Global Scientific JOURNALS

GSJ: Volume 8, Issue 9, September 2020, Online: ISSN 2320-9186
www.globalscientificjournal.com

ETHICS IN BIOMETRICS AUTHENTICATION

Adedeji Adegbenle*[1] Uchenna Nzenwata[1] Olugbohungbe Rotimi [1] Adesegun Oreoluwa[1] Adegboye James[2]

1. Department of Computing and Engineering Sciences, Babcock University, Ogun State, Ilishan-Remo 121103, Nigeria
2. Computer Science Department, Federal Polytechnic Ilaro, Ogun State, Nigeria.

* E-mail of the corresponding author: nzenwatauchennajeremiah@gmail.com

Abstract

The September 11, 2001 terrorist attack birth the idea of biometric measures, when the traditional methods of identification were concluded to be prone to leakage of personal information, identity theft, fraud, etc., and there are great security risks in identity recognition. Biometrics is a device used to identify and reliably confirm a person's individuality using the physiological or behavioral characteristics. This term paper examined some of the gray areas surrounding biometric technology and informs the public about the growing number of ethical concerns associated with the use. The idea came up as a result of the rising popularity of biometric systems and their application in mainstream society which led to many ethical concerns, where biometric sensors and scanners are being implemented with no consideration for unintended negative consequences. A systematic review of related literatures was adopted and used to examine the relevant ethical issues. The identified ethical issues paved way for the recommendation of 7 points guidelines, which when adopted will alleviate the fear associated with biometric technology.

Key words: Biometrics, Technology, Social Exclusivity, Ethics, Legality, Theft.

1.0 Introduction

(Sivakumar, 2019) defined Biometrics as a device used to identify and reliably confirm a person's individuality using the physiological or behavioral characteristics.

In our daily living, we often encounter the need to verify identity, or confirm who someone is, which requires identification. The traditional identification methods mainly include two types: one is to identify the identity of the individual through physical objects, such as ID card, smart card, passport, and key, etc.; the second is to identify the relevant password by agreement, such as verification code, password, account number and Password, etc. However,

the traditional methods of identification are prone to being stolen, lost, forgotten, etc., which is prone to leakage of personal information, identity theft, fraud, etc., and there are great security risks in identity recognition. Since the "September 11 terrorist attacks", traditional identification methods have become increasingly unable to meet people's requirements for security level growth, and people urgently need more secure and convenient identification methods. Intelligent biometrics is rapidly evolving in this social context (Cooper & Yon, 2019).

1.1 Background to the study

Biometrics defined broadly is the scientific discipline of observing and measuring relevant attributes of living individuals or populations to identify active properties or unique characteristics. Biometrics looks for patterns of change by measuring attributes over time or look for consistency by measuring attributes of identity or unique differentiation. When looking for patterns of change, biometrics can be considered a tool for research, diagnosis, or medical monitoring. When looking for consistency, biometrics becomes a useful vehicle for security (Gatali, Lee, Park, & Kang, 2016).

The first scientific paper discussing biometric technology was published by (Trauring, 1963). The report examined how computer algorithms could identify someone based on unique ridges and valleys on their fingertips. Since then, biometric technology has rapidly risen in popularity, giving way to devices that can use fingertips, irises, and even a subject's walking pace to identify them (Sareen, 2014). However, it has become a thing of concern why our local and national governments have been unable to keep up with the usage growth in this technology; and few regulations exist on biometric technology. Possibly the issues could be the poor enforcement of the legal guidelines on the use of Biometrics. Also, should there be existing guidelines to demystify the fear in the usage of biometric technology, how can the general populace be brought to knowledge of how safe and quick this technology is?

1.2 Statement of Problem

The rising popularity of biometric systems and their application in mainstream society has led to many ethical concerns that need to be addressed by governments or individual companies. Also, amidst the state of confusion in the use of biometrics, biometric sensors and scanners are being implemented with no consideration for unintended negative consequences. All these are problems that really need to be addressed.

1.3 Objective of this term paper

This term paper is aimed to examine some of the gray areas surrounding biometric technology and address its usage with the objective to informing the public about the growing number of ethical concerns associated with the use.

1.4 Methodology

This term paper used the systematic review of related literatures to examine some of the gray areas surrounding the privacy and legality of biometric technology. The identified ethical concerns were subjected to the views of privacy and social exclusivity effects.

1.5 Significance of the Study

This term paper report will end by summarizing the main points and providing recommendations the governmental utilization, social use, and private companies consumptions.

2.0 Literature Review

In the words of Wikipedia, Ethics is also known as moral philosophy, and it's defined as a branch of philosophy that "involves systematizing, defending, and recommending concepts of right and wrong behavior. Hooking up this definition with technology presents an implementation that would have great impact on both human and the society at large. It is very much obvious that many events in likes of organizations fairly subscribe to the biometrics as no ethical measures are strictly adhered. Legislating legal guidelines on the use and application of biometrics devices is sure to demystify the fear of biodata compromise.

The above statement is in sync with (Karkazis & Fishman, 2017). In their work, they valued biometric as a new technology that could be ethically assessed. Using the advancement of these technologies posed challenges to existing ethical frameworks, putting collective values and public interests above individual rights. They compared biometric databases with medical research oriented genetic databases to show that public interest may be differently constructed: while genetic databases projects create a discourse of hope, biometric databases are surrounded by a discourse of threat. Also, the Ethical issues surrounding the actual and proposed use of biometric identifiers within the EU were identified using biometric identifiers which is in use presently in private applications across the world (Sprokkereef & De Hert, 2007). (Superiore, 2007) highlighted the most relevant ethical and social implications by giving a brief overview of the contents of the main institutional documents produced both on an international and domestic level in the various countries. His report also brings to the fore the main challenges which society shall have to deal with, in the near future and on a long-term basis, as a consequence of the extremely rapid diffusion of those technologies which use biometric data request.

(Lunn, 2016) referred to Gifford lectures published in Ethics in the Age of Technology (1993), Ian Barbour has shown that appraisals of modern technology diverge widely. With proper description of Ian Barbour's work, Lunn summarized it into two major groups views of technology under three headings: Technology as Liberator, Technology as Threat, and Technology as Instrument of Power.

When we look at the ethical discussion surrounding the application of biometric technology today, the situation presented above is similar. One group of people hypothesizes biometrics as Liberator, believing: in the power of technology to bring convenience (avoiding queues, faster answers, an immediate access to information), efficiency (cutting costs, producing efficiency gains for administration). This group may also welcome more powerful surveillance (to monitor migration, combat identity theft and fraud). The other group sees biometrics as a threat: they believe that surveil- lance technology is inhumane, untrustworthy, and destructive of liberty. A third group sees biometrics as "a sword with multiple edges", the use of which depends on the carrier and aims followed.

It is very clear, that the views of technology vary according to the differing needs of people and institutions. However, different views of technology also reflect our different value judgements. Values are rooted in hierarchies of beliefs, cultures and forms of life. Even if we share primary values which are related to our basic physiological and psychological needs, our secondary values may still differ, depending on our historical, religious, cultural experience, on our understanding of the good life and ways of living. And even if we all agree that security, privacy, autonomy, and liberty are important, we rank these values differently. The value conflicts (e.g. privacy versus

security, autonomy versus solidarity) make it difficult to take a broad and consistent position in favour of, or against, expanding or restricting biometric technologies.

I tend to tow in the words of Garry T. Marx. He said, "Diverse settings e.g., national security, domestic law enforcement, maintenance of public order, health and welfare, commerce, banking, insurance, public and private spaces and roles –do not allow for the rigid application of the same policies. The different roles of employer-employee, merchant-consumer, landlord-tenant, police-suspect, and health provider-patient involve legitimate conflicts of interests. Any social practice is likely to involve conflict of values." (Marx, 2007).

The highlighted discussed thoughts as reviewed above, gave in to the reason of having unified guidelines for the use of biometric technology.

With this quick review on what is being evoked in ethical stance of biometric technology, we shall continue with other sections of this term paper so as to have some of these ethical implications discussed.

3.0 Ethics and Biometrics

This section discusses questions of great concern, and if well answered, they provide a soft landing for the assessment of ethics in biometric technology. As with any other technology, we can ask two questions about biometrics: first, what are its ethical implications? Secondly, what kind of challenges does this technology present to ethics?

Biometrics are now increasingly used for user identification and/or authentication in information systems, in border controls, in health systems. Rapid decreases in price and better performance have made biometric technology practical for consumer applications and for governmental purposes. Yet any innovative technology program needs a continuous investigation of its possible ethical implications. The relevance of ethical implications of bio- metrics is self-evident: it is not only a consequence of the scale of the phenomenon and of the current historical period where security is the centre of attention in many countries. Its relevance is mainly a consequence of the deeply-rooted ethical significance of some issues raised by biometrics. Many of the problems are related to individual rights such as the protection of personal data, confidentiality, personal liberty, the relationship between individual and collective rights. Biometrics is one of the most significant examples of how complex it is to match individual and collective needs. It inevitably leads to questions related to personal, social and collective identity which according to some authors are essential study domains for contemporary sociology (Yanushkevich, Stoica, Shmerko, & Popel, 2018).

3.1 Ethical Issues in Biometrics

Some problems in the application of biometrics have been studied for a long time from the ethical point of view, there is no holistic and detailed analysis of the ethical issues of biometrics in the world. According to (Cooper & Yon, 2019), there were only a few reports on ethical issues in biometrics, before 2007, such as the 2001 RAND Corporation report "Identification and Addressing Sociocultural Concerns in Army Biometric Applications", where social concerns were identified and analyzed; 2003 Working Paper of the Data Protection Working Party

of the European Commission (Biometrics); 2004 Biological Vision Report "From User and System Credits" BIOVISION - Roadmap to Successful Deployments from the User and System Integrator Perspective; 2004 Economic Cooperation and Development Organization Report "Organisation for Biotechnology" Economic Co-operation and Development (OECD) Report: Biometric-based Technologies; 2005 report of the European Commission Joint Research Centre, a forward-looking technology research institute Biometrics at the Frontiers: Assessing the Impact on Society; 2006 National Science and Technology Commission's National Biometrics Challenge Report (and other Reports) of the National Science And Technology Council of the United States. It was understood that these reports were directed to underscore following ethical considerations in regards to biometric technology;

1. **Privacy in Data Storage**

   Data storage proves difficult to navigate for any type of information, but this is especially true for biometrics. Because the information collected are biological features and behavior that are unique to each individual, it is essential that the data is secured. Regardless of the measures taken to protect and store users' information, the data can always be breached. Since biometrics is a rapidly growing method of authentication, the way in which the data is stored is crucial to users' privacy.

   Hackers and scammers evolve parallel to technology, and as a consequence, roughly 5.6 million people's fingerprints were jeopardized when the Office of Personnel Management was hacked in 2015 (Ayereby, 2018). Although fingerprinting is more secure than PINs, researchers from a mobile security firm "were able to break into Apple's Touch ID system with a small piece of Play Doh" (Ayereby, 2018). These experiments illustrate that with a simple hack, large amounts of data can be compromised and used without user consent. This situation is very dangerous because with traditional authentication methods such as a PINs, the code can be changed if an unwanted login is detected. However, information such as fingerprints, faces, and voices, cannot be changed. Extra verification can increase the difficulty in using the stolen biometric data, but the core of the issue is in secure storage of the data. Companies have an ethical obligation to their users to protect their data, but many companies are setting this aside in favor of technological innovation.

2. **Third Party Storage**

   The storage of data in large databases makes biodata more susceptible to being accessed, rightfully or not, by third parties who wish to use large amounts of personal data in order to influence future business decisions. For example, Aadhaar in India is the largest biometric database (Rao & Nair, 2019). Originally, the database was voluntary for citizens to participate in. However, the database became standard in order to use basic institutions, such as receiving school meals or opening bank accounts. Therefore, participation in the database became mandatory to function in society, and citizens had no choice but to provide the biometric data. Numerous non-governmental organizations were able to access the database for various purposes, all without user consent. The citizens were obliged to add their data to the database, but had no voice in who received the data. The database did provide for an easy and consistent method of

authentication and identification, but because the database was so widely used, citizens' privacy was compromised.

Elaborating on the unauthorized use of data, a user's biometric data can be used and manipulated for private motives. Targeted advertising is a common example of this. Because characteristics such as age and gender can be automatically detected by face or voice recognition software, products and services can be advertised to select individuals. Algorithmic content can provide individuals with skewed information about the world around them, increasing various forms of biases. Private organizations having the ability to use biometric data to manipulate individuals is ethically contentious (Sun, 2018).

3. **Legality & Regulation**

Biometric technology is rapidly growing and the government is struggling to keep up, turning a blind eye to ethical considerations. There is a lack of regulation regarding the privacy and use of biometric data. To begin with, biometric identification methods are legal in 48 states when in public, and is legal in all states for law enforcement purposes (Rao & Nair, 2019). These minimal regulations show how biometric data can be recorded, but there is a lack of regulation in how that data is stored and protected. Additionally, there is a lack of regulation to deal with situations when biometric data is breached.

It is difficult to pinpoint what falls under the umbrella of biometrics and whether all types of biometric data should be treated the same. An analysis of the European Union (EU) regulations found that it is important to have a clear distinction between various types of biometric data (Tikkinen-Piri, Rohunen, & Markkula, 2018). From the same analysis, the EU regulations fail to provide clear rules and protection for the fundamental rights of privacy when it comes to biometric data. Legally, it is generally agreed upon that different types of biodata should be treated differently than others, but governments have been unable to dictate laws that respect those distinctions.

Since the government has poorly regulated the use of biometrics, the technology industry has had the freedom to introduce technology to the masses without concerns for the user. For example, technology companies provide hidden sentences in the Terms and Conditions explaining the contentious use and storage of users' biometric data (Sun, 2018). Because most users fail to read the terms and conditions, the user provides consent for the use of their data without being aware of how it is being used and where their data is being sent. Without clear regulation, companies and organizations are not transparent with the storage and use of biometric data. This method of receiving consent is ethically contentious because biodata can be used to access bank accounts, emails, and other sensitive materials.

4. Accessibility and Discrimination: Non-inclusive Biometrics

Ethical concerns surrounding biometric systems examine more than user privacy and data storage, and include discussions about the inclusivity of the technologies as they grow. For example, even the initial

step of the enrollment of biometric data can prove difficult for certain groups of people, and a failure to enroll (FTE) problem may arise. FTE rates for fingerprints are typically higher for elderly users who sometimes have poor circulation and also for some construction workers and artisans, whose fingerprint ridges may be worn down due to heavy work with the hands (Brown, 2010). Non-inclusive technology and designs lead to inconvenience and frustration for minority groups which will amplify as biometrics become more prevalent.

5. Disability

Different biometric authentication systems can present multiple problems to persons with different disabilities. A study involving both a control group and a disabled group found that speaker recognition was difficult for many people with cognitive learning disabilities and for people with hand and arm disabilities because they had to press a button while speaking (Blanco-Gonzalo, Lunerti, Sanchez-Reillo, & Guest, 2018).

Many groups, including people with a physical or learning disability, people suffering from mental illness, the elderly, and people of minority race or minority religion, may become increasingly socially excluded as biometrics grows and expands (Blanco-Gonzalo, et al., 2018). They can fall behind due to various reasons aversions to new technology, distrust of technology, or difficulties enrolling and verifying with biometric data. However, if biometric authentication becomes a requirement to receive government assistance, social services, and benefits, many of these groups will become even further disadvantaged. As biometric technology becomes more popular, this will lead to an unethical lack of equity because certain populations will be excluded from receiving benefits and services that are available to others.

6. **When Biometrics Fail**

Biometric authentication can be viewed as a probability of how likely the user is who they claim to be (Hamidi, 2019). This authentication can fail in one of two ways; it can produce a false positive (known as a false match rate) or a false negative (known as a false non-match rate). Each of these failures carries its own set of issues. If a false positive occurs, someone who should not have access to the restricted task or information will wrongfully gain access to it, which could lead to impersonation or a catastrophic breach of data. On the other hand, false negatives can prevent someone who should rightfully have access to a system or service from accessing it (Hamidi, 2019). Occurences of false negatives and false positives have an inverse relationship, and the designer of each biometric system decides which direction and to what direction the relationship leans. Most designers are interested in having less false positives, which results in more occurrences of false negatives that can negatively impact the lives of regular users. Because of non-

inclusive design, certain minority populations are disproportionately affected by false non-match rates and thus suffer more from the prevalence of false negative failures (Hamidi, 2019).

4.0 Outcomes and Discussions

It now appears that the application of biometric technology has brought about a series of ethical issues, especially ethical issues related to privacy protection, physical information, autonomy, and social exclusion. As with other technologies, the ethical issues associated with the application of biometrics are determined by the way it is used, i.e., how the technology is used and how the resulting data/information is handled. When we consider the ethical issues brought about by the application of biometric technology, we should be linked to the innovation and development of other related technologies, such as monitoring technology, big data technology, network information communication technology, database security and other technologies.

From the above ethical issues as discussed in this term paper, one can conclude that privacy protection is at the core of ethical issues related to biometrics. In the context of biometrics, privacy is more about information privacy and is generally equivalent to biometric information. Unlike general personal information, biometric information has new features such as permanence, invasive concealment, and reveals ability of medical information. Therefore, when collecting, storing, and using/sharing biometric information, it should be treated as sensitive personal information. If not handled properly, there may be many risks such as identity theft and fraudulent biometric systems, and since biometric information is not resettable, these effects will be irreversible. This is what it means to protect biometric information.

Body information is an ethical issue unique to the application of biometrics. If data mining is used properly, it can be applied to the diagnosis and prevention of diseases based on the relationship between certain types of biometrics and certain diseases. However, due to the different values and orientations of individuals, organizations or organizations that use biometrics, body Information may also lead to risks such as discrimination and stigma, uneasiness and fear, classification and social exclusion. Social exclusion in the context of biometrics refers to the social situation and ethical dilemma that some special groups cannot enjoy because they cannot be recognized by any biometric system. The issue of social exclusion is actually a matter of justice, and personal interests and public interests should be properly weighed. It is reasonable to take certain measures to include as many individuals as possible, and to provide other alternative rights or services for those who cannot be included, and try to avoid social exclusion to harm these vulnerable groups and ensure that they do not in- cur disproportionate damage.

5.0 Conclusion

To resolve the previously discussed ethical concerns, biometric technology needs to be improved. Biometrics is a growing field, and biometric systems are increasingly being used in a variety of settings. Biometric technology has potential to be a more efficient and secure method to confirm identity and authenticate users by removing the problems associated with forgetting a password and by eliminating common security breaches that occur with stolen PINs and passwords. However, the ethical complications of biometric technology must also be considered. Biometrics are unique to each individual and thus are closely tied to an individual's identity, so

privacy becomes a concern. Once biometric data is enrolled and stored, third parties often gain access to the information without user knowledge, and consistent standards have not yet been developed to regulate this data.

I hereby recommend the following;

1. Although the possibility of a data breach always exists, measures should be taken to increase the security and privacy of biometric data.
2. The method by which the data is stored and protected should be thoroughly examined.
3. Companies and Organizations should be cautious with granting access to the data, and importantly, should be transparent with the use of the data.
4. Governments have to hold companies and organizations accountable by providing clear and thorough rules of the collection, storage, and use of biometric data.
5. There should also be a clear and thorough system to penalize companies and organizations that violate the regulations.
6. Matching and identification algorithms must be improved to account for a diverse array of ethnic features.
7. A biometric system should not be implemented anywhere unless it has a roughly even failure to enroll (FTE) or false negative rates among different races and groups of people.

References

[1] Sivakumar, S. (2019). Biometric Authentication Techniques and Its Future. In *Biometric Authentication in Online Learning Environments* (pp. 122-149). IGI Global.

[2] Cooper, I., & Yon, J. (2019). Ethical Issues in Biometrics. *Science Insights*, *30*(2), 63–69. https://doi.org/10.15354/si.19.re095

[3] Gatali, I. F., Lee, K. Y., Park, S. U., & Kang, J. (2016, August). A qualitative study on adoption of biometrics technologies: Canadian banking industry. In *Proceedings of the 18th annual international conference on electronic commerce: e-Commerce in smart connected world* (pp. 1-8).

[4] Sareen. P, "Biometrics — Introduction, Characteristics, Basic Technique, Its Types and Various Performance Measures," *International Journal of Emerging Research in Management & Technology*, vol. 3, no. 4, p. 109–119, Apr 2014. Available: https://www.ermt.net/docs/papers/Volume_3/4_April2014/V3N4-120.pdf. [Accessed: May 20, 2020]

[5] https://en.wikipedia.org/wiki/Ethics#Defining_ethics

[6] Karkazis, K., & Fishman, J. R. (2017). Tracking US professional athletes: The ethics of biometric technologies. *The American Journal of Bioethics*, *17*(1), 45-60.

[7] Sprokkereef, A., & De Hert, P. (2007). Ethical practice in the use of biometric indentifiers within the EU. *Law, Science and Policy*, *3*(2), 177–201.

[8] Superiore, I. (2007). *The section "Ethical and social implications of biometric identification technology" of this issue of*. 3–4.

[9] Lunn, D. (2016). *The gift of creativity: an approach to a theology of technology* (Doctoral dissertation, Thesis

submitted to the Department of Theology and Religion, Durham University. Available at Durham e-theses online: http://etheses. dur. ac. uk/11083/. Accessed May 20, 2020).

[10] Marx, G.T.: Hey Buddy Can You Spare a DNA? New Surveillance Technology and the Growth of Mandatory Volunteerism in Collecting Personal Information. Annali dell'Instituto Superiore di Sanità 1(43), 12–19 (2007)

[11] Yanushkevich, S. N., Stoica, A., Shmerko, V. P., & Popel, D. V. (2018). *Biometric inverse problems*. CRC Press.

[12] Ayereby, M. P. M. (2018). Overcoming Data Breaches and Human Factors in Minimizing Threats to Cyber-Security Ecosystems.

[13] Rao, U., & Nair, V. (2019). Aadhaar: governing with biometrics.

[14] Sun. Y, "Demographic Analysis From Biometric Data: Achievements, Challenges, and New Frontiers," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 40, no. 2, p. 332–351, Feb 2018. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7855777. [Accessed: May 20, 2020].

[15] Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. *Computer Law & Security Review*, *34*(1), 134-153.

[16] Browne, "Digital Epidermalization: Race, Identity and Biometrics," *Critical Sociology*, vol. 36, no. 1, p. 131–150, Feb 2010. [Online]. Available: http://journals.sagepub.com/doi/pdf/10.1177/0896920509347144. [Accessed: May 20, 2020].

[17] Blanco-Gonzalo, R., Lunerti, C., Sanchez-Reillo, R., & Guest, R. M. (2018). Biometrics: Accessibility challenge or opportunity?. *PloS one*, *13*(3).

[18] Hamidi, H. (2019). An approach to develop the smart health using Internet of Things and authentication based on biometric technology. *Future generation computer systems*, *91*, 434-449.