Biometrics in Security: Ethical Implications and Privacy Risks

Yazed AlKhalaf*, Khaled AlAnbar†

*Al Yamamah University, *202211123@yu.edu.sa*

†Al Yamamah University, *202211365@yu.edu.sa*

I. Introduction

Biometrics have recently become a way to authenticate humans before giving them access to their accounts. NIST defines **Biometrics** as: "A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics." [1]. Its ease of use, and high security make developers confident when putting them in. If that is the case, then we have a few challenges we have to address, mostly on the ethical and privacy sides. Of course things aren't plain white and plain black, there is always the area in between, the grey area in which most of the discussions happen. The Ethical Implications section discusses whether it is okay to keep those records or use them for other purposes without the consent of their users. The Privacy Risks section dicusses which data is considered private and which is public and proves your identity, and if all of the data is private then how to make sure users know what they are getting into.

II. Ethical Implications

Using the biometric data collected from users for purposes other than the reason they have been collected for is unethical. But who decides what is ethical and what is unethical? The answer to this question depends on which view you use to view the case. For us as Muslims, our belief aligns well with the deontological view. That is, an action is wrong even if the outcome is good, and an action is good even if the outcome might not seem good if looked at in isolation. Our beleif is that Allah is the one who decides what is ethical and what is not because people can't decide if something is ethical or not. We are all the same, humans, and everyone would choose what suits him or her better if given the choice to decide. An example of this is whether killing someone because they killed is ethical or unethical. People of the killer might claim it is unethical to kill someone, so why kill our son? But he killed someone, so they are basically having a double-standard. Well, in Islam, if someone kills someone they are beheaded with a sword unless the people who have the right of the killed person forgive in return of "Deyya", aka money. So basically Allah is the one who decides which actions are good, "ethical", and which actions are bad, "unethical".

Keeping the context above in mind, it is unethical to keep the biometric data of users for any purpose other than what they have been collected for. Keeping it is basically stealing the data, and that is unethical. But let us say a bad actor keeps the data and doesn't follow the guidelines, what are the implications?

If the data is leaked, the user's identity can be stolen online if a website uses only biometrics data to authenticate. The biometrics data can also be sold in the black market, identity theft but with the biometrics of a real human being! This is bad and totally unethical.

Using a human being's data without their consent is like any other crime, it is a crime! Companies might be able to get away with it now, but we should stand up for our rights and protect them. People might say they have nothing to hide, and this is a well known argument when studying ethics. But still, having nothing to hide doesn't mean companies get to keep your data without your consent, this data can be used to access your accounts and steal your identity as mentioned above. And just to make things clear, it is like someone taking your car for themselves because "you don't need it". As Edward Snowden says: "Arguing that you don't care about the right to privacy because you have nothing to hide is no different from saying you don't care about free speech because you have nothing to say.". [2]

III. Privacy Risks

Identification through biometrics has become common, yet it comes with a major drawback, and that is often privacy loss. When comparing biometrics data like fingerprints, facial or voice and conventional identification data like passwords or PINs, biometric data is strong and personal (one of one), which makes it nearly impossible to replicate or even fabricate it. Even though it is hard to be fooled this are some privacy risks according to Maurice Uenuma: "Data theft, Spoofing and impersonation, Privacy concerns, and Integration challenges". [3]

Starting with data theft, "Stolen biometric data can lead to unauthorized access to enterprise systems and theft of sensitive information" [3]. When discussing unauthorized access or data theft, you're addressing the primary privacy risk, which is why i began with it initially. This attack occurs when an individual gains access to the data either during transmission or by retrieving it from its storage location, such as a computer database.

Secondly with spoofing and impersonation, "Biometric systems can be tricked using various spoofing techniques, such as fake fingerprints, facial images, or voice recordings" [3].

Thirdly with privacy concerns, “Collecting and storing biometric data raises privacy concerns, as individuals may worry about the misuse of or unauthorized access to their personal information” [3]. Due to technological advancements, it is increasingly difficult to keep personal data private. Personal information includes everything from a person’s name to their IP address to their face. For instance, on Facebook, you can typically search for a person’s name and gain access to all their personal information.

Lastly with Integration challenges, “Poorly integrated biometric systems may introduce vulnerabilities, especially when integrated with other security or IT systems” [3]. By providing the precise details required for authorization, integration aims to enhance security. However, achieving this can be challenging due to factors such as image quality, environmental conditions, and system limitations.

IV. Disadvantages of Biometrics in Security

Using biometrics in securing assets makes it easy to deal with them. But in cybersecurity, and security in general, ease of use usually comes with a tax, and that tax is less security! If a thing is secure and easy to use, then it is too good to be true, or in other words a lie or nonexistent. The first two disadvantages have been already discussed in this report:

- Ethical Implications
- Privacy Risks

But there exists more disadvantages of biometrics in security that we didn’t touch on, namely:

- Can’t be Changed
- Can be Spoofed

Biometric data can’t be changed, there is no easy way to ”reset biometric data”, you are born with it and it stays with you forever! If it gets compromised, then it is compromised forever! That is a huge risk so securing this data should be a number one priority of every company on this planet.

Another disadvantage is the fact that they can be spoofed, since at the end of the day they are saved as 0’s and 1’s on some storage medium. It can be argued that this can be said about anything, but this doesn’t change the fact that not handling this biometric data securly and safely causes catastrophic results. It can have the same effect as using the same leaked password on all your online accounts, including your bank accounts!

V. Conclusion

All in all, biometrics in security is curcial to the life of every human on this planet. Before it was only used by goverments and companies to authenticate people. But nowadays, it is in every device, like your phone, and smart home devices. People often don’t give weight to the risk they are putting themselves in by handing out their biometric data to random companies. We believe that human beings should be more aware of what they are giving out about themselves, especially when it comes to things like biometrics, since once they are out, they are out forever, and you won’t be able to get new ones either.

References

[1] National Institute of Standards and Technology (NIST). (2024) Biometrics - glossary — csrc. Definition: A measurable physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics. [Online]. Available: https://csrc.nist.gov/glossary/term/biometrics

[2] E. Snowden, “Arguing that you don’t care about the right to privacy because you have nothing to hide is no different from saying you don’t care about free speech because you have nothing to say.” https://gnupg.org/, n.d., accessed: 2024-11-23.

[3] M. Uenuma, “Navigating biometric data security risks in the digital age,” Mar 2024, accessed: 2024-11-23. [Online]. Available: https://www.darkreading.com/cyber-risk/navigating-biometric-data-security-risks-digital-age