INFO215 Social Aspects of Information Systems
College of Computing & Informatics
Drexel University

Biometrics: Finding the degree to master this Pandora's Box

Harry Zhao, Yi Pan, Carl Shen, Ziyan Di

December 7, 2021

Introduction

Today, there is a growing trend in the use of biometrics technology. The emergence of services such as fingerprint unlocking and face payment has undoubtedly made people enjoy unprecedented convenience. However, these services are often accompanied by conquests or organizations that violate people's privacy. Not only that, but the misuse of these data is also accompanied by potential threats to the safety of people's property and even their lives. This paper focuses on the pros and cons of using biometric information as an individual. We also propose the degree of personal use of biometrics based on the concerns it raises. Overall, the purpose of this paper is to answer the question of what biometric data is available and how much is appropriate to provide? In addition, we give methods to help biometrics users find this “degree."

Social-technical Impact of Biometrics

Nowadays, more and more applications use our biometric information as a password to verify our identity. Using those technologies makes it more convenient for us to get things done. Many organizations can offer us better services by using our data. Just because of its convenience and high efficiency, and all kinds of advantages, every government, enterprise, and organization is trying to use that and get a better method to use biometric data. For example, India's national ID program called Aadhaar is the largest biometric database in the world. That is a biological-information-based digital identity for every person[1], and the identity can be examined anywhere, anytime in the public area. Moreover, a brand-new type of identity card, called MyKad, was introduced by the National Registration Department of Malaysia on September 5, 2001, with Malaysia becoming the first country in the world to use an identification card that incorporates both photo identification and fingerprint biometric data on an in-built computer chip embedded in a piece of plastic.[2]

With the development of biometric technology, people's fingerprints, faces, DNA, and other personal biometric information can be stored and become more convenient to be used, like many platforms make these data passwords for users to log in. Even the payment can be completed by just scanning people's faces. Furthermore, that payment path has been widely used in retail, medical care, etc.

With the maturity of artificial intelligence applications, more and more biometric technologies are widely used in life and work, and people are paying more and more attention to their bio-information security issues. As a result, many scholars from universities or research institutes started to research and expressed their opinions on the topics related to biometrics. Professor Liaoyuan Zeng from the University of Electronic Science and Technology said: "The convenience and security cannot be kept simultaneously" [3]. He thought that regardless of technology, face recognition can be considered one of the methods to examine our identity, but it cannot be the only critical method. When it comes to a scenario requiring a high level of security, it cannot be used as a single way of identification. Yi Tong, the Beijing Science Research Center deputy director, said that personal private information is not the same as the passwords we often use because if we leak the password by mistake, we can just reset it. However, as for personal biometric information, it will be leaked forever. Security is placed in great uncertainty, which in turn causes a series of risks [3].

With concerns about the widespread use of biometrics, several countries have introduced regulations to guide the industry's development. For example, the "Personal Information Protection Law of the People's Republic of China" came into effect on November 1. This new law stipulates that the prohibition of excessive collection of personal information, abuse of face recognition technology, etc. [4]

Discussion about the “degree"

Pros and cons of biometrics

To define a clear boundary for the degree to which biometric information can be used, we will first explore the pros and cons of biometrics.

Over the years, biometric has been proved to help consumers. People have chosen to use biometric input devices. The technology serves the purpose of attendance, authentication monitoring, and even the entry and exit method. Second, authentication is pretty fast and accurate. Previously people used passwords and codes. This technique, however, is easy to hack and can pass access between individuals with or without permission [5].

The use of biometrics also plays a crucial role in crime tracing. People will be held accountable for their actions because biometric evidence can be used to prove guilt.

Biometrics is also highly efficient. Convenience is the keyword for efficiency. Businesses will save more money by using biometric as a more secure system, curbing losses from fraud or unauthorized entries. Then more budget to spend on other production [5].

In addition, in 2021, Mitek, a global company focused on providing integrated software, gave us a summary of biometrics' four main benefits: High security and assurance, User experience are convenient and fast, Non-transferable, and Near spoof-proof [6].

When it comes to the downside of biometrics, the cases are endless. In July 2019, the United Nations World Food Program and Houthi Rebels were involved in a significant dispute over the use of biometrics to ensure resources are provided to the hundreds of thousands of civilians in Yemen whose lives are threatened. In times of crisis, many aid programs use biometrics to prevent fraud and ensure that appropriate resources are provided to those in need, but the use of biometrics as a form of humanitarian surveillance can create conflict [7]. Disputes over the use of biometrics between aid programs and party officials stalls the distribution of resources to people that need help the most. And these conflicts caused by deep-rooted political problems makes biometrics technology may not be suited for chaotic times of crisis.

In 2004, Italian philosopher Giorgio Agamben refused to enter the United States in protest at the United States Visitor and Immigrant Status Indicator (US-VISIT) program's requirement for visitors to be fingerprinted and photographed. Agamben argued that gathering biometric data is a form of bio-political tattooing akin to the tattooing of Jews during the Holocaust. This is considered a severe violation of human rights by biometrics data [8].

If the above cases of humanitarian or privacy violations are not enough to raise concerns about biometrics, the following cases are a real threat to owners of secured items. In 2005, Malaysian car thieves cut off the finger of a Mercedes-Benz S-Class owner when attempting to steal the car [9]. When thieves cannot get access to secure properties, there is a chance that the thieves will stalk and assault the property owner to gain access. This case illustrates how biometrics services are even potentially threatening to human life.

Based on the above examples, we know that providing biometrics data is necessary and dangerous. For individuals, we give a method or, more generally, a principle to biometrics users to measure and test the reasonableness of using biometrics data.

The principle of non-dependence

We propose the principle of non-dependency to help people get rid of the overuse of biometrics data, which is defined as using biometrics non-dependently, i.e., only enjoying the convenience of biometrics under the condition that the disappearance of biometrics would not prevent things from accomplishment, goals from being achieved, or physical and mental health from being affected.

For example, for people using a biometric security door, can they solve the problem of whether they can get in when biometrics fail to work or when the power goes out? If the answer to such a question is no, we believe that they are violating the principle of non-dependence in the use of biometrics.

When it comes to physical and mental health, we are more concerned with mental health. Because we have a good grasp of how the overuse of biometrics can often lead to negative personal emotions, for example, when the fingerprint information required to log in to an online banking app fails, users will be asked to use a password. Will they get annoyed at this point because of forgetting the password? Or feel emotionally drained by typing out multiple passwords on such a tiny phone screen? If you cannot face these dilemmas head-on, we think you are violating the principle of non-dependence in the use of biometrics.

Consequences of overusing biometrics

Next, we will discuss the consequences of the misuse of biometrics. In addition to privacy violations, this article summarizes some other serious consequences that can occur.

Biometrics can identify, track, single out, profile, and follow people, thereby undermining human rights and civil liberties. They violate privacy and data protection rights, exacerbate inequality and discrimination, and have the potential to suppress freedom of expression and assembly - paving the way for the criminalization of protesters and protestors. [10] People would live under oppressive conditions, feeling fearful and cautious daily in countries or regions where biometrics are rife.

For commercial companies that operate for profit, the data they collect through biometrics does not preclude the risk of trafficking to other organizations. It is a concern for these organizations to use our biometrics data for whatever purpose, especially physical data. Let's imagine an extreme but possible scenario. A person with Meniere's disease [11] has his biometrics data sold through the dark web to his enemies, who use his biometrics data to infer the person's disease, whose symptom is afraid of loud noises, to create noise around the person to aggravate his disease. Clearly, we have reason to believe that the consequences of biometrics data being used for nefarious purposes can be far more serious than that of ordinary data.

Moreover, we imagined a dramatic but thought-provoking future scenario where biometrics data is overused exaggeratedly in our game developed in this project. The game is about a technologically advanced future where biometric data and services are the most common in life, and they are often traded as commodities. The protagonist must choose a series of complex challenges related to biometric data, and the consequences that await him will correspond to his choice.

Conclusion and Recommendations

This article has discussed the pros and cons of biometrics based on plenty of material and how we are supposed to use biometrics wisely as ordinary people. Similarly, the discussion of biometrics can be extended to many other technologies because almost all technologies are double-edged swords. To use technology better rather than let it use us, we should understand how to apply the using “degree” to all technology used in our lives.

The consequences of relying too heavily on biometrics are undesirable. If you violate the non-dependency principle, we recommend that you make improvements and adjustments to your use of biometrics to reduce your dependency on it. We offer some suggestions for your consideration：

- Deliberately reduce the use of biometrics apps. This is a training exercise to free yourself from over-reliance on biometrics, and it should be effective in helping you at least recognize which biometrics services are unnecessary.
- Do not provide data other than the commonly used biometrics data like fingerprinting, such as metabolic data and other physical characteristics data. Since this data has not been tested and fed back by many users, we have two concerns: first, is this data easy to falsify, which will affect personal safety? Second, are these data the core characteristics of human beings? Will people's fundamental rights be unacceptably violated because of their extreme importance and representativeness?

- Always think of plan B while using biometrics. Biometrics is not yet fully mature as a solution to some problems. As discussed above, the failure or infringement of biometrics is likely to result in some goals not being met. Therefore, as a biometrics user, anticipating and preparing for violations can prevent you from being compromised to some extent.

From this project, we also learned many valuable lessons. First of all, it is essential to look at things for what they bring and what they take away. There are many things like biometrics technology that is double-edged swords. A more proper way to evaluate service or technology is to analyze it from multiple perspectives. Second, besides developing technologies, we should also find the appropriate “degree“ to use them. Millions of cases have shown us that excessive abuse will lead to disastrous consequences. The game we developed in this project demonstrates one possible result from the misuse of biological information in the future, which is horrific and desperate.

References

[1] *P.* (2017, August 30). *Aadhaar data kept, processed only on own secure servers: UIDAI*. The Economic Times. https://economictimes.indiatimes.com/news/politics-and-nation/aadhaar-data-kept-processed-only-on-own-secure-servers-uidai/articleshow/60295134.cms

[2] *Wehr, J.* (2004, March 1). *Malaysia's national 'MyKad' ID card succeeding through service to citizens*. SecureIDNews. https://www.secureidnews.com/news-item/malaysias-national-mykad-id-card-succeeding-through-service-to-citizens/

[3] *Procuratorate Daily.* (2019, April 17).”"Human faces and fingerprints are running naked" Personal biometric information is expected to be protected by legislation." Xinhua News. http://www.xinhuanet.com/politics/2019-04/17/c_1124376731.htm

[4] *Deutsche Welle*. (2021, November 1). 中国实施《个人信息保护法》 数据隐私"安全锁"？. DW.COM. https://www.dw.com/zh/%E4%B8%AD%E5%9B%BD%E5%AE%9E%E6%96%BD%E4%B8%AA%E4%BA%BA%E4%BF%A1%E6%81%AF%E4%BF%9D%E6%8A%A4%E6%B3%95-%E6%95%B0%E6%8D%AE%E9%9A%90%E7%A7%81%E5%AE%89%E5%85%A8%E9%94%81/a-59683984

[5] *Aichouni, A. B., Kamaruddin, A. I., & Burhan, M. F. (2020, March). Review Paper On Ethics Regarding Biometric Technology*

[6] *Advantages and disadvantages of biometrics | Mitek*. (2021, March 15). Mitek. https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics

[7] *Latonero, Mark (July 12 2019). "Opinion | Stop Surveillance Humanitarianism". The New York Times*

[8] *Agamben, G. (2008). "No to bio-political tattooing". Communication and Critical/Cultural Studies, 5(2), 201–202. Reproduced from Le Monde (January 10 2004).*

[9] *Kent, Jonathan (March 31 2005). "Malaysia car thieves steal finger". BBC Online. Kuala Lumpur. Archived from the original on November 20 2010. Retrieved December 11 2010*

[10] *Statewatch | "The potential for abuse is too great": Global call to ban biometric surveillance in public spaces*. (2021, June 7). Statewatch. https://www.statewatch.org/news/2021/june/the-potential-for-abuse-is-too-great-global-call-to-ban-biometric-surveillance-in-public-spaces/

[11] *Meniere's disease - Symptoms and causes*. (2020, December 2). Mayo Clinic. https://www.mayoclinic.org/diseases-conditions/menieres-disease/symptoms-causes/syc-20374910