is to be meaningful consent. In the context of providing aid, migrants often do not have any real choice but to provide their biometric data if they want to receive the aid.[58] The existence of an alternative means of participation is an important element of voluntary consent. If there is no alternative to identification other than through a biometric system, it cannot be said that the individual has provided meaningful consent to their biometric data being collected.[59] Where biometric data is used for identity matching purposes at checkpoints (e.g., airports and ports), this has the potential to impact on a person's freedom of movement (Article 12, ICCPR).

Case study: Data collected from Rohingya refugees in Bangladesh

In 2021, a Human Rights Watch (HRW) investigation revealed that data collected by the United Nations refugee agency, the UNHCR, from Rohingya refugees in Bangladesh had subsequently been shared by the Government of Bangladesh with the Government of Myanmar. There were conflicting reports on whether informed consent had been obtained from the refugees. According to HRW, some of the refugees they had interviewed 'had been told that their data would be used to issue an identity card which was required by the Government of Bangladesh to access aid and services and would not be linked to repatriation.'[60] The UNHCR responded to HRW by stating that it had 'explained all purposes of the data gathering exercise and obtained consent…and that no Rohingya [refugees] were put at risk'.[61] One of the refugees said that he had been asked if he consented to his information being shared with the Myanmar Government and he had felt that he "could not say no because I needed the Smart Card and I did not think that I could say no to the data-sharing question and still get the card."[62] In a meeting with HRW, UNHCR stated that it had, in fact, made it clear that 'a Smart Card would still be issued to those [refugees] who did not agree to share their data.'[63] The complexity and conflicting accounts of whether informed consent was obtained in this situation is *evidence* that gaining (and verifying whether this is true) informed consent is often difficult. However, there is a clear lesson here: entities should take all reasonable steps to get informed consent from individuals to mitigate their risk of being harmed.

Humanity First principle: Be transparent about intentions, capability and use of data and privacy.

In building security systems for biometrics, it is necessary to be transparent and realistic about the problems that come with the use of biometrics and any potential solutions. This will help build the dignity, safety, and trust of communities using or impacted by the technology. The use of biometrics is problematic in the areas of security, theft, and fraud of data, and serious consideration should be given as to whether the use of the technology is legitimate and proportionate in chosen settings.

Security of biometrics

Biometric data must be stored in secure systems to ensure the data is protected from theft, fraud, and misuse and is only used for legitimate and proportionate aims.

Legitimate aim, necessity and proportionality

Biometric information should only be collected and used if it is necessary to fulfil a legitimate purpose. Due to the risks associated with biometric data, only the minimum biometric information should be collected that is necessary to achieve a legitimate aim.[64] Organisations must be mindful that biometric systems have the potential to violate an individual's privacy.[65] As the Office of the United Nations Human Rights Commissioner has indicated "any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case."[66] Before using biometric systems, organisations should query whether the use of biometrics is proportionate, reasonable, and necessary to achieve its objectives. The risk of theft and fraud and privacy implications must be balanced against the need for the organisation to carry out its objectives.

Biometric systems should not be employed merely for the sake of convenience and the purpose of maintaining general security does not warrant their use.[67]

Controls and oversight

Due to the risks associated with biometric data, the oversight of the retention, collection, and use of biometric information is a critical role. Organisations using biometric systems must have appropriate controls and limitations in place. The more that a system is left to the discretion of individuals to use biometric data, the greater the risk of a breach of security and inaccuracy in the collection and use of the data. Therefore, a clear governance framework for sharing and using the data (and the consequences for breach of those rules) should be developed. Organisations should consider what conditions need to be met before a staff member can access an individual's biometric data and the process for verifying that those conditions have been met. To lower security risks, the storage of raw data (e.g., facial images) should be avoided and biometric data should be stored as templates that are encrypted.[68] If raw biometric characteristics are to be stored, security controls must be put in place and regulator monitoring and audit of those controls should be undertaken.[69]

In developing a security framework, organisations must assess the impact of the biometric system on the privacy of individuals, identify any potential risks of a breach of privacy, and develop mitigation strategies to address those risks.[70] One method in development is to store biometrics in a centralised database or on a public cloud and to process biometric data so that it works like password hashing, where the information about the individual is not revealed. [71] Another method involves removing parts of the biometric sample or distorting the data by adding noise to it.[72] In developing a security system, it is important to consider measures that adequately lower the security risks associated with storing biometric data.

Targets of identity theft and fraud

Once an organisation stores biometric information, it becomes a potential target for identity theft and fraud. If possible, centralised databases of biometric information should not be created, as they create a 'Fort Knox' effect and can be perceived as a valuable prize and prominent target for people seeking to engage in identity theft.[73] Any database is under risk of being hacked or the data may be compromised even with technical, organisational, or regulatory controls in place.[74] Whilst it is largely considered that biometric cannot be reversed engineered, advanced technologies have shown that this is not always the case. For example, fingerprints can be reconstructed using minutiae templates.[75]

Case Study: Stolen fingerprints in the Indian Aadhaar system

Since the inception of the Aadhaar system in India, there have been multiple reported cases of stolen fingerprint casts being used for fraud. Syndicates of racketeers would make the fingerprint casts to endorse documents, open locked apps, mobile phones, and bypass bio-metric barriers using fingerprints.[76] Corrupted fair price shop owners would provide the fingerprints and data to third parties that would create fingerprint casts out of silicon-like material. The casts were than used to imprint fingerprints to siphon off food rations from the public distribution system and sell these back in the open market with fair price shop owners pocketing the difference.

Irrevocability

The difficulty with using biometric systems is that a biometric identifier cannot be revoked or reissued if it is compromised. Once this occurs, the biometric data can no longer be used. This may have significant impacts on an individual's ability to access benefits and services if their identification is reliant upon the system. One idea that has been suggested is to transform the biometric data to generate a template that is revocable.[77] It is important that the revocability of biometric data, and the availability of alternate identification methods, be considered when using biometric systems.

Protecting data in humanitarian settings

In humanitarian contexts, the need to protect individuals' biometric data is particularly acute, as those individuals may face other vulnerabilities if they're misused and/or mishandled. Following recent biometric data breaches of personal data entrusted to the International Committee of the Red Cross and National Red Cross and Red Crescent societies (the Red Cross Movement), the Council of Delegates of the International Movement passed a resolution in June 2022 that *committed* the Red Cross Movement, ….to ensure "appropriate and strong levels of data security when processing data, [and] to apply best practices in data governance for all humanitarian data".[78]

Conclusion

When considering the use of biometrics as part of a solution to a governmental, corporate, or societal problem in Australia, a Humanity First approach can help ensure the technology is developed and used ethically, inclusively, and responsibly. Biometrics can be an enabler of economic development and access to government services, improve digital inclusion and serve as a gateway to increased independence. However, its improper development and use can also lead to individuals facing discrimination and their privacy and dignity being violated.

In this paper, a Humanity First approach has been proposed to developing and using biometrics. In practice, this means consulting with civil societies in a timely way to understand the problem, risks, and vulnerabilities in the communities amongst which biometrics will be (or is proposed to be) used; clearly telling people why their information is being collected and what it will be used for; inviting people at risk of harm to be at the centre of the design and decision-making process to avoid unintended consequences; getting people's informed consent; and being transparent about the security risks around people's data and putting in place risk mitigation strategies.

In sum, a Humanity First approach to developing and using biometric technologies is a way for us – civil society, policy makers, practitioners, technologists – to preserve the dignity, safety and trust of people and our communities, whilst maximising the benefits of the technology amongst society.

Endnotes

[1] Dentons 2020, *GDPR Update – Biometric Data*, viewed 25 February 2022, <https://www.dentons.com/en/insights/alerts/2020/december/22/gdpr-update-biometric-data>.
[2] Narbel, V & Sukaitis, J 2021, 'Biometrics in humanitarian action: a delicate balance', *Humanitarian Law & Policy*, 2 September, viewed 25 February 2022, <https://blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/>.
[3] Ibid.
[4] Treasury 2019, *Government Response and Implementation Roadmap for the Digital Platforms Inquiry*, viewed 25 February 2022, <https://treasury.gov.au/publication/p2019-41708>.
[5] Biometrics Institute, *Types of Biometrics*, viewed 25 February 2022, <https://www.biometricsinstitute.org/what-is-biometrics/types-of-biometrics/>.
[6] Office of the Victorian Information Commissioner, 2019, *Biometrics and Privacy - Issues and Challenges*, viewed 25 February 2022, <https://ovic.vic.gov.au/privacy/biometrics-and-privacy-issues-and-challenges/>.
[7] Ibid.
[8] Ibid.
[9] Ibid.
[10] Office of the Privacy Commissioner of Canada 2013, *Automated Facial Recognition in the Public and Private Sectors*, viewed 25 February 2022, <https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2013/fr_201303/>.
[11] O'Callahan, T 2020, 'What happens when a billion identities are digitized?', *Yale Insights*, 27 March, viewed 25 February 2022, < https://insights.som.yale.edu/insights/what-happens-when-billion-identities-are-digitized>.
[12] Vanguard 2020, *Unilag, IT firm, launch biometric verification solution for pensioners*, viewed 25 February 2022, < https://www.vanguardngr.com/2020/12/unilag-it-firm-launch-biometric-verification-solution-for-pensioners/>.
[13] Center of Human Rights and Global Justice, Initiative for Social and Economic Rights, and Unwanted Witness 2021, 'Chased Away and Left to Die: How a National Security Approach to Uganda's National Digital ID Has Led to Wholesale Exclusion of Women and Older Persons', 8 June, viewed 25 February 2022, <http://www.indiaenvironmentportal.org.in/files/file/chased%20away%20and%20left%20to%20die.pdf>.
[14] Latham, B 2020, 'Zimbabwe Removes 10,000 Ghost Workers from Payroll, Herald Says', *Bloomberg*, viewed 25 February 2022, <https://www.bloomberg.com/news/articles/2020-12-21/zimbabwe-removes-10-000-ghost-workers-from-payroll-herald-says#:~:text=Zimbabwe's%20government%20has%20removed%20more,based%20newspaper%20said%20on%20Monday>.
[15] Evlin, L 2021, 'Tamils in Australia condemn Border Force's gifting of surveillance drones to Sri Lankan authorities', *SBS News*, viewed 25 February 2022, <https://www.sbs.com.au/news/tamils-in-australia-condemn-border-force-s-gifting-of-surveillance-drones-to-sri-lankan-authorities/5a0a18c1-69d2-4d6f-abf5-640f43a5a56e>.
[16] Mann, M and Smith, M 2017, 'Automated Facial Recognition Technology: Recent Developments and Approaches to Oversight', *University of New South Wales Law Journal* (Advance), vol. 40, no. 1, p. 4.
[17] Hersey, F 2021, 'UN 'should follow EC' in starting to regulate biometrics, artificial intelligence', *Biometric update.com*, viewed 25 February 2022, <https://www.biometricupdate.com/202106/un-should-follow-ec-in-starting-to-regulate-biometrics-artificial-intelligence>.
[18] Bogle, A 2019, 'Biometric data is increasingly popular in aid work, but critics say it puts refugees at risk', *ABC news*, viewed 25 February 2022, <https://www.abc.net.au/news/science/2019-06-21/biometric-data-is-being-collected-from-refugees-asylum-seekers/11209274>.
[19] Lee, J 2016, *UNHCR, IrisGuard launch EyeCloud to assist refugees with biometric banking*, viewed 25 February 2022, <https://www.biometricupdate.com/201601/unhcr-irisguard-launch-eyecloud-to-assist-refugees-with-biometric-banking>.

[20] ICRC, 'Restoring Family Links, viewed on 16 August 2022, https://www.icrc.org/en/what-we-do/restoring-family-links>.
[21] Schedule 1, *Privacy Act 1988* (Cth).
[22] Section 3.3(a), *Privacy Act 1988* (Cth).
[23] Office of the Australian Information Commissioner, *Australian Privacy Principles Guidelines*, viewed 25 February 2022, < https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/>.
[24] Section 5.2, *Privacy Act 1988* (Cth).
[25] Office of the Victorian Information Commissioner, 2019, *Biometrics and Privacy - Issues and Challenges*, viewed 25 February 2022, <https://ovic.vic.gov.au/privacy/biometrics-and-privacy-issues-and-challenges/>.
[26] Narbel, V & Sukaitis, J 2021.
[27] Treasury 2019, *Government Response and Implementation Roadmap for the Digital Platforms Inquiry*, viewed 25 February 2022, <https://treasury.gov.au/publication/p2019-41708>.
[28] Attorney-General's Department 2021, *Privacy Act Review – Discussion Paper*, viewed 25 February 2021, <https://consultations.ag.gov.au/rights-and-protections/privacy-act-review-discussion-paper/>.
[29] Ibid, p. 12.
[30] Ibid, p. 34.
[31] Ibid, p. 34.
[32] Ibid, p. 34.
[33] Ibid, p. 7.
[34] Ibid, p. 7.
[35] Ibid, p. 168.
[36] Ibid, p. 94.
[37] Ibid, p. 95.
[38] Ibid, p. 14.
[39] Ibid, p. 15.
[40] Office of the Victorian Information Commissioner 2019.
[41] Ibid.
[42] Ibid.
[43] Ibid.
[44] Ibid.
[45] Ibid.
[46] Yoti 2020, *Marginalised Aadhaar: Digital identity in the time of COVID-19*, viewed 25 February 2022, <https://www.yoti.com/blog/marginalizedaadhaar-digital-identity-in-the-time-of-covid-19/>.
[47] Reuters 2019, *Aadhaar still excludes homeless and transgender people from being enrolled: Study*, viewed 25 February 2022, <https://www.firstpost.com/india/aadhaar-still-excludes-homeless-and-transgender-people-from-being-enrolled-study-7706061.html>.
[48] Hao, K 2020, 'A US government study confirms most face recognition systems are racist', *MIT Technology Review*, December, viewed 25 February 2022, <https://www.technologyreview.com/2019/12/20/79/ai-face-recognition-racist-us-government-nist-study/>.
[49] Ibid.
[50] Office of the Victorian Information Commissioner 2019.
[51] Grother, P et al 2019, 'Ongoing Face Recognition Vendor Test (FRVT) Part 2: Identification', *National Institute of Standards and Technology*, 13 September, viewed 25 February 2022, <https://www.nist.gov/publications/face-recognition-vendor-test-frvt-part-2-identification>.
[52] Ibid.
[53] Australian Human Rights Commission 2019, 'Review of the Identity-matching Service Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018', *Australian Human Rights Commission Submission to Parliamentary Joint Committee on Intelligence and Security*.
[54] Zuboff, S & Schwandt, K 2019, *The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power*, Profile Books.
[55] Office of the Victorian Information Commissioner 2019.

[56] Hersey, F 2021, 'Red Cross issues recommendations for digital ID in humanitarian sector', *Biometric update.com*, 11 June, viewed 25 February 2022, <https://www.biometricupdate.com/202106/red-cross-issues-recommendations-for-digital-id-in-humanitarian-sector>.
[57] IFRC et al 2021, *Digital Identity: Enabling Dignified Access to Humanitarian Services in Migration*, viewed 25 February 2022, <https://preparecenter.org/resource/digital-identity-enabling-dignified-access-to-humanitarian-services-in-migration/>.
[58] Zuboff, S & Schwandt, K 2019.
[59] Office of the Victorian Information Commissioner 2019.
[60] Human Rights Watch 2021, 'UN Shared Rohingya Data Without Informed Consent', June 2021, viewed 16 August 2022, https://www.hrw.org/news/2021/06/15/un-shared-rohingya-data-without-informed-consent>.
[61] Ibid.
[62] Ibid.
[63] Ibid.
[64] Council of Europe 2012, Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies*, Doc 00720/12/EN/WP193, 27 April.
[65] Office of the Victorian Information Commissioner 2019.
[66] United Nations Human Rights Council 2014, *The right to privacy in the digital age: Report of the Office of the United Nations High Commissioner for Human Rights*, viewed 25 February 2022, <https://digitallibrary.un.org/record/777869?ln=en>.
[67] Council of Europe 2005, *Progress Report on the Application of the Principles of Convention 108 to the Collection and Processing of Biometric Information Data* (2005), Recommendation 3.
[68] Office of the Victorian Information Commissioner 2019.
[69] Ibid.
[70] Ibid.
[71] Narbel, V & Sukaitis, J 2021.
[72] Narbel, V & Sukaitis, J 2021.
[73] Crompton, M 2002, 'Biometrics and Privacy', *PrivLawPRpr*, p. 36.
[74] Council of Europe 2005.
[75] Campisi, P (ed) 2013, *Security and Privacy in Biometrics*, Springer, p. 187.
[76] The Economic Times 2017, *Watch out, Aadhaar biometrics are an easy target for hackers*, viewed 25 February 2022, <https://economictimes.indiatimes.com/tech/internet/watch-out-aadhar-biometrics-are-an-easy-target-for-hackers/articleshow/61183055.cms?from=mdr>.
[77] Narbel, V & Sukaitis, J 2021.
[78] Council of Delegates 2022, *Safeguarding Humanitarian Data*, viewed on 16 August 2022, https://rcrcconference.org/app/uploads/2022/04/CoD22-SafeguardingHumanitarian-Data-draft-zero-resoluton-EN.pdf>.

humanitech

Powered by Australian Red Cross