Forum:	Special Conference on the Paradox of Progress (SPECON)
Issue:	Addressing the Risks Posed to Human Rights by Biometric Technologies
Student Officer:	Christina Antonakou, Konstantina Plesti
Position:	Deputy Presidents

PERSONAL INTRODUCTION

Dear delegates,

My name is Christina Antonakou, I am a 10th grade student at Pierce (The American College of Greece) and it is my utmost honor and pleasure to serve as the Deputy President of this year's Platon School Model United Nations conference, in the Special Conference on the Paradox of Progress.

Having recently been a delegate myself, I acknowledge that most of you will be anxious, especially the newcomers. The key to be properly prepared in order to be ready to conduct a fruitful debate upon all topics, is to read this guide which provides you eminent information to the topic "Addressing the Risks posed to Human Rights by Biometric Technologies", but keep in mind that you should also engage in your personal research regarding the policy of your countries. I look forward to meeting you all and listening to all of your ideas, as we will be discussing a crucial topic which concerns us all, living in a society which is surrounded by biometric technologies.

Should you have any questions, do not hesitate to contact me at cantonakou@gmail.com.

Best Regards,
Christina Antonakou

Dear delegates,

My name is Konstantina Plesti and I am an IB1 student at HAEF Psychico College. The 13th PSMUN will be my 8th MUN Conference overall and my 2nd time chairing. For this year's session, I have the great honor of serving as one of the Deputy Presidents in the Special Conference on the Paradox of Progress (SPECON).

First of all, I want to congratulate you all for participating in this committee for the 13th session of PSMUN. During the conference, I hope that we will be able to get to know each other, prepare resolutions, debate and have a great time! This year's topics are closely related to the theme of this year's theme: the Paradox of Progress. This study guide concerns the 2nd topic of the agenda: Addressing the Risks Posed to

Human Rights by Biometric Technologies", and it should provide you with the fundamental information on this topic. Nevertheless, you are highly encouraged to conduct your own research to get a better and more profound understanding of the topic. The bibliography can be beneficial to the research process.

Should you have any questions about the topic, committee or conference, do not hesitate to contact me via email at kplesti@athenscollege.edu.gr.

I am looking forward to meeting all of you in March!

Best regards,

Konstantina Plesti

INTRODUCTION

The necessity for accurate identification arose as early as the 1800s with the advent of the Industrial Revolution and the subsequent rapid growth of the human population. However, it wasn't until the end of the 20th century that certain biometric identifiers became feasible. The biometric technology industry is estimated to be worth 47.8 billion US dollars in 2023 and is expected to grow to US$86.1B by 2028.[1] As biometric technologies continue to expand across various industries due to technological advancements, the imperative to address human rights violations stemming from their use becomes increasingly critical.

Biometrics are utilized as identifiers primarily because they remain immutable and unique. Nevertheless, if this data is compromised, it can pose significant privacy and security risks. Consequently, concerns arise regarding how to ensure the safe and ethical use of biometric technologies, the consensual collection of personal and sensitive data, and the legal handling of information to prevent data breaches and violations of human rights. Therefore, it is essential to analyze the causes and consequences of this situation in order to provide appropriate solutions and effectively address the issue.

The rapid proliferation of biometric technologies underscores the need to tackle the ethical and legal implications associated with their use. While biometric technologies offer accurate identification, their misuse can lead to privacy breaches and human rights violations. To effectively address this issue, it is crucial to first identify the causes and consequences of biometric technology misuse in order to develop solutions that uphold privacy and safeguard the human rights of all individuals.

[1] "Biometrics Market Reports | Biometric Update." *Biometric Update | Biometrics News, Companies and Explainers*, 7 Feb. 2024, www.biometricupdate.com/biometric-news/biometric-research.

DEFINITION OF KEY TERMS

Authentication

Authentication is defined as "the process of recognizing a user's identity." It is the process of matching an incoming user request with "a set of identifying credentials." "The credentials provided are compared to those on a file in a database of the authorized user's information within an authentication server."[2]

Biometrics

Biometrics are defined as "a measurable physical characteristic or personal behavioral trait" that can be used to verify the identity of a user. Examples of biometrics include fingerprints, facial images, iris samples, and more.[3]

Data breach

A data breach refers to "a security incident in which malicious insiders or external attackers gain unauthorized access to confidential data or sensitive information such as medical records, financial information or personally identifiable information (PII)."[4]

Database

A database is an "organized collection of structured information, or data, typically stored electronically in a computer system. A database is usually controlled by a database management system (DBMS)."[5]

Privacy

Privacy is the right of an individual "to maintain control over and confidentiality of information about themselves."[6]

Function creep

Function creep is "the gradual widening of the use of a technology or system beyond the purpose for which it was originally intended, esp when this leads to potential invasion of privacy."[7]

---

[2] "What Is Authentication? Definition of Authentication, Authentication Meaning." *The Economic Times*, economictimes.indiatimes.com/definition/authentication

[3] Editor, CSRC Content. "Biometrics - Glossary: CSRC." *CSRC Content Editor*, csrc.nist.gov/glossary/term/biometrics

[4] "Data Breach." *CyberArk*, 20 Apr. 2023, www.cyberark.com/what-is/data-breach/.

[5] "What Is a Database?" *Oracle*, www.oracle.com/database/what-is-database/.

[6] Editor, CSRC Content. "Privacy - Glossary: CSRC." *CSRC Content Editor*, csrc.nist.gov/glossary/term/privacy

[7] "FUNCTION CREEP Definition and Meaning | Collins English Dictionary." *Collins Dictionaries*, 8 Feb. 2024, www.collinsdictionary.com/dictionary/english/function-creep#:~:text=function%20creep%20in%20British%20English,to%20potential%20invasion%20of%20privacy.

Hacking

Hacking is defined as "the unauthorized access to or control over computer network security systems for some illicit purpose."[8]

Human rights

According to the UN, human rights are "rights inherent to all human beings, regardless of race, sex, nationality, ethnicity, language, religion, or any other status."[9]

Personal data

According to the GDPR (General Data Protection Regulation), "personal data is any information which is related to an identified or identifiable natural person."[10]

BACKGROUND INFORMATION

The Evolution of Biometric Technologies

In the 1800s, the rapid urbanization resulting from the industrial revolution created a pressing need for accurate identification. With larger populations in cities, merchants and authorities found it increasingly difficult to rely solely on personal experiences and local knowledge. This demand for identification was particularly crucial in the justice system, where distinguishing first-time offenders from repeat offenders became imperative. Prior to this period, such differentiation was challenging. Consequently, there arose a necessity for a formal system that could record offenses alongside specific identity traits of individuals. The first systematic approach to this challenge originated in France with the Bertillon system, which focused on measuring various body dimensions to create a standardized method of identification, known as anthropometry. Meanwhile, another approach emerged involving the formal use of fingerprints by police departments across South America, Asia, and Europe. By the late 1800s, a method was developed that focused on identifying individuals based on unique fingerprint patterns and ridges, providing a more individualized metric compared to Bertillon's method.

The development of more sophisticated biometric systems continued into the late 20th century, coinciding with advancements in computer technology. In 1991, real-time face recognition became feasible with the introduction of eigenfaces, an appearance-based approach to face recognition pioneered by computer scientists Turk and Pentland at MIT. Despite being susceptible to environmental factors, this discovery marked a significant breakthrough in face recognition technology. In 1996, hand geometry was implemented for the first time at the Atlanta Olympic Games to

[8] "What Is Hacking? Definition of Hacking, Hacking Meaning." *The Economic Times*, economictimes.indiatimes.com/definition/hacking.

[9] "Universal Declaration of Human Rights." *United Nations*, www.un.org/en/about-us/universal-declaration-of-human-rights.

[10] "Personal Data." *General Data Protection Regulation (GDPR)*, 22 Oct. 2021, gdpr-info.eu/issues/personal-data/

control access to the Olympic Village, showcasing the scalability and efficiency of biometric systems, as over 65,000 individuals were enrolled and over 1 million transactions were processed within a 28-day period.

The latest advancement in biometric technology is exemplified by the Mastercard Biometric Card, introduced in 2020. This innovative card combines chip technology with fingerprint recognition to verify the cardholder's identity for in-store purchases. Equipped with an embedded sensor powered by the chip, the card authenticates the buyer's identity through their fingerprint, enhancing security and convenience in transactions.

Examples and Evolution of Biometric Technologies

Fingerprints

Fingerprints are among the most widely utilized biometric technologies, offering a reliable method for identifying individuals through the unique patterns found on the tips of their fingers. These patterns, known as dermatoglyphs, consist of intricate ridges and valleys that are exclusive to each person, making fingerprints highly distinctive and virtually impossible to replicate.[11]

The process of fingerprint recognition typically involves specialized scanners. Two primary types of scanners are commonly used: optical scanners and thermal scanners. Optical scanners work by illuminating the finger with a prism and capturing a digital image based on the reflections of light off the ridges and valleys. Thermal scanners, on the other hand, utilize heat to differentiate between the temperature variances of the ridges and valleys, generating an image based on this contrast. In both cases, the captured data is processed, filtered, and converted into a mathematical representation known as an algorithm. Importantly, only this algorithmic representation of the fingerprint is stored for verification purposes, ensuring the security and privacy of individuals' biometric data.

The advantages of fingerprint biometrics are manifold. Firstly, fingerprints are inherently tied to the individual and cannot be lost or misplaced, providing a high level of accuracy and security for identity verification. Moreover, fingerprint recognition is cost-effective and user-friendly compared to alternative biometric technologies such as ear recognition, which may be utilized when facial recognition is impractical due to obstructions. Fingerprint recognition is widely employed in everyday scenarios, such as unlocking smartphones. Many modern smartphones feature fingerprint sensors embedded either within the display or on the device's surface, enabling users to unlock their phones, authorize transactions, and access specific applications with a simple touch of their fingertip.

[11] Dermatoglyphics. (n.d.). SienceDirect. https://www.sciencedirect.com/topics/medicine-and-dentistry/dermatoglyphics

Vein biometrics

Vein or vascular biometrics is a cutting-edge technique for biometric authentication that analyzes the unique pattern of blood vessels visible from the surface of the skin, particularly in the fingers. This method is considered highly secure and accurate for verifying individuals' identities, as the intricate structure of finger veins cannot be easily replicated or stolen without the subject's knowledge. This makes vein recognition a particularly robust solution for safeguarding personal information during identity verification processes.

The development of vein recognition technology continues to advance, with increasing integration into various aspects of daily life. Currently, it is utilized for a range of applications including credit card authentication, employee attendance tracking, network security authentication, and widespread use at ATMs. Notably, Egypt has emerged as a pioneer in adopting vein recognition technology by integrating it into their national ID program. This strategic move reflects the country's commitment to investing in science and technology to bolster innovation and global competitiveness. Furthermore, it sets a precedent for other nations to follow suit, potentially leading to widespread adoption of vein recognition technology worldwide.

However, there are certain limitations and considerations associated with vein recognition. One such limitation is the natural changes that occur in finger vein patterns over time, particularly as individuals age. The consistency of vein patterns is highest between the ages of 20 and 50, making this age range optimal for accurate identification using vein biometrics.[12] Additionally, environmental factors can affect the efficiency of vein recognition systems. For instance, extreme temperatures can alter blood flow and vein size, leading to variations in vein patterns and potentially resulting in false negatives during identification processes, particularly in regions with extreme climates.

Despite these challenges, vein recognition remains a highly promising biometric technology with significant potential for enhancing security and identity verification across various sectors. Continued research and development efforts are essential for overcoming these limitations and further advancing the reliability and applicability of vein recognition technology in real-world scenarios.

Electroencephalography

Electroencephalography (EEG) is a technique used to measure and record electrical signals produced by the brain. These signals represent the combined activity of numerous neurons in the cerebral cortex, providing insights into the

[12] Finger vein recognition biometrics. (2021, August 20). Identity Verification Software & Mobile Check Deposit | Mitek. https://www.miteksystems.com/blog/finger-vein-recognition-biometrics

functioning of both the central and autonomic nervous systems.[13] Unlike conventional biometric methods such as fingerprints and retinal scans, which are susceptible to forgery and hacking, EEG signals offer a more secure alternative due to their inherent complexity and difficulty in replication

Despite the robustness of EEG signals against hacking attempts, the practical implementation of EEG-based biometric systems remains limited. One significant challenge is the sensitivity of EEG signals to various physical and mental states of individuals. EEG signals exhibit different frequencies corresponding to different neural states of brain activity, typically categorized into resting state and event-related potential (ERP). Resting state EEG recordings capture brain activity during idle or relaxed conditions, while ERP recordings measure voltage changes in response to specific stimuli.

Although resting state EEG may seem ideal for biometric applications due to its simplicity in data acquisition, it presents challenges due to the inherent ambiguity arising from the lack of experimental control over users' mental states. The variability in individuals' cognitive and emotional states during resting conditions complicates the interpretation and standardization of EEG signals for reliable biometric identification.

Addressing these challenges requires advancements in signal processing techniques and the development of standardized protocols for acquiring and analyzing EEG data. Additionally, research efforts are needed to explore alternative approaches, such as leveraging ERP signals, which offer more controlled and context-specific brain responses to external stimuli. By overcoming these hurdles, EEG-based biometric systems hold great promise for enhancing security and privacy in various applications, ranging from access control to personalized authentication.

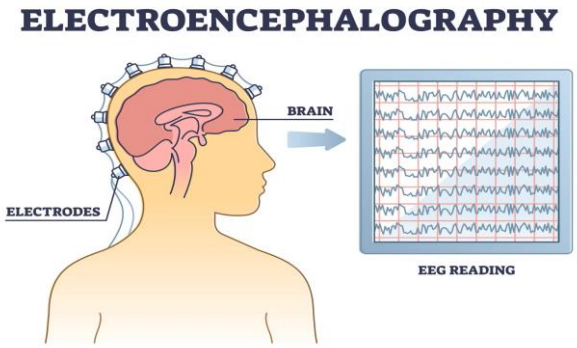

Figure 1: An Electroencephalography[14]

[13] Review on EEG-based authentication technology. (2021, December 24). Publishing Open Access research journals & papers | Hindawi. https://www.hindawi.com/journals/cin/2021/5229576/

[14] What is an electroencephalogram (EEG) test? (2023, September 19). Simply Psychology. https://www.simplypsychology.org/what-is-an-eeg.html

Industries capitalizing on Biometrics

Airports

Biometric technologies have become integral to the operations of airports, streamlining the travel process and enhancing security measures. Many airports now leverage mobile phone applications to facilitate efficient check-in procedures for passengers. For instance, London's Heathrow Airport and Athens International Airport have partnered with digital identity companies to enable travelers to verify their identity using facial recognition technology on their mobile devices. Passengers can store their tickets digitally and use their faces for identity verification throughout the airport.

Similarly, collaborations between airlines and biometric technology providers, such as Elenium Automation and Etihad Airways, allow travelers to register their biometric data via smartphone before embarking on their journey. This pre-registration enables passengers to drop off their baggage seamlessly without the need for additional check-in procedures, as their identity is authenticated automatically through facial recognition technology. Baggage is assigned to a unique biometric token, eliminating the need for traditional tags, while personalized information is displayed via airport monitors.

Another significant advancement in airport biometric technology is the widespread implementation of electronic gates (eGates). These automated passport control systems utilize biometric technology to authenticate passengers' identities. Upon scanning the passport, the eGates capture a photo of the passenger's face, which is then compared to the digital image stored in the passport's microchip for verification purposes.

Banking

Financial services have increasingly embraced biometric technologies to enhance security and streamline transactions, with biometric payment being a prominent example. Biometric payment systems, such as Apple Pay and Google Pay, enable users to make purchases at point-of-sale (POS) terminals using facial recognition or fingerprint authentication, eliminating the need for physical cards or passwords.

Moreover, banks leverage biometric verification methods to bolster security, particularly for high-risk transactions like large monetary transfers. One common practice involves scanning a customer's trusted identity document, such as a passport or ID card, followed by a brief biometric facial scan for authentication. This enables banks to verify the identity of customers remotely, without requiring in-person interaction.

The adoption of biometric technologies in financial services is driven by the need to combat fraud and protect customers' assets. By employing biometric authentication methods, financial institutions can significantly reduce the risk of unauthorized transactions and identity theft. Additionally, biometric verification enhances the customer experience by offering a seamless and secure authentication process, thereby fostering trust and confidence in financial transactions.

Military Defense

Biometric technologies play a crucial role in military operations, serving to enhance security, authentication, and communication among military personnel. One such technology is facial recognition, which analyzes unique facial features to accurately identify individuals. This capability is particularly valuable in verifying authorized personnel and minimizing the risk of unauthorized access to sensitive information and classified documents. By providing a secure means of authentication, facial recognition technology facilitates efficient communication and coordination within the armed forces and paramilitary units, thereby bolstering operational security and effectiveness.

Voice biometrics represent another vital component of military communication systems. By analyzing specific vocal characteristics, voice biometric technology ensures secure and reliable voice communication, especially during critical military operations. The use of voice biometrics not only enhances the authentication process but also contributes to efficient decision-making by providing verification of personnel identities. This capability strengthens overall communication reliability and security, thereby improving operational effectiveness in demanding military environments.

Furthermore, wearable biometric devices, such as smartwatches and biometric sensors, offer real-time monitoring capabilities that are invaluable to military personnel. These devices enable continuous data collection and analysis, providing insights into the health and well-being of soldiers. For example, health monitoring features can track stress levels and fatigue among military personnel, ensuring their physical and mental well-being during operations. Additionally, wearable devices equipped with GPS technology enable military commanders to monitor the real-time location of personnel, enhancing safety, coordination, and situational awareness on the battlefield.

Risks Biometric Technologies pose to Human Rights

Privacy Challenges and Risks

With the widespread adoption and rapid expansion of biometric technologies, concerns regarding human rights violations, individual privacy, identity protection, and the safeguarding of personal data have become increasingly prominent. These technologies present various risks and dangers that need to be addressed comprehensively.

Firstly, a significant threat arises from the compromise of users' personal privacy. Physiological identifiers such as fingerprints and iris recognition are inherently unique to each individual and cannot be easily modified like traditional authentication methods such as passwords. Therefore, the misuse or unauthorized access to such biometric data can lead to severe privacy breaches.

Another pressing concern is the phenomenon known as "function creep," which refers to the gradual expansion of a technology's usage beyond its original intended purpose, often resulting in potential invasions of privacy.[15] Function creep becomes alarming when individuals are unaware of the secondary use of their personal information at the time of its collection. For example, an organization collecting facial biometric information for access control purposes may later utilize this data for unrelated purposes such as monitoring employee performance, productivity, or work hours without the individual's consent.

Additionally, the covert or passive collection of individuals' biometric information without their explicit consent, participation, or knowledge poses a significant risk. Consent, traditionally based on a transactional model, allows individuals to make informed choices about the collection and usage of their personal information. Any collection of personal data without consent may violate regulations such as the GDPR (General Data Protection Regulation), which prohibits the processing of personal data without lawful justification or consent.[16] An example of convert or passive collection of personal information is the facial biometric information that can be captured from photographs of which the users were not aware.

---

[15] "FUNCTION CREEP Definition and Meaning | Collins English Dictionary." *Collins Dictionaries*, 8 Feb. 2024, www.collinsdictionary.com/dictionary/english/function-creep#:~:text=function%20creep%20in%20British%20English,to%20potential%20invasion%20of%20privacy.

[16] "Consent - General Data Protection Regulation (GDPR)." *General Data Protection Regulation (GDPR)*, 22 Oct. 2021, gdpr-info.eu/issues/consent/#:~:text=Processing%20personal%20data%20is%20generally,Data%20Protection%20Regulation%20(GDPR).

Biometric hacking presents yet another privacy risk associated with the use of biometric technologies. If an attacker gains unauthorized access to an individual's biometric data, they can exploit it to impersonate the victim and gain access to sensitive accounts and confidential information. Biometric data, considered highly valuable by hackers due to its uniqueness to each individual, can include physiological identifiers like DNA samples, raising concerns about bodily privacy infringements.

Bias and Racial Discrimination

Another critical aspect to consider when addressing the risks posed to human rights by biometric technologies is the issue of bias and racial discrimination. While face recognition algorithms often boast high classification accuracy rates of over 90%, these results are not consistent across all demographic groups. The "Gender Shades" project, for instance, applied an intersectional approach to assess three gender classification algorithms developed by IBM and Microsoft. Subjects were categorized into four groups based on skin tone and gender. The findings revealed significant discrepancies, with all three algorithms exhibiting the poorest performance on darker-skinned females and the best performance on lighter-skinned males. These disparities have prompted immediate action from companies like Microsoft and IBM, which have pledged to address bias by improving data collection practices and making their technologies more inclusive.

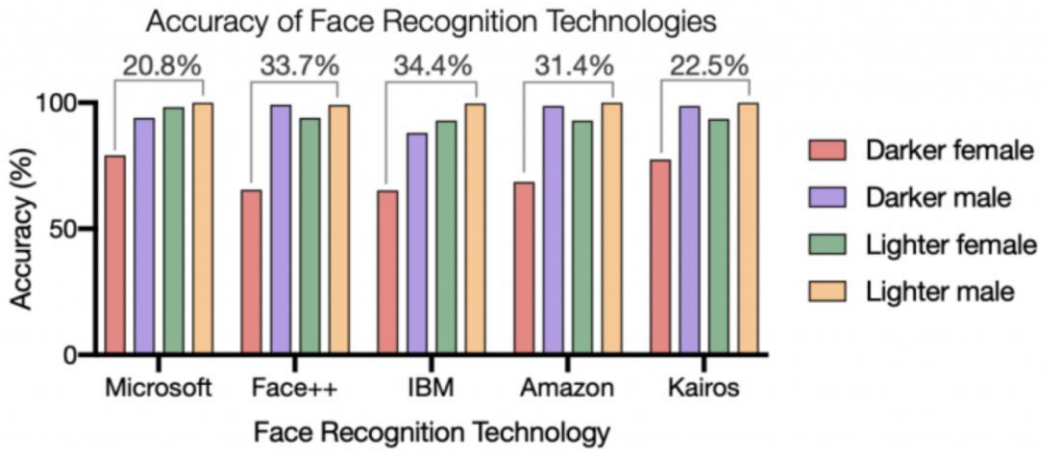

Figure 2: Auditing five face recognition technologies. The discrepancies the Gender Shades project revealed.[17]

Additionally, there's a risk of racial discrimination by law enforcement agencies using biometric technologies. Drawing parallels to historical injustices like the lantern laws in 18th-century New York, concerns have been raised about the potential inequity in face recognition algorithms, particularly in their impact

[17] Jo. *Gender Shades*. gendershades.org/overview.html.

on marginalized communities such as the Black population. Events like the murder of George Floyd by the Minneapolis Police Department have further underscored the existence of systemic racism within law enforcement, highlighting the potential for racial bias and discrimination in the use of facial recognition technology.

Furthermore, the overrepresentation of Black individuals in mugshot databases due to systemic biases in law enforcement practices exacerbates the issue. Because facial recognition algorithms often rely on mugshots for training data, this overrepresentation can result in disproportionately high rates of false positives and wrongful arrests for Black individuals. For example, the New York Police Department's database of "gang affiliates" is overwhelmingly comprised of Black and Latinx individuals, with little to no requirements for proving suspected gang affiliation.[18]

The presence of racial bias and discrimination in biometric technologies contravenes several international human rights instruments, including the Universal Declaration of Human Rights (UDHR), the International Convention on the Elimination of all Forms of Racial Discrimination (ICERD), and the International Covenant on Civil and Political Rights (ICCPR). These violations undermine individuals' rights to non-discrimination, equity before the law, privacy, and effective protection and remedies, as outlined in these international agreements. Consequently, the use of biometric technologies can result in breaches of international law and human rights, posing significant risks to both individuals and the broader international community in terms of security, privacy, and safety.

Case Studies of Human Rights Violations

There are numerous instances that highlight human rights violations stemming from the use of biometric technologies. One such example involves a Swedish school that incurred fines from the Swedish Data Protection Authority (DPA) for utilizing facial recognition technology to track attendance. This practice involved processing biometric data, a violation of the General Data Protection Regulation (GDPR), particularly Article 9, which prohibits the processing of sensitive biometric data without explicit consent.[19] This action further infringed upon Article 12 of the UDHR[20],

[18] SITNFlash. "Racial Discrimination in Face Recognition Technology - Science in the News." *Science in the News*, 26 Oct. 2020, sitn.hms.harvard.edu/flash/2020/racial-discrimination-in-face-recognition-technology.

[19] "Art. 9 GDPR – Processing of Special Categories of Personal Data - General Data Protection Regulation (GDPR)." *General Data Protection Regulation (GDPR)*, 30 Aug. 2016, gdpr-info.eu/art-9-gdpr.

[20] https://www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%2012,against%20such%20interference%20or%20attacks.

Article 8 of the European Convention on Human Rights (ECHR)[21], and Article 16 of the Convention on the Rights of the Child.[22] These violations concern the rights of an individual to consent to the processing of personal and private data, and respect for a private life.

Another example is the Clearview AI and the fine of 20 million by the French DPA in 2022. The DPA required that the platform not use the biometric data of individuals in France without a legal basis and that the already collected data be deleted on the legal basis of the GDPR. The DPA found that this platform breached several articles under the GDPR as it had collected over 20 billion photographs online from images on social media to establish a "biometric template", of which most people were unaware and did not know about the collection of their sensitive personal data of personal physical characteristics.[23] In this example, the platform Clearview AI violated Articles 5, 6, 7, 9 and 14 of the GDPR, article 12 of the UDHR and Article 17 the ICCPR.[24] All of these violations relate to the rights of An individual to privacy, lawfulness during the processing of personal data and information, consent and transparency.

There are also examples of human rights violations by biometrics hacking, thus emphasizing the need for safer platforms for personal and sensitive biometric data to be stored. In 2015, the U.S. Office of Personnel Management (OPM) experienced a situation of hacked biometric information, which compromised the personal information of over 21 million people. This event is one of the largest known biometric data breaches, as hackers had access to the fingerprints of more than 5.6 million individuals. Consequently, hackers not only violated the rights of these individuals, but they could also impersonate them. This data breach raised questions and concerns as to how the data was able to be hacked and if databases can be easily hacked to gain access to sensitive information. Indeed, Nasir Memon, a New York University professor of computer science and engineering, conducted a research which showed that Android devices were flawed in how they handled fingerprint data.[25] His research illustrated how fingerprint data could be extracted and used for the creation of a 3D replica of the fingerprint of the user. Nasir Memon also discovered that this data was not encrypted, and thus easier to get stolen. All of these examples raise concerns as

[21] https://www.equalityhumanrights.com/human-rights/human-rights-act/article-8-respect-your-private-and-family-life#:~:text=and%20family%20life-,Article%208%20protects%20your%20right%20to%20respect%20for%20your%20private,and%20emails%2C%20for%20example).

[22] https://www.coe.int/en/web/compass/convention-on-the-rights-of-the-child#:~:text=Article%2016,his%2Fher%20honour%20and%20reputation.

[23] Blessing. "Biometric Data and Privacy: Issues Arising - Hedman." *Hedman*, 5 Dec. 2023, hedman.legal/articles/biometric-data-and-privacy-issues-arising.#

[24] OHCHR. "International Covenant on Civil and Political Rights." *OHCHR*, www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights.

[25] Goel, Vindu. "That Fingerprint Sensor on Your Phone Is Not as Safe as You Think." *The New York Times*, 11 Apr. 2017, www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html.

to how biometric data and personal information are stored, how the human rights of the users are respected and how this data is protected from malicious purposes.

MAJOR COUNTRIES AND ORGANIZATIONS INVOLVED

United States of America (USA)

The United States of America has introduced biometric technologies to have security, efficiency and safety. The US Custom and Border Protection has successfully implemented facial biometrics into 238 airports, 92 pedestrian crossings and 40 open loop entry points. According to the CBP, up to date, CBP has processed more than 300 million travelers using biometric facial comparison technology and prevented more than 1,900 impostors from entry to the U.S. [26] However, the USA does not have a federal law regarding the tackling of the use of biometric information, but the state of Illinois has the Biometric Information Protection Act (BIPA). BIPA sets specific regulations and obligations of the organizations in control of biometric data. BIPA does oblige organizations to get the written consent of the data subject before they process biometric data. But comparatively, the BIPA is not as effective as the GDPR since the penalties are much lower. Moreover, following BIPA, more states such as California, Texas and Washington have enhanced their privacy laws. Overall, although there have been certain efforts to regulate the safe use of biometrics technologies, due to the inexistence of a federal law regarding privacy, the issue has not been addressed efficiently.

South Africa

The Republic of South Africa has worked towards addressing the dangers biometric technologies pose. The Protection of Personal Information (POPIA) was the first legal document that introduced the term “biometrics” into South African law. According to POPIA, biometrics are defined as a “technique of personal identification based on physical, physiological or behavioral characterization…”. [27] While there is a general prohibition on the processing of biometric information with the protection of biometric information as special information, the Act does give general authorization and specific authorization for different types of special and biometric information. As for the use of biometric technologies, the primary type of biometric technology is fingerprints with an increasing number of organizations utilizing fingerprints, facial and voice recognition. Thulani Mavuso, deputy director general for institutional planning and support at the Department of Home Affairs (DHA) disclosed plans to develop and expand infrastructure for such technologies in some of the country’s

[26] “Biometrics.” U.S. Customs And Border Protection, www.cbp.gov/travel/biometrics.

[27] Michalsons. “Biometric Laws Around the World.” Michalsons, 22 Jan. 2024, www.michalsons.com/blog/biometrics-laws-around-the-world/42094#:~:text=Biometrics%20under%20POPIA&text=Biometrics%20are%20defined%20as%20a,information%20as%20special%20personal%20information.

ports of entry by the DHA. The system to be used in the 34 existing ports of entry/exit is the Biometric Movement Control System (BMCS) to capture the fingerprint and face biometrics of all travelers getting inside/outside the country. [28]

People's Republic of China

China is fully engaged in biometric technologies, as Beijing pushes biometrics recognition into many areas of the country. An example is Super Red, also known as the Beijing Wanlihong Technology, which makes iris scanning and data-protection software. It claims revenue over 1.43 billion dollars, and it connects to the Chinese Academy of Sciences, which is part of the central government and Communist Party. Another example is the Xinjiang Uyghur Autonomous Region (XUAR)[29]. Xinjiang, is an autonomous region of China and it has been a testbed for AI surveillance systems. It is primarily made up of Uyghurs civilians living in Xinjiang. Human rights groups believe that China has detained more than one million Uyghurs against their will over the past few years in a large network of what the state calls "re-education camps", and sentenced hundreds of thousands to prison terms; but China denies these allegations. In the last decade, the government has funded advancements in facial recognition software and camera and network hardware. The result is an international market for Chinese biometric surveillance systems, while the respective re-education camps in Xinjiang, make a density of equipment.

The Biometrics Institute

The Biometrics Institute was established in 2001 and constitutes an expanding, unbiased platform that welcomes different perspectives to provide a balanced viewpoint on biometrics. It represents “a unique multi-stakeholder community spreading across the globe including a large number of government agencies, banks, airlines, airports, biometric experts, privacy experts, regulators, suppliers and academics as well as international observers such as United Nations agencies, EU institutions and IGOs.”[30] The Biometrics Institute aims to act as a connector to key stakeholders on the topic of global biometrics and facilitate transferring knowledge whilst guiding towards the responsible and ethical use of biometric technologies. Up to date, the Biometrics Institute has collaborated with many government bodies, organizations and corporations to achieve those goals. In fact, the Biometric Institute has collaborated with the United Nations Counter-Terrorism Committee Executive Directorate (CTED) and the United Nations Counter-Terrorism Centre (UNCTC) and released the United Nations’ Compendium of Recommended Practices for the

[28] Macdonald, Ayang. “South Africa Plans Biometric System at Ports of Entry, US and Canada Announce New Deployments.” Biometric Update | Biometrics News, Companies and Explainers, 28 Mar. 2022, www.biometricupdate.com/202203/south-africa-plans-biometric-system-at-ports-of-entry-us-and-canada-announce-new-deployments.

[29] Who are the Uyghurs and why is China being accused of genocide? (2013, April 24). BBC News. https://www.bbc.com/news/world-asia-china-22278037

[30] Biometrics Institute. “About - Biometrics Institute.” *Biometrics Institute*, 7 Dec. 2022, www.biometricsinstitute.org/about/#:~:text=The%20Biometrics%20Institute%20was%20founded,as%20international%20observers%20such%20as.

Responsible Use and Sharing of Biometrics in Counter Terrorism. This compendium provides an overview of biometric technologies and operating systems within the context of counter-terrorism and is aimed at the member States with no to little experience regarding the use of Biometric Technologies in counter-terrorism.

United Nations High Commissioner for Refugees (UNHCR)

Since 2004, the United Nations High Commissioner for Refugees (UNHCR) has been trying to use biometric technologies as a way of providing refugees food, water, shelters, money, and education. They have achieved this with the creation of an ID Card which is made by collecting a photograph, iris scans, fingerprints, personal and family history, health data, and all available prior legal documentation of the refugee in question. According to a January 2020 UN report, eight out of every 10 refugees registered with the UNHCR, or about 37 million, has already been biometrically tagged and entered into the organization's Global Distribution Tool (GDT). The UNHCR began to expand this project called "Project Profile'' in 2013 with the development of Biometric Identity Management System (BIMS). It was officially launched in 2015 and the registration process takes seconds and allows the UNHCR to provide refugees a UN ID card. Regarding the card's validity period, it is decided by the operation, and host governments. In some contexts, it may be appropriate to follow the national standard for validity relating to ID documents. In others, the operation may choose to establish a shorter validity period in order to be able to verify the population more frequently.

Figure 3: UNHCR ID Card[31]

[31] Documentation – UNHCR – Guidance on registration and identity management. (n.d.). UNHCR, the UN Refugee Agency | UNHCR.https://www.unhcr.org/registration-guidance/chapter5/documentation/

TIMELINE OF EVENTS

DATE	DESCRIPTION OF EVENT
1901	The "first British fingerprint files" are installed by a British police officer.
1903	Fingerprint identification for criminals is established in the United States in a New York prison.
6 September 1947	The International Biometric Society (IBS) is established.
10 December 1948	The Universal Declaration of Human Rights is proclaimed by the United Nations General Assembly.
14 December 1950	The Office of the United Nations High Commissioner for Refugees (UNHCR) is established by the General Assembly.
21 December 1965	The United Nations General Assembly adopts the International Convention on the Elimination of All Forms of Racial Discrimination.
20 November 1989	The United Nations Convention on the Rights of the Child is signed by 140 Member States.
October 1995	The European Union (EU) Data Protection Directive is enacted.
9 September 2001	The extremist group of Al-Qaeda launches airline attacks against the United States.
October 2001	The Biometrics Institute is established.
2007	The National Science & Technology Council (NSTC) releases the NSTC Policy for Enabling the Development, Adoption and Use of Biometric Standards.
25 May 2018	The General Data Protection Regulation (GDPR) is put into effect.
29 June 2018	The United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism is released.

PREVIOUS ATTEMPTS TO SOLVE THE ISSUE

The United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism

The United Nations Compendium of Recommended Practices for the Responsible Use and Sharing of Biometrics in Counter-Terrorism was created by the United Nations Working Group on Border Management and Law Enforcement related to Counter-

Terrorism, in cooperation with the Biometrics Institute. The goal of the Compendium is to reach Member States with limited technical knowledge, experience and capacity regarding the use and misuse of biometric technologies. It also aims to improve the capacity of Member States and international and/or regional bodies to ensure and promote the responsible and ethical collection and use of biometric information and safety and privacy of all individuals. The Compendium includes an extensive overview of the responsible and ethical use of biometric technologies and recommended practices in Counter-Terrorism, which addresses the topics of data protection, human rights, privacy and vulnerability assessments.

Rising pan-European and International Awareness of Biometrics and Security Ethics (RISE)

RISE is a coordination action[32] which lasts for three years, organized by the Community Research and Development Information Service (CORDIS) of the European Commission. It aims to deepen and ensure continuity to European and international dialogue. Its primary goal is to maintain a global dialogue and all Member States to be constantly informed about the latest developments of the biometric industry and be always involved when it comes to international law and safety. The international conferences will debate upon ethical issues arising from the use of biometrics, and there will be reports detailing discussed issues, while press releases and websites that will share further information.

POSSIBLE SOLUTIONS

Implementing regulations for Artificial Intelligence (AI)

Artificial Intelligence has not only created chatbots and is not only able to generate pictures or well written essays, but it is also an eminent part of biometric technologies, as it is used to make such techniques more efficient and precise. Living in the digital age, obeying the rules of a government regarding the use of Artificial Intelligence can be intimidating as we have seen in the past, and many tech leaders are worried about where the consequences of AI's exploitation might lead to. An open letter has been signed by more than one thousand researchers and CEOs, urging for a moratorium on the development of AI. "The pause would provide time to introduce *shared safety protocols* for A.I. systems, the letter said. *If such a pause cannot be enacted quickly, governments should step in and institute a moratorium*, it added."[33] Strengthening or implementing laws, could eliminate possible dangers and not leave space for manipulation of this powerful weapon that is a threat to our society as we know it.

[32] Coordination. (n.d.). Department of Computing | Faculty of Engineering | Imperial College London. https://www.doc.ic.ac.uk/project/examples/2005/163/g0516319/coordination.html

[33] Nytimes.com. (2023, March 29). The New York Times - Breaking News, US News, World News and Videos. https://www.nytimes.com/2023/03/29/technology/ai-artificial-intelligence-musk-risks.html

UN Compendium

"UN Compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism" is a document written in association with the Biometric Institute. It provides an overview of Biometric Technology and "It is aimed primarily at Member States who may have little or no experience of biometric applications and who may also face technical assistance and capacity building challenges when implementing this technology."[34] It discusses main elements of biometric technology and the use of biometrics in the fields of forensic science and law enforcement investigations and the additional complexity that this presents. On the note of law enforcement, another section of the document deals with the governance and regulatory requirements for biometric technology from the perspectives of international law, human rights law, ethical reviews, data protection requirements and the right to privacy. Finally, it presents potential vulnerabilities of biometric systems and some of the control measures that can be used to mitigate the risks. It is important that this document is read and implemented by all Member States, as it can enhance governments' ability to deal with upcoming problems due to the excessive use of biometric technologies.

Establishment of an international legal framework for the regulation of Biometric Technologies

Another possible solution could be the establishment of a regulatory, international legal framework that will set specific standards for the use of biometric technologies to address human rights violations efficiently. This can be achieved through the collaboration of UN bodies such as the United Nations Office of the High Commissioner for Human Rights (OHCHR), the International Telecommunication Union (ITU) and the United Nations Human Rights Council (UNHRC) with other organizations, like the Biometrics Institute. This would ensure the ethical and efficient use of biometric technologies and sanctions for human rights violations, providing a sense of security to human beings.

Bias mitigation

Bias in biometric technologies can perpetuate unfair outcomes and discriminatory practices, making bias mitigation strategies crucial for ensuring fairness and equity. Diverse and representative datasets are foundational for training biometric algorithms, as they help mitigate the risk of biases being amplified in the system. Continuous monitoring and testing of biometric systems for bias across different demographic groups are essential to identify and address any disparities or discriminatory patterns. Implementing bias correction techniques, such as algorithmic

[34] UN compendium of recommended practices for the responsible use and sharing of biometrics in counter-terrorism. (n.d.). Welcome to the United Nations. https://www.un.org/securitycouncil/ctc/content/un-compendium-recommended-practices-responsible-use-and-sharing-biometrics-counter-0

adjustments or data preprocessing methods, can help mitigate the impact of biases identified in biometric systems. Additionally, fostering collaboration among diverse stakeholders, including researchers, developers, policymakers, and community representatives, is vital for developing comprehensive solutions to bias mitigation.

BIBLIOGRAPHY

"Biometric Technology." Biometric Technology - an Overview | ScienceDirect Topics, www.sciencedirect.com/topics/computer-science/biometric-technology.

Gillis, Alexander S., et al. "What Is Biometrics?" Security, TechTarget, 26 July 2021, www.techtarget.com/searchsecurity/definition/biometrics.

Ikeda, Scott. "Breach of Biometrics Database Exposes 28 Million Records Containing Fingerprint and Facial Recognition Data." CPO Magazine, 13 Apr. 2020, www.cpomagazine.com/cyber-security/breach-of-biometrics-database-exposes-28-million-records-containing-fingerprint-and-facial-recognition-data/.

"Identification and Biometric Technology - Social Protection and Human Rights." Social Protection and Human Rights, 11 June 2015, socialprotection-humanrights.org/key-issues/administration-and-delivery-of-benefits-and-services/identification-and-biometric-technology.

"Biometrics: Definition, Use Cases, Latest News." Thales Group, www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics.

Zarkowsky, Andrew. "Biometrics: An Evolving Industry with Unique Risks." The Hartford, 20 May 2021, www.thehartford.com/insights/technology/biometrics.

Editor, CSRC Content. "Biometrics - Glossary: CSRC." CSRC Content Editor, csrc.nist.gov/glossary/term/biometrics.

"What Is Authentication? Definition of Authentication, Authentication Meaning." The Economic Times, economictimes.indiatimes.com/definition/authentication.

"Data Breach." CyberArk, 20 Apr. 2023, www.cyberark.com/what-is/data-breach/.

Editor, CSRC Content. "Privacy - Glossary: CSRC." CSRC Content Editor, csrc.nist.gov/glossary/term/privacy.

"Personal Data." General Data Protection Regulation (GDPR), 22 Oct. 2021, gdpr-info.eu/issues/personal-data/.

Clark, Mary. "How Does Biometric Technology Impacts Society?" Bayometric, 8 Aug. 2018, www.bayometric.com/biometric-technology-impacts-society/.

"Human Rights." United Nations, www.un.org/en/global-issues/human-rights.

"International Journal of Engineering Research & Technology." IJERT, www.ijert.org/.

"Ibia." IBIA, www.ibia.org/.

Biometric Organizations, www.ibia.org/cbeff/iso/biometric-organizations.

"Biometric Identity Management System." UNHCR, www.unhcr.org/media/biometric-identity-management-system.

Ahmed, Farzi. "A Historical Timeline of Biometric Authentication." ClockIt, 1 Sept. 2023, clockit.io/historical-timeline-biometric-authentication/.

Mitek. "What Are Biometrics in the Digital World." Mitek, 10 Nov. 2022, www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics.

"African Countries Embracing Biometrics, Digital Ids | Africa Renewal." United Nations, www.un.org/africarenewal/magazine/february-2021/african-countries-embracing-biometrics-digital-ids.

Dbarreto. "Racial Bias in Facial Recognition Algorithms." Amnesty International Canada, 8 June 2023, www.amnesty.ca/surveillance/racial-bias-in-facial-recognition-algorithms/.

"'immature Biometric Technologies Could Be Discriminating against People' Says ICO in Warning to Organisations." ICO, ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/10/immature-biometric-technologies-could-be-discriminating-against-people-says-ico-in-warning-to-organisations/.

"Misuse of Personal Data and Biometrics." NAACP, 13 June 2022, naacp.org/resources/misuse-personal-data-and-biometrics.

Tsui, Quito. "New Report: Biometrics in the Humanitarian Sector [2023]: The Engine Room." The Engine Room | Accelerating Social Change., 2 Aug. 2023, www.theengineroom.org/biometrics-humanitarian-sector-2023/.

Gavin. “The Top 9 Common Uses of Biometrics in Everyday Life - NEC NZ.” NEC, 11 Oct. 2021, www.nec.co.nz/market-leadership/publications-media/the-top-9-common-uses-of-biometrics-in-everyday-life/.

“Questioning the Use of Biometric Technology in Humanitarian Response - World.” ReliefWeb, 17 Mar. 2018, reliefweb.int/report/world/questioning-use-biometric-technology-humanitarian-response.

Utilities one. (2023, November 18). Utilities One. https://utilitiesone.com/exploring-biometric-technologies-for-secure-military-communication#anchor-0

Rushing, Elizabeth. “Biometrics in Humanitarian Action: A Delicate Balance.” Humanitarian Law & Policy Blog, 2 Sept. 2021, blogs.icrc.org/law-and-policy/2021/09/02/biometrics-humanitarian-delicate-balance/.

Jul 21, 2023. “International Biometrics + Identity Association (IBIA): Biometric Update.” Biometric Update |, 11 Dec. 2018, www.biometricupdate.com/companies/international-biometrics-identity-association-ibia.

“European Association for Biometrics.” EAB, 26 June 2023, eab.org/.

“Biometric Data and Privacy Laws (GDPR, CCPA/CPRA).” Thales Group, www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data.

Welcome to the United Nations, www.un.org/securitycouncil/ctc/sites/www.un.org.securitycouncil.ctc/files/files/documents/2021/Jan/compendium_on_biometrics_ch.pdf.

Marketing, CDVI, and CDVI Marketing. “Biometrics & GDPR: Stay Compliant with Biometrics: Ievo.” Ievo Ltd, 10 June 2020, ievoreader.com/biometrics-and-the-gdpr-why-you-should-adopt-the-technology/.

National Institute of Standards and Technology, www.nist.gov/system/files/documents/2019/12/06/00-20-h133_final120419web.pdf.

Biometrics En Final April2022 - UNHCR, help.unhcr.org/jordan/wp-content/uploads/sites/46/2022/04/Biometrics-EN_Final_April2022.pdf.

“USA Border Plan Requires ‘Continuous and Systematic’ Transfers of Biometric Data.” Statewatch, www.statewatch.org/news/2023/april/usa-border-plan-requires-continuous-and-systematic-transfers-of-biometric-data/.

Katja Drinhausen, "China's Handling of Biometric Data: Trends and Implications for Europe." Merics, merics.org/en/events/chinas-handling-biometric-data-trends-and-implications-europe.

Knight, Will. "China Is the World's Biggest Face Recognition Dealer." Wired, Conde Nast, 24 Jan. 2023, www.wired.com/story/china-is-the-worlds-biggest-face-recognition-dealer/.

"Universal Declaration of Human Rights." United Nations, www.un.org/en/about-us/universal-declaration-of-human-rights.

"What Is GDPR, the EU's New Data Protection Law?" GDPR.Eu, 14 Sept. 2023, gdpr.eu/what-is-gdpr/.

"Security Council - Counter-Terrorism Committee (CTC) | Counter-Terrorism Committee Executive Directorate (CTED)." United Nations, www.un.org/securitycouncil/ctc/.

CORDIS, cordis.europa.eu. "Final Report Summary - Rise (Rising Pan-European and International Awareness of Biometric and Security Ethics): FP7: CORDIS: European Commission." CORDIS, 12 Aug. 2009, cordis.europa.eu/project/id/230389/reporting.

Unusual biometric techniques. (2013, November 14). Security Solutions Media. https://www.securitysolutionsmedia.com/2013/11/14/unusual-biometric-techniques/

Are fingerprints determined by genetics?: MedlinePlus genetics. (n.d.). MedlinePlus - Health Information from the National Library of Medicine. https://medlineplus.gov/genetics/understanding/traits/fingerprints/

Finger vein recognition biometrics. (2021, August 20). Identity Verification Software & Mobile Check Deposit | Mitek. https://www.miteksystems.com/blog/finger-vein-recognition-biometrics

Biometrics for industry 4.0: A survey of recent applications. (n.d.). PubMed Central (PMC). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10230486/

Vein recognition. (n.d.). FindBiometrics. https://findbiometrics.com/solutions/vein-recognition/

EEG Based biometric system. (n.d.). Science Direct . https://www.sciencedirect.com/science/article/abs/pii/S1746809422003123

History of biometrics. (2018, July 20). Biometric Update |. https://www.biometricupdate.com/201802/history-of-biometrics-2

The history of biometric authentication. (n.d.). Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-biometric-authentication

Eigenfaces - Scholarpedia. (n.d.). https://www.scholarpedia.org/article/Eigenfaces

Race and statistics in facial recognition: Producing types, physical attributes, and genealogies. (n.d.). PubMed Central (PMC). https://www.ncbi.nlm.nih.gov/pmc/articles/PMC10696907/

The history of biometric authentication. (n.d.). Thales Group. https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-biometric-authentication

Mastercard biometric payment card | Fingerprint authentication. (n.d.). Mastercard - A Global Technology Company in The Payments Industry. https://www.mastercard.us/en-us/business/overview/safety-and security/authentication-services/biometrics/biometrics-card.html

Documentation – UNHCR – Guidance on registration and identity management. (n.d.). UNHCR, the UN Refugee Agency | UNHCR. https://www.unhcr.org/registration-guidance/chapter5/documentation/

Documentation – UNHCR – Guidance on registration and identity management. (n.d.). UNHCR, the UN Refugee Agency | UNHCR. https://www.unhcr.org/registration-guidance/chapter5/documentation/

Who are the Uyghurs and why is China being accused of genocide? (2013, April 24). BBC News. https://www.bbc.com/news/world-asia-china-22278037

Garcia-Rojas, Claudia. “The Surveillance of Blackness: From the Trans-Atlantic Slave

Trade to Contemporary Surveillance Technologies.” *Truthout*, 3 Mar. 2016, truthout.org/articles/the-surveillance-of-blackness-from-the-slave-trade-to-the-police.

Goel, Vindu. “That Fingerprint Sensor on Your Phone Is Not as Safe as You Think.” *The New York Times*, 11 Apr. 2017, www.nytimes.com/2017/04/10/technology/fingerprint-security-smartphones-apple-google-samsung.html.

Jo. *Gender Shades*. gendershades.org/overview.html.

Michalsons. “Biometric Laws Around the World.” *Michalsons*, 22 Jan. 2024, www.michalsons.com/blog/biometrics-laws-around-the-world/42094#:~:text=Biomtrics%20under%20POPIA&text=Biometrics%20are%20defined%20as%20a,informatin%20as%20special%20personal%20information.

“Biometric Laws Around the World.” *Michalsons*, 22 Feb. 2024, www.michalsons.com/blog/biometrics-laws-around-the-world/42094.

Today, Brad Heath Usa. “Racial Gap in U.S. Arrest Rates: ‘Staggering Disparity.’” *USAToday*, 19 Nov. 2014, eu.usatoday.com/story/news/nation/2014/11/18/ferguson-black-arrest-rates/19042077.

United Nations. “Universal Declaration of Human Rights | United Nations.” *United Nations*, www.un.org/en/about-us/universal-declaration-of-human-rights#:~:text=Article%12,against%20such%20interference%20or%20attacks.