Biometrics as Authentication:

An Exploration of Privacy, Failures and Regulations.

Navya Shah

USC ID: 4062254582

DSCI 429

I have read the Guide to Avoiding Plagiarism published by the student affairs office. I understand what is expected of me with respect to properly citing sources, and how to avoid representing the work of others as my own. The material in this paper was written by me, except for such material that is quoted or indented and properly cited to indicated the sources of the material. I understand that using the words of others, and simply tagging the sentence, paragraph, or section with a tag to the copied source does not constitute proper citation and that if such material is used verbatim or paraphrased it must be specifically conveyed (such as through the use of quotation marks or indentation) together with the citation. I further understand that overuse of properly cited quotations to avoid conveying the information in my own words, while it will not subject me to disciplinary action, does convey to the instructor that I do not understand the material enough to explain it in my own words, and will likely result in a lesser grade on the paper.

Signed: Navya Shah

Introduction

Whether you realize it or not, daily, you give up some of your most personal information that is so innately identifiable to you: your biometric information. It could be your face in a security camera, fingerprint access into your office building, face ID on your phone, or even your photo library constantly conducting facial recognition. Biometric information can stretch so much to include your behavioral patterns, such as the way you type, the tone of your voice, your gait, and so on. In the background, algorithms are constantly running to scan information that truly defines you and collect it. It raises the question of how private it is or whether it can ever be private. In this paper, I will explore these questions to understand the privacy aspects of data collection, especially on a global scale, and how internet governance differs. I also want to compare biometric uses for identification beyond just authentication, examining the privacy concerns behind these processes. Lastly, I will explore the weaknesses of using biometric information and the types of failures that can occur. Once I have established a thorough understanding of biometric data usage, privacy, and weaknesses, I will expand my analysis to examine global perspectives on Internet governance and biometric regulation.

About Biometrics

Before further delving into the topic, it is essential to establish the basics. Biometrics is a part of one of the bases for authentication; something about you. It is information that is inherently about you and can include various human features, including behavioral characteristics. Most biometrics would combine the two, consisting of your identifying feature and your behavior. The technology sounds very sophisticated and advanced. However, it is present in almost every authentication, using something about you that is unbeknownst to you. Take your computer's fingerprint unlock as an example; not only does it register your fingerprint and match it to the saved prints, but it also picks up on the input device's usage, which includes how you touch the scanner and the pressure on the sensor, which is behavioral. Thus, the recognition engine inputs a combination of physiological and behavioral characteristics (Abdulla, 2023). Such a distinction can also help distinguish between family members regarding their physiological features, as they can often be shared from birth or picked up over time, such as how you talk or your gait. Furthermore, it can help to tell twins apart as facial features might be the same, but the way the features are conveyed depends on their behavior, which cannot be completely the same. For a system, there are various biometrics that can be used for authentication. The choice of a biometric depends on various factors such as Universality, uniqueness, permanence, collectability, performance, acceptability, and circumvention. Universality outlines how the system should be accessible and authenticated by everyone, as in the trait everyone should possess. Uniqueness refers to how the trait should be distinct to an individual. Permanence refers to having a trait that does not just fade over time or is temporary in nature. Acceptability points to the idea that using biometrics should be widely acceptable such that the user is willing to present it to the system. Circumvention is also factored in to consider how easily the trait can be replicated and the system could potentially be compromised, much like a spy movie where they make artificial fingers to bypass systems (Abdulla, 2023). Keeping these factors in mind, it is easy to tell how fingerprints are the most common form of biometric authentication. This is also largely due to the balance that the systems must strike between making it less precise to allow more people to get in or making it more precise to limit access but also frustrate the user.

The lack of balance has reduced the development of biometric authentication to be more for convenience rather than for added security.

Types of Failure

To further understand biometric authentication, the weaknesses and failures must also be discussed. Like any system, biometric systems have flaws as well, and they have been classified into four main types: Type I error, Type II error, Type III error, and Crossover Error (Novriansyah, 2024). The Type I error is the False Rejection Rate (FFR), which happens when the biometric system wrongly rejects an authorized user. This causes issues with providing timely access as it causes user frustration and access delay to the system. Type II error is the False Acceptance Rate (FAR), which outlines the scenario of a system accidentally accepting an unauthorized user. This would create significant security risks as it exposes sensitive information to users who shouldn't be allowed to see it, causing serious problems in a high-sector environment. Thus, this is considered the most crucial type of error and must be extensively prevented. Type III error, the misidentification error, is when a system matches a user's biometric to a different identity. The mismatch can lead to issues with authorization of access to sensitive information. It can also lead to problems in tracking or auditing user information, which can compromise security measures in place. There is also the Crossover Error Rate (CER), which occurs when FFR is equal to FAR. This serves as a measure to analyze the accuracy of the biometric system. A lower CER is better and indicates a sound biometric system whereas a higher rate signals trouble (Novriansyah, 2024).

These possible errors bring to focus the weakness of the biometric system in maintaining data integrity. To ensure the integrity of data, the system must make sure the data is reliable by ensuring accuracy and no alterations. The integrity is impacted by a variety of factors, such as the quality of the collection through a camera or a sensor, the storage and management of the data, and access control to maintain unaltered data. Since sensors are the collection point for data, they largely impact the quality and accuracy of verification. The class lecture on the Internet of Things touched upon this concept as well, and we discussed the security and efficacy of sensors in promoting usability and ensuring the protection of the devices. Likewise, there are concerns of compromised security through sensors in biometrics as well, where adversaries could collect sensitive data of the users. Data integrity is also impacted by the algorithms in place to protect the data storage. Biometrics involves varying data that cannot use the same cryptographic system as passwords. Instead, it employs the fuzzy commitment technique, which closely matches the input with a range of stored encrypted values to allow a little discrepancy when comparing inputs. Let's say you looked a little different today for your Face ID; maybe the lighting is different, but the system would still give you access due to this technique being employed. This algorithm can allow a higher success rate, but the possibility of false positives or misidentification increases, which compromises data integrity (*Pros and cons of fuzzy matching*, 2024). The failures and weaknesses of biometric systems highlight the trade-off between accuracy and accessibility into the systems, which also points to maintaining the balance between the privacy of users and providing them the convenience of this authentication style.

Privacy Concerns and Challenges

To understand the privacy aspects of biometric data collection, it is important to acknowledge the varying applications. Biometric applications are largely used to mitigate cryptographic vulnerabilities as something you know can be found out, and something you have can be stolen. It adds another layer of security to genuinely identify a user, which goes both ways, as having regular cryptographic authentication prevents circumvention (Shahriar, 2024). Applications of biometric authentication exist in three sectors: Commercial, Government, and Forensic.

Commercial applications include general activities on the Internet like e-commerce, net banking, medical record management, etc. Government use cases include social security, passport control, national or state identification issuance or verification. Lastly, forensic usages vary from criminal to DNA sampling for parenthood to even corpse identification (Abdulla, 2023). It can be referenced that these crucial applications require robust privacy measures to protect them. These authentication systems might be sound in privacy in theory; however, the practical measures to protect them are not as well established, making it open to vulnerabilities in how securely the data is maintained. Successful attacks on biometric systems can lead to serious ramifications regarding a person's identity, such as exposing details about their ethnic group, genetic features, medical conditions, etc. Biometric information cannot be kept secret or concealed, and if it is stolen, compromised information cannot be easily revoked, unlike a password that can be changed. This makes such information vulnerable to risks of capturing, cloning, or forgery, which can result in identity theft or individual profiling. Considering the sensitive nature of their applications, when biometrics are used across multiple databases, the risk grows exponentially (Shahriar, 2024). Regardless, the benefits and accuracy of authenticating an individual trumps the usage risk as such practices are largely employed throughout the public sector.

Such privacy concerns build the foundation of issues that arise due to the usage of biometric information. This section covers the various challenges rooted in the aforementioned vulnerabilities. The first to discuss is function creep, which occurs when information is used for a different purpose than what it had originally been collected for. This problem presents itself when usages are not adequately communicated to the users when they agree to provide their information; it could also be due to data breaches. Covert collection is another issue where there is a passive collection of people's biometric data without their consent, participation, or knowledge (*Biometric & Privacy,* 2024). This is very common when considering facial bios that can be captured from public images that someone would not even know are being taken. This can extend to fingerprints being lifted from public spaces. Such a challenge is only set to grow as AI becomes further integrated into our daily lives. Clearview AI is a popular example of the misuse of facial recognition. They faced legal controversy when they installed face scanners to automatically collect images from social media and other public websites (Wang, 2024). Through this issue, another arises of secondary information. It refers to the idea that when collecting some biometric data, there can be secondary information revealed because of that, which differs from the reason and use it was collected for in the first place. An example of this would be collecting a facial scan that could also reveal information about the person's health that they would not want to provide. Furthermore, consent is a crucial issue that biometrics brings up due to the possibility of covert and almost constant collection of data. It limits the ability of users to make choices about their personal information and what is collected when (*Biometric & Privacy,* 2024). With these challenges being so multifaceted, a solution can only arise with robust regulations and sound encryption of data. Regulations can go beyond the legal scope and embody healthy data privacy practices in the public sector as well.

India's Aadhar: A Case Study

In this exploration, it would be helpful to synthesize the points made and express them through an example. After 2014, India laid a heavy focus on developing a robust identification system for their citizens. This was partly because of the lack of such identification existing but also to single out the disenfranchised Muslim population amid religious and political tensions with Pakistan. As a result, India built a massive identification system called Aadhar, which consists of a collection of fingerprints, iris scans, and face photos in the biometric database of approximately 1.2 billion Indian citizens (Sandhya, 2024). For entities, iris or fingerprint patterns authenticate the claimed identities, which means that an Aadhaar number is matched with an individual's biometric information stored. Considering that Aadhar is supposed to be a one-stop shop for all identification needs in the country for such a staggering number of people, there are numerous scopes for vulnerabilities that arise and have dire consequences. This example highlights privacy concerns that can arise in a nationwide context, such as if the biometric data is stolen or copied, it gives up access to an individual's private and confidential information like bank account details, which can lead to financial ramifications (Sandhya, 2024). There can also be unauthorized uses of the collected fingerprints and other scans that are beyond legal scope. Also, this serves as an invaluable tool for surveillance, which can also go against legal provisions as you can track all activity conducted by a person by obtaining something about them that they cannot conceal either. This raises questions about the role of governments in this monitoring; it is also almost as if every user signs up to be a part of an identification-based tracking system where if you are to be found, commit a crime, or your activity needs to be monitoring, it becomes exponentially easier for the government to do so. This system might be a step forward for Digital India, but it exposes an entire nation to vulnerabilities through the use of biometric technology.

Global Regulation

While biometric data privacy is largely dependent on cryptographic protections, which are constantly advancing in this field, it is important to consider the legal considerations for regulation and how they differ globally. This is largely because technological advancements can only do so much as they are limited in their usage. However, policies set in place can enforce the usage and set a standard for data privacy when handling biometrics. As a field in cybersecurity, biometrics is widely under-regulated. The European Union's GDPR provides protections for processing sensitive, private data; however, nothing has been concretely defined for biometrics specifically. The regulations cover almost all types of user data when it is collected; this includes holding the data to the six principles laid out by the GDPR for data processing. GDPR requires opting in rather than being able to opt out of your data collection, but with the unclear collection of biometric information, it is more or less a gray area. However, Article 9(4) of the GDPR would allow EU Member States to set their own conditions regarding the use of biometric data. The European Commission has been considering the issue of biometrics interfering with "human rights, liberty, intimacy, human dignity and privacy" and that using a biometric system must be in line with the European Convention on Human Rights and with the Data Protection Directive (Dewa, 2017). Additionally, due to the existence of transborder data flows, the Court of Justice of Europe (CJEU) will extend its jurisdiction to lay enforcement of data privacy regulations on non-EU entities that handle or process the data of EU citizens or residents (Dewa, 2017). As it can be seen, the scope of the GDPR is robust and overarching. However, it can be difficult to single out issues with biometric data regulation when frameworks are so broad.

In the United States, Illinois' Biometric Information Privacy Act (BIPA), introduced in 2008, was the first of its kind to be introduced by a state in the US. BIPA requires that entities comply with specified rules when using and storing biometric identifiers. It also gives plaintiffs a private right of action so that they can recover statutory damages when entities fail to meet such standards. Soon after BIPA, several states began to start modeling their consumer privacy laws to include biometric information usage protection in one way or another (*Is Biometric,* 2024).

Another set of prominent data privacy laws in the US include the California Consumer Privacy Act and the supplement to it, the California Privacy Rights Act. Recently, these laws have come into the spotlight as a potential model to base federal data privacy law. It outlines the rights that CA residents possess relating to data privacy (*Biometric Data*, 2024). These are largely based on an "Opt out" style, which means that users must be informed of their rights and must be given the option to opt out of data collection. There is also the Delete Act, which allows Californians to make a single request to ask data brokers to delete their personal information. This would make opting out a one-time thing, erasing the problem of having to do it multiple times, allowing users to be more mindful of what they opt into now, and having proper transparency about the usage of their data. Both CCPA and CPRA include biometric data in their regulations and group it with sensitive personal information but do little to lay out special protections. Beyond state laws, it can also be seen that government agencies and industry leaders have taken the lead and set regulatory guidelines themselves (*Biometric Data,* 2024). However, this would pose problems for various stakeholders involved as interests may not always align, leading to the consumer suffering due to a lack of advocating on their behalf.

Globally, the most relevant examples to discuss would be India and China, with India considering the Aadhar example and China to examine how they balance surveillance and privacy. In 2017, India established privacy as a fundamental right and went further in 2018 to rule it unconstitutional for private companies to utilize Aadhar's biometric data. This was achieved through a Supreme Court ruling. However, it was never passed into law. India's prime minister then added amendments to the national identification, allowing private companies to use it through a 'know-your-customer' verification process. Through this, businesses can authenticate users through a separate, government-based process without having to collect and process biometric data (*Biometric Data,* 2024). While this protects the privacy of private companies, there is a lack of enforcing transparency of data usage and storage from and for the government as well since they conduct the entire identification system. In China, biometric data is protected by two most important laws, which are the Cybersecurity Law and the Personal Information Protection Law, which are converging towards strong EU laws for privacy protection. The Cybersecurity law includes biometric data specifically as well, but it deals with the paradox of reducing the amount of data stored by companies and third parties while increasing state surveillance (*Biometric Data,* 2024). This is similar to Indian privacy laws but a lot more obvious, especially with China's emphasis on data localization, which outlines how Chinese people's data must be stored in China. Overall, there is a noticeable trend of businesses moving away from handling private and sensitive data, including biometrics, especially regarding the consequences of the mismanagement of such data. However, the differing role of the government is an interesting differentiator, largely dependent on the sovereign nation's rules.

Conclusion

As the paper has described, biometrics have grown to become a cornerstone of modern authentication systems, offering convenience and occasionally enhanced security. Its usage does raise significant questions about privacy, data integrity, and global regulatory frameworks. Examining biometric systems highlights their inherent vulnerabilities, including errors in recognition, risks of data breaches, and ethical concerns such as covert collection and function creep. These challenges require using a balanced approach to tackle them by prioritizing both technological advancements and legal frameworks to ensure user privacy and trust. Exploring global practices, from India's Aadhaar system to regulations under the GDPR and BIPA, reveals diverse strategies that reflect the socio-political context of each region. Ultimately, the integration of biometrics into everyday life must be accompanied by transparent data practices, user consent, and enforceable privacy protections. As the technology continues to evolve, fostering collaboration between policymakers, technologists, and global stakeholders will be essential in addressing the multifaceted implications of biometric systems. Through such measures, society can harness the benefits of biometrics while ensuring the dignity and privacy of individuals remain uncompromised. Moving forward, the biometrics space is set to see numerous changes, whether in adoption or regulation, with the increasing incorporation of AI into our daily lives and the tremendous dissemination of information online, some of which can also be fake. Using this time to shape how biometric authentication and its regulation will look in the future is essential to getting ahead of the curve.

Works Cited

Abdulla, Waleed H., Felix Marattukalam, and Vedrana Krivokuća Hahn. "Exploring Human Biometrics: A Focus on Security Concerns and Deep Neural Networks." APSIPA Transactions on Signal and Information Processing 12.1 (2023).

Biometrics and Privacy – Issues and Challenges. (2019). Retrieved from https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/#biometrics-in-the-public-sector

Biometric data and privacy laws (GDPR, CCPA/CPRA). (2021). Retrieved from https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data

Dewa, Z. (2017). The Relationship between Biometric Technology and Privacy: A Systematic Review. Future Technologies Conference (FTC) 2017, 105, 739–748. doi:https://saiconference.com/Downloads/FTC2017/Proceedings/105_Paper_62-The_Relationship_between_Biometric_Technology.pdf

Is biometric information protected by privacy laws? (2024). Retrieved from https://pro.bloomberglaw.com/insights/privacy/biometric-data-privacy-laws/#state

Ng, Lynnette HX, et al. "Digital Ethics for Biometric Applications in a Smart City." Digital Government: Research and Practice 4.4 (2023): 1-6.

Novriansyah, N. (2024). Types of Errors in Biometric Systems. Retrieved from https://medium.com/novai-cissp-ciso/understanding-types-of-errors-in-biometric-systems-88bcb22422ba

Pros and cons of fuzzy matching. (2024). Retrieved from https://financialcrimeacademy.org/pros-and-cons-of-fuzzy-matching/

Sadhya, Debanjan, and Tanya Sahu. "A critical survey of the security and privacy aspects of the Aadhaar framework." Computers & Security 140 (2024): 103782.

Shahriar, Arman & Yang, Tao & Shahed, Shahadat & Mazroa, Alanoud & Attiah, Afraa & Mohaisen, Linda. (2024). A Comprehensive Survey for Privacy-Preserving Biometrics: Recent Approaches, Challenges, and Future Directions. Computers, Materials & Continua. 78. 2087-2110. 10.32604/cmc.2024.047870.

Wang, Xukang, et al. "Beyond surveillance: privacy, ethics, and regulations in face recognition technology." Frontiers in big data 7 (2024): 1337465