Proceedings of the International Conference on Social Psychology and Humanity Studies
DOI: 10.54254/2753-7048/10/20230321

Bioinformation Control Regimes and Protections: Based on the Biometric Information Privacy Act in Illinois

Hequn Ren[1, a, *]

[1]*Department of Law, Southwest University of Political Science and Law, Baosheng Avenue, Chongqing, China*
a. 2021022065@stu.swupl.edu.cn
**corresponding author*

Abstract: With the development of the times, the advanced technologies have brought social life with great convenience. The biometrics has integrated into various aspects of daily activities. To some extent it may increase the efficiency of life and provide more methods to protect the security in essential fields. Nevertheless, as the recent creations, many problems have been exposed during the social practice. All over the world, the giant companies including Facebook, Twitter and Marriott have been reported in unauthorized using or selling the bioinformation of users. The absence of supervision and the imperfect legislation led to large number of illegal behaviors. Biological information is unique and unchangeable with special risks. Once it is leaked, it will be exposed for whole life. Its sensitivity and utilization value are much higher than general information, but such actions will invade customers' biological privacy. An increasing number of citizens have realized the fact and become anxiety for the biometric technique. However, the generally consensus in the academic is that the advantages may outweigh its drawbacks. Therefore, this essay will analyze the infringements which may be caused in different stages when using bioinformation and the effective solutions towards them. In order to have a more comprehensive and logical content, the methods used in creating this thesis including the case study, regulatory research and the comparative research. It could be discovered that even though the bioinformation control regimes and protections lacks supervision and relevant regulatory which has led to practical issues frequently, such technology could surely benefit humans with correct measures in the long term.

Keywords: bioinformation, privacy protection, biometric technology, systematic information legislation

1. Introduction

With the rapid development of technology, the high-tech devices have changed the way of citizens' life and brought convenience to many aspects including trades, medical treatment and transportation. Nevertheless, exposures of the illegal usage of the bioinformation emerge in endlessly, which has caused massive social panic [1]. In 2017, the world-famous enterprise Facebook was accused by collecting biometric data illegally using the facial recognition software. It happens that there is a similar case in recent years in China. In the case Hangzhou Wild Animal World Co. LTD v Bing Guo, the zoo, which is the defendant in this case, collected and used the information of tourists'

DOI: 10.54254/2753-7048/10/20230321

fingerprints and facial recognition without their permission. Hangzhou Intermediate People's Court in Zhejiang has made the judgment demanding the zoo to delete visitors' biometric information to protect such the sensitive information.

Such cases occurred with an increasing trend globally because of the more and more advanced technology. The governments have also realized the severity and taken actions to handle with such crimes. The mainland of China established the Act on the Protection of Personal Information in 2021 in order to clarify the principle in employing users' bioinformation. The European Union Committee also implement the Act on General Data Protection Regulation (GDPR) since the May of 2018. In essence, it could be the compulsive requirements for all market entities in the EU to unify the standard of data protection. Actually, Illinois in America is the earliest region to enact a biometric data privacy law all around the world. In 2008, the Illinois legislature unanimously passed the Biometric Information Privacy Act. According to a survey, the act has been used in the US District Court for at least 90 times in 2022. It is also the accordance to initiate legal proceedings in the case related to Facebook mentioned above. It could be discovered that the major countries have legislated closely to the practice of biometric information privacy [2]. Nevertheless, relevant details should be further improved and the new phenomenons are emerging continuously. In this occasion, the essay will illustrate the existing global dilemmas on the protection of biometric information privacy in reality, giving out some fundamental solutions towards them.

2. Overview of Traditional Types of Bioinformation

The bioinformation could be defined as the information that reflects the state, feature and the mode of movement of creatures. This word has been invented since the origin of the biological study. But it only came to the attention of the larger public accompanied with the development of high technologies. In this circumstance, the bioinformation derives another technique called the biometric. According to the definition of the US government, a biometric is a measurable biological, including the contents of anatomical and physiological, and behavioral characteristics that can be used for automated recognition. These biological features could be directly applied to the usage in high-tech areas with various functions in different aspects. The biometrics are unique physical characteristics from person to person, which could distinguish between individuals [3]. Undoubtedly, it addresses a longstanding concern to prove one's identity. The similar method could be dated back to the second century B.C., when the Chinese emperor Qing has already authenticated specific seals with the fingerprints. The biometric information has been popularized since the late 19th century and generally combines with other security technologies for instance the smart I.D. cards and chips.

The practice of bioinformation mainly have three forms.

2.1. Fingerprint

The bioinformation could be defined as the information that reflects the state, feature and the mode of as the unique feature in different fingers that every person has, the fingerprint is some of the first and most commonly used types of biometrics nowadays. Since it was invented, the fingerprint biometrics has been used for decades. The recent advanced technology allows for the more widespread use of this important tool. The theory to obtain the image of fingerprints is mainly based on the scanners, including optical scanner, capacitive scanner and ultrasound scanner.

The fingerprint biometrics have several outstanding advantages. They are always with persons and could not be lost or forgotten. Also such biometric techniques are fast and simple to use with low cost, with the characteristics of easily deployable and non-transferable. Nevertheless, such data could be left anywhere the fingers touched and be acquired easily.

DOI: 10.54254/2753-7048/10/20230321

2.2. Facial Features

This facial technology works by creating a digital representation of the facial characteristics through specific software. Such recognition is accomplished by analyzing the faces' structures including eyes, nose and cheekbones. The facial recognition could be divided into the 2D version and 3D version. The former method is generally considered as one of the fastest methods of biometrics for the images can be taken without interacting with the individuals [4]. However, the accuracy and security of it inferiors to the 3D version which needs more details of the facial features. Also, the flourish of social applications makes it easier to access others' photos with clear faces. The existed face detection technique is not adequate for the actual requirement any more in recent years. The advanced technology has become increasingly necessary in more complicit situations including learning the changes because of natural aging, illumination changes, and occlusions such as wearing mask or glasses.

2.3. Iris

As biometrics has advanced in recent years, iris has been considered a preferred trait for its unique pattern texture, lifetime stability, and regular shape contribute to good segmentation and recognition performance. According to its definition, iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of irises in individual's eyes [5]. Invented and patented by John Daugman, the algorithm of this system is quite complex, making its scanners relatively more expensive compared to other biometric modalities. In this occasion, it is not that possible to spread this technology into the public. The infrared light it used also cause harm to irises after constant use. But it should be admitted that the iris recognition is one of the most accurate biometric modalities. The low false acceptance rate and false rejection rate directly lead to a higher precision in its results.

3. Possible Infringements in Different Stages When Using Bioinformation

In order to improve the accuracy in specific essential areas including finance, government and aviation, many sorts of the bioinformation have played a role. Nevertheless, the operations lack of standardization or even the illegal ones could do harm to individuals' privacy. The usage of bioinformation would go through several stages after applying into the practice. All the steps are able to occur problems which will be analyzed afterwards. Even though the legislation has been improved in relevant area in recent years, the leftover problems should not be ignored at the meanwhile.

3.1. Pick-up Information

This collection would be generally considered as the most complicated stage during the whole procedure. It may involve many legal issues. Such situation happened in the latest case Carpenter v. McDonald's Corporation which has been appealed to the federal court in the US. The world-famous fast-food company was accused for the invasion of bioinformation privacy through its business AI drive-thru. According to its announcement, McDonald's AI voice assistant's voice recognition technology collects customers' voiceprint biometrics aiming at improving and providing better and more accurate services to customers with a tailored experience [6]. The fact is that plaintiff's complaint pointed out McDonald did not notify and acquired permission for the customers for their recordings, which violate the Illinois Biometric Information Privacy Act. According to the BIPA 740 ILCS 14/10, any sorts of biometric information should be permitted before accessing.

DOI: 10.54254/2753-7048/10/20230321

Not only in America, but it has also become a global trend to clarify the public's right in knowing about the collections of biological privacy. There has been administrative penalty in sales of real estates and cars because of the violation operations in China. The corporations saved the images of customers' facial features and voices to judge if they had been to their sales center to acquaint the products. With different marketing programs for different customers, they have earned more profits. Actually, their behaviors are considered illegally with the regulation in the Civil Code of Personality Rights. In current society for most formal applications and websites, users could authorize the background to collect and store their private information including the biological ones. But it could not be denied that some companies bundle the collection of biometric information with consumption and software applications, forcing the public to voluntarily give up the control and protection of information [7].

3.2. Storage

The corporations usually have the specialized database to store the information of their customers. Generally speaking, the storage of such privacy should be stable and safe. However, information leakage have happened in large modern corporations for many times. Reported by the Reuters in 2022, Facebook was fined by Data Protection Commission of Ireland for 265 million euros. About 533 million Facebook users had their personal data stolen by hackers in 106 countries. Such data includes their locations, email addresses and bioinformation for instance the facial images for face ID and fingerprints. It is not unique, the same incidents had occurred in Marriott International Inc. since 2014. Until it was investigated in 2018, that information included records from up to 500 million guests even with the duplicated ones. If the biological information which are stable once leaked, the personal rights and interests will be irreparable infringement. It revealed that the storage of bioinformation should further step up its security measures to resist loopholes like hackers.

3.3. Application

As mentioned above, the platforms need permission to acquire the biometric information of users. But the concealment clauses or the ambiguous phrasing may cheat the user of the available range of applications for their biometric privacy. Therefore, the newly enacted Connecticut Privacy Act which will come into effect since the July of 2023 has focused on this area. It has stipulated that no more default user consent to enable personalized advertisements. The situation is similar to the biometrics information. The New York City Biometric Information Privacy Act requires businesses that collect, retain or use biometric information from customers, to issue formal notices disclosing their activities and ensuring that customers are fully informed [8]. For example, when the user only authorizes to use the facial recognition technology when unlocking the account, the operators are legally prohibited to use such images in transactions.

3.4. Limitation to Transfer Bioinformation to Other Subjects

In the possession of a large quantity records of users' bioinformation, the corporations could make small profits but quick turnover with them. Recently the famous car-hailing app in China Didi was detected that it had over-collected 107 million pieces of facial recognition information from passengers. Be fined RMB 8.026 billion yuan, the sheer number of violations revealed by Didi shocked the public. Without ownership, it is at least immoral to sell personal biometrics information. The illegal use of personal biometric information could be various. They include the deep forgery technology which can change another person's face into the protagonist of a video, or the speech recognition technology that can match others' voice to video or audio. Even worse the publish facial information of another person on the virtual network may contribute to the cyberviolence called

DOI: 10.54254/2753-7048/10/20230321

cyber manhunt. To prevent such negative impacts, codes in many countries or regions, for instance the New York BIPC prohibit private entities from profiting by selling, leasing or trading biometric information. Actions of sharing between enterprises also need to be operated in accordance with the law and can not be carried out casually.

4. Resolutions towards These Dilemmas

As a part of a growing information society, nowadays the issue of bioinformation security is more crucial than ever. According to US media reports, more than one thousand class action lawsuits have been filed since BIPA was introduced. The giants like Microsoft, Google, Amazon and many other companies have all been accused of violating the act, for example, by using users' photos to train facial recognition systems without their explicit consent [9]. That has even got some tech companies into difficulties. It could be found that such measures have had the practical effect, while more resolutions are greatly needed as new problems arising. The followings are several steps that this essay illustrated and proposed. In recent years, the leftover problems should not be ignored at the meanwhile.

4.1. Accelerate the Improvement of Relevant Legal Regime

Law is the final but the most powerful constraint in ruling the codes of practice in the area of biometric privacy protection. Therefore, the authorities in different countries have realized the importance of the legislation and have already taken steps. The progress could be different between countries with different legal system and each has its advantages and disadvantages [10]. In the Common Law System countries like England, the precedents decided by higher hierarchy courts can quickly adapt to the latest situations. These cases could set examples on the basic rational concepts of courts towards the biometric information. As an essential source of law, such precedents may have dramatic effect on normalizing the usage of users' bioinformation in these countries. Nevertheless, for the Civil Law System countries including China, it usually takes a long period of time and complex procedures to enact a law. Until 2023, China only has the Act on the Protection of Personal Information. There has been no national special legislation for the bioinformation except for the local laws and regulations. Derecognition the effect of precedents, it could be harder to manage the market order in this field.

The relevant legal regime refers to two parts, including the professional standard for biometrics information, punishment situations and mechanism. It should be the national-wide criterion, acting as constraints across the whole country. Such regulations mainly considered two subjects as regulation objects: the government and the enterprises. For the authority, laws and regulations should clarify the subject qualification that can be allowed to enter the biometrics information industry by the network information department [11]. If an enterprise is found to have improperly kept or maliciously leaked the collected personal biological information, its business license should be revoked. It shall be put into the industry blacklist at the meanwhile. For enterprises, legislation should set specific requirements and stipulations to make all stages of collecting, storing and processing biometrics information become open and transparent. Such measure could contribute to facilitate the assignment of specific responsibilities to specific sections. In addition, companies should be required to carefully review the credentials of data protection commissioners, conducting regular internal audits as well as setting up internal data regulators.at the meanwhile.

4.2. Enhance Judicial Relief

Considered as the technological innovation, biometrics information are also accompanied by certain safety defects. In the case that it is difficult to completely avoid the risk of information loss or theft

DOI: 10.54254/2753-7048/10/20230321

at the present stage, it is necessary for legislation to provide appropriate risk recovery measures. It could provide timely and effective relief for relevant subjects. Akin to the right to be forgotten, most laws lack the similar rights which compulsively required the illegal recipients to completely and permanently delete others' personal biometrics information. The relief is suggested to regulate and authorize the courts to set the injunction or restraining order according to application from the injured party. Even though the privacy of bioinformation may not be materially harmed at this time, this kind of preventive judicial relief measures could prohibit it from being stored or used in any form illegally. In addition, in the event of biometrics information being disclosed, the information controller must fulfill the obligation of informing the security incident to other parties to minimize the occurrence or expansion of losses.data regulators at the meanwhile.

4.3. Raise Industry Standards and Barriers to Entry

According to the Face Recognition Application Public Research Report (2020) issued by the National Information Security Standardization Technical Committee of China and other institutions, the qualification of suppliers in biometrics technology varied widely, while most companies were even in the early stages. The low industry entry threshold leads to possible dilemmas for citizens in safeguarding rights of bioinformation, for instance, the companies may disappear or directly file for bankruptcy [12]. Therefore, the requirements for enterprise qualification should be clearly defined in order to implement the market entry certification system. Under this circumstance, the relevant activities can only be engaged after the relevant competent department approves and issues the license or qualification. It may improve the qualification of the biometrics information to some extent.

5. Frontier: Genetic Privacy

Accompanied with the development of technology, new sorts of biometric information have occurred and even applied to the practice. The genetic information, usually known as DNA, has an gradual effect on various aspects including criminal investigation and medical treatment [13]. As the latest technique, the privacy of it could be even difficult and complex to protect with no legislation or few precedents globally. In the American case Maryland v King, the Supreme Court finally indicated that DNA testing of felony arrestees could exist under the special requirements to look for and verify its identity. The similar situation happened in China that the authority used genetic information to search for a serial murderer and raper in 2016, who had been disappeared for nearly twenty years. While praising that DNA collection of arrestees aids in the accuracy of the criminal justice system, the public start to query whether such bioinformation could be used randomly by public institutions. As the most advanced method nowadays, the lack of regulation brings disorder to the criminal justice practice. Such arrests have sparked a fierce debate about the storage, disclosure and use of genetic data in the digital era [14]. As the essay mentioned above, with the progress of science and technology, the biometrics information may contain more types including the gene information. The authority is ought to pay more attention to adapt the rapid changes of practical bioinformation privacy protections.

6. Conclusion

As the cognition level of human in this field improves, the biometric technology will take on more forms and continue to revolutionize practice. It should be admitted that the biometrics have had huge beneficial impacts in citizens' life. However, on this occasion, more disputes may occur. The multiple attributes of individual bioinformation legal interests include the protection of privacy, personality and property. Under the circumstances of sudden and increasing bio-security risk factors

DOI: 10.54254/2753-7048/10/20230321

and potential threat factors, the pursuit of public safety has become the general mentality and legislative choice of the state and the public. It has been realized that the leakage of bioinformation may lead to serious implications which should be prevented through the joint efforts of the whole society. Relevant stakeholders should abide by the legal provisions and moral bottom line and consciously protect the security of users' biological information. Also, there is still a long way for the authorities to improve and consolidate relevant legal regulations. It could be estimated that the bioinformation would bring the humans with a promising future in numerous aspects with the correct specifications.

References

[1] *Kugler, M. B. (2019). From identification to identity theft: public perceptions of biometric privacy harms. UC Irvine Law Review, 10(1), 107-152.*

[2] *Oberly, D. J. (2020). Complying with the world's most stringent biometric privacy law. Ohio Lawyer, 34(1), 24-26.*

[3] *Hu, M. (2022). Biometrics and an ai bill of rights. Duquesne Law Review, 60(2), 283-301.*

[4] *Bharvada, K. (2002). Electronic signatures, biometrics and pki in the uk. International Review of Law, Computers & Technology, 16(3), 265-276.*

[5] *Roberg-Perez, S. (2017). The future is now: biometric information and data privacy. Antitrust, 31(3), 60-65.*

[6] *Nothing to Supersize Here: McDonald's Moves for Dismissal of Drive-Thru Data Privacy Litigation on Basis "Training Data" Not Regulated Under BIPA. (n.d.). The National Law Review, 10,2-9.*

[7] *Imaoka, H., Hashimoto, H., Takahashi, K., Ebihara, A., Liu, J., Hayasaka, A., Morishita, Y., & Sakurai, K. (2021). The future of biometrics technology: from face recognition to related applications. APSIPA Transactions on Signal and Information Processing, 10(1),8.*

[8] *Anderson, M. J., & Halpert, J. (2018). Washington become the third state with biometric privacy law: five key differences. RAIL: The Journal of Robotics, Artificial Intelligence & Law, 1(1), 41-46.*

[9] *Imperiali, R. (2012). The data protection compliance program. Journal of International Commercial Law and Technology, 7(3), 285-288.*

[10] *Kindt, E. J. (2013). Privacy and Data Protection Issues of Biometric Applications: A Comparative Legal Analysis. Springer Science & Business Media.*

[11] *Risher, M. (2023). Supreme Court Ruling a Blow to Genetic Privacy. American Civil Liberties Union. 27, 10-20.*

[12] *Stewart, L. (2019). Big data discrimination: maintaining protection of individual privacy without disincentivizing businesses' use of biometric data to enhance security. Boston College Law Review, 60(1), 349-386.*

[13] *Cofone, I. N. (2016). healthy amount of privacy: quantifying privacy concerns in medicine. Cleveland State Law Review, 65(1), 1-26.*

[14] *European, M. E. &. A. S. F. B. a. B., Lauss, G., & Taupitz, J. (2012). Private.Gen: Beyond Genetic Privacy ; Past, Present and Future of Bioinformation-control-regimes ; Draft Version Prsentet at the ESBB Conference Granada November.*