Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 241 (2024) 48–55

Procedia Computer Science

www.elsevier.com/locate/procedia

The 19th International Conference on Future Networks and Communications (FNC)
August 5-7, 2024, Marshall University, Huntington, WV, USA

Analysis of Legislative Framework Governing Biometric Data

Youna Jung[a,*], Ethan D. Virgil[a]

[a]*Knoury Colleage of Computer Science, Northeastern University, 1300 17th St N #1500, Arlington, VA 22209, United States*

Abstract

Biometrics has permeated modern technology, particularly within mobile devices, integrating into daily life. From the 14th century, biometrics has served as a foundational method for security, aiding in criminal identification through physical characteristics records. Advancements in technology have propelled the evolution of precise and automated systems for analyzing facial, vocal, and ocular biometrics. Major tech companies have adopted biometrics as the primary mode of user authentication, catapulting biometric security into the forefront of cybersecurity discussions. Despite the promising future of biometrics, governments worldwide are grappling with the challenging task of regulating the handling of biometric data. Mismanagement of biometric data could pose significant security risks to both individuals and public safety. Therefore, it is crucial to implement comprehensive regulations and legislative reforms to safeguard privacy and security in the era of biometrics. Towards this goal, this paper contributes to the discourse by identifying security and privacy issues related to biometric data. It conducts a comprehensive analysis of current legal frameworks governing biometric data through the lens of the CIAAA (Confidentiality, Integrity, Availability, Authenticity, and Accountability) security framework. Additionally, it highlights emerging trends and outlines the implications for future policymaking and technological advancements in this field.

Keywords: **Biometric Data; Security; Privacy; Regulations; Analysis**

1. Introduction

Biometric data, which includes fingerprint, iris, voice, and facial, has been widely used over the past decade and plays a key role in our everyday life, but its application is not new. In the 14th century, biometrics was utilized for storing criminal records and identifying suspects [1]. Over time, the technology that collects, processes, and analyzes

* Corresponding author. Tel.: +1-571-206-8719; fax: +1-571-206-8719.
E-mail address: yo.jung@northeastern.edu

10.1016/j.procs.2024.08.009

biometric data has evolved to automated and highly accurate systems, significantly contributing to diverse fields. The driving factor of the diverse and rapid adoption lies in its uniqueness and reliability. For instance, every individual, including identical twins, has a unique fingerprint that is exceptionally difficult to forge. Utilizing techniques like fingerprints or face recognition, we can effectively identify users and grant them necessary access to computing devices and services. In addition, biometric data facilitates a user-friendly and seamless experience, allowing even non-technical users to interact with services through simple touch or glance gestures. Compared to the traditional password-based authorization, biometrics democratize access by providing high-quality security based on users' unique biometric traits [2]. The widespread integration of biometric data, however, also introduces new challenges concerning security and privacy, which could pose threats to individuals, companies, and government. In the following section, we discuss the potential issues related to biometric data, including privacy breaches, lack of legal protection, and the risks associated with overreliance and overconfidence in biometric technology.

2. Security and Privacy Issues on Biometric Data

2.1. Issue 1: Privacy breaches

The uniqueness and immutability of biometric data in general provides us with more reliable, effective, and user-friendly ways to identify individuals, but at the same time, could arise a critical issue in security and privacy. Let us assume that a person's fingerprint gets compromised. The replicated fingerprint could be used by others against the desire of the fingerprint's owner and then the fingerprint will be permanently discarded. Even though there is a technical barrier to replicate or alter biometric data, the possibility of identity breaches has become serious threats in industry. Additionally, the collections of biometric data raise critical privacy concerns. Unlike the traditional authentication data such as passwords or secret keys, biometrics data including fingerprint, iris, retina, voice, and face, may contain critical personal data like gender, race, and health status. If biometric data is misused or shared by other parties, the consequences will tremendously impact users' everyday lives. For example, health insurance companies could use biometric data to refuse renewal of insurance contracts by identifying potential health problems of customers. On the other hand, biometrics stolen by others could be used to commit health fraud or give unauthorized individuals access to private healthcare records. Furthermore, biometrics could be utilized to create high-quality deep fake images and videos misrepresenting individuals. However, people are currently relying on the companies' honor systems, and existing fraud detection technologies with biometrics have failed to prove their correctness [3]. The requirements for new hardware like scanners and addition computation to detect synthetic data also becomes burdensome [4].

2.2. Issue 2: Lack of legal protection

Despite the potential catastrophic consequences of biometrics misuse, the legal aspects related to biometrics have not fully considered yet. Compared to the robust legal frameworks governing traditional authentication methods, regulations on biometric-based authentication are relatively deficient across countries. For example, in the United Sates (US), individuals can refuse to disclose a conventional password under the fifth amendment, which protects citizens against self-incrimination. However, the applicability of this protection to biometric-based credential often remains unclear [5]. While a few laws specify the legitimate use of biometrics and penalties for non-compliance, such as the General Data Protection Regulation (GDPR) in Europe and the Biometric Information Privacy Act (BIPA) of Illinois in U.S., their scope is limited, often failing to extend jurisdiction to address digital crimes committed across states or national borders. The lack of comprehensive legal framework for biometrics may result in the development and adoption of security technologies on biometric data that prioritize data collection and use over privacy protection. Consequently, there is an urgent need for explicit and thorough regulations that balance privacy protection with usability consideration, while incentivizing compliance with privacy regulations [6].

2.3. Issue 3: Overreliance and overconfidence on biometric-based security

Due to the substantial benefits described above, numerous applications and systems have adopted biometrics-based technologies for user authentication and authorization. As biometrics has been widely employed across diverse domains, people tend to lower their guard against these new technologies, placing trust in them without certified evaluations on their validity and reliability. However, excessive dependence and confidence in biometric-based technologies could bring significant privacy breaches and risk individuals' daily lives. The efficacy of biometric-based security services indeed heavily relies on the performance of the hardware and software responsible for reading and processing biometric data. As shown in [7], many existing services exhibit vulnerabilities to security attacks. In addition, biases inherent in the development process of some biometric-based services impede their performance. These biases embedded in services showing that specific physical attributes of users, such as skin color, can result in higher rates of false positives or false negatives, significantly diminishing their usability [8]. As evidenced by prior research, the performance and security level of biometric-based services are still in its development phase, requiring careful consideration before their widespread adoption.

3. Security and Privacy of Biometric Data through the CIAAA Security Framework

Before proceeding further, this section will delve into the pre-established CIAAA security framework and analyze the security of biometric data within the scope of CIAAA. CIAAA, an acronym for *Confidentiality*, *Integrity*, *Availability*, *Authenticity*, and *Accountability*, encapsulates five essential aspects of security frequently used to assess the security of applications and systems. Let us explore how CIAAA applies to the biometric data domain.

- *Confidentiality* – The confidentiality of biometric information, which is immutable and irreplaceable, could be more critical due to the severity of potential damage of data leakage [9]. It is the reason that confidentiality of biometrics is being treated with the highest priority in this domain.
- *Integrity* – The protection of biometric data against unauthorized modification or destruction is imperative. To this end, we need to effectively deter malicious actors from compromising the integrity of data, while incentivizing entities that successfully maintain data integrity.
- *Availability* – Biometric data must be accessible and available in a timely manner. Typically, private sector entities focus on availability, albeit public sector entities do not focus on availability of biometric data.
- *Authenticity* – Identifying users with their biometric data and granting necessary permissions based on their identification are pivotal for effective access control in applications and systems. Along with *confidentiality*, hence, any failure in *authenticity* regarding biometric data could yield disastrous consequences.
- *Accountability* – Once a user is authenticated and authorized to access data and services, it is required for systems to log an audit trail to keep a record. The *accountability* of systems becomes crucial during security event investigations and post-recovery from security attacks. For this reason, governments and judicial agencies dealing with biometric data necessitate robust system accountability.

To evaluate the efficacy of a security system, CIAAA is frequently used [10]. Therefore, it is important to identify pertinent issues within each security aspect, assess the extent of coverage of such issues in existing privacy legal framework, and discuss potential enhancements to promote the development of more impactful legislation.

4. Security and Privacy Regulations on Biometric Data

To diagnose both what we are doing well and what we are not, it is required to examine the current legislative framework on biometric data. This analysis entails an exploration of how biometric data is defined, how the security and privacy issues listed above are addressed, what types of rights and actions are allowed, as well as the enforcement methods.

1) ***Biometric Information Privacy Act (BIPA) of Illinois state-*** In 2008, the state of Illinois state enacted the Illinois Biometric Information Privacy Act (BIPA), marking one of the earliest attempts in the US to legislate the collection, use, storage, retention, and/or alteration of biometric data by companies. Operating at the state-level, BIPA affects exclusively private organizations, excluding government entities. The fundamental concept of BIPA is that an

individual's biometric data is their own property, affording them complete autonomy over its preservation, alteration, and access permission. To realize the concept, BIPA mandates companies utilizing biometric data to 1) establish clear and concise collection and retention policies accessible to all users, 2) obtain consents from users for the collection and retention of biometric data, 3) notify individuals of any modification to initial consented agreement or biometric data, 4) securely store biometric data, and 5) refrain from selling or profiting from biometric data [11]. The act empowers any private citizen whose right listed above is infringed upon by a company to seek resources, entitling them to potential compensation of up to $5,000 per violation. Since its inception, BIPA has become a cornerstone of biometric data privacy, leading to a myriad of cases at both the state and federal levels. One of the most well-known cases is the Rosenbach vs. Six Flags Entertainment Corp. in 2019, where in it was established that a plaintiff does not have to specify damages beyond violation of the rights enshrined in BIPA to initiate legal proceedings [12, 13]. Similarly, in the case Patel vs. Facebook in 2019, the court confirmed users' right to sue Facebook for mishandling facial recognition data under BIPA, providing a way for a class action lawsuit against the corporation in Illinois. This federal case proved the enforceability of BIPA violations at the federal level. In January 2020, the American Civil Liberties Union (ACLU) filed suit against *Clearview AI* for violating BIPA by building and selling a massive facial recognition database without explicit consent from Illinois residents. While initially focused on BIPA violations, the final ruling prohibited *Clearview AI*'s biometric data practices nationwide, severely limiting the data collection. According to CIAAA, BIPA targets to ensure robust protection of biometric data by encouraging its confidential and authorized use, along with metadata requirements for accountability. More than 182 cases have been alleged violations so far [14], but there is still room to enhance security and privacy further.

2) ***Capture or Use of Biometric Identifier Act (CUBI) of Texas state*** - The state of Texas passed the Capture or Use of Biometric Identifier Act (CUBI) in 2009 to govern the gathering and utilization of biometric data. The act stipulates that a private-sector company cannot capture biometric data for commercial purposes without obtaining informed consent and the subsequent consent is required for its commercial utilization. It also mandates that companies must securely store and destroy the collected data within a year of its collection except for some specific cases [15]. In contrast to Illinois's BIPA that allows citizens to litigate against companies, CUBI grants Texas's Attorney General the authority to pursue damages for CUBI violations, with significantly higher fines amounting to a civil penalty of $25,000 per violation. Compared to BIPA, CUBI only requires consent, not specifically written consent. In addition, CUBI solely addresses biometric information, whereas BIPA encompasses both biometric data and its derived information [16]. Despite its enactment in 2009, CUBI was first applied in March 2022 in the lawsuit against Meta, accusing the company of unlawfully capturing biometric data for over a decade and building an artificial intelligence database using data from Texans. Although the case remains ongoing, it comes after a class action lawsuit regarding the same data collection, in which Meta was found liable for $650 million in damages [17]. CUBI aligns with the CIAAA framework, but on a smaller scale compared to BIPA. It mandates that the applications and systems handling biometric data must disclose the company's data collection policy and offer an opt-out mechanism on their website. In addition, a secure and resilient database system and data removal upon user requests are required. However, the confidentiality requirement is relatively less stringent.
3) ***California Consumer Protection Act (CCPA) of California state*** - The California Consumer Protection Act (CCPA) and its extension, the California Privacy Rights Act (CPRA), stand as two legislative pillars aimed at ensuring security and privacy on data in California. Although these acts do not directly target biometric data, they provide essential privacy rights to the citizens, which include the right to know what data is being collected and sold, the right to deny the data collection or sale, and a non-discrimination clause for those opting out of collection. Both acts are relatively recent, with CCPA passed in 2018 and CPRA amendments approved in 2020 [18]. Similar to BIPA, CCPA and CPRA provide for private right of action, allowing individuals whose rights have been violated to sue offending companies. Currently, this private right of action is, however, limited primarily to the cases involving data breach. Since their enactment, over 300 cases have cited the CCPA, primarily concerning data breaches in finance, healthcare, and cloud services. As both acts address a broad spectrum of data collections beyond biometrics, they leave room for improvement regarding the right to action and potential compensation, and it is unclear their

alignment with the CIAAA framework compared to other acts. Nevertheless, they effectively emphasis data integrity and confidentiality by regulating that data sharing is permissible only with individuals who are the subject of the personal data and who have given consent, which can be revoked at any time.

4) ***General Data Protection Regulation (GDPR) of EU*** - The General Data Protection Regulation (GDPR) enacted in 2016 has been implemented across the European Union (EU) countries to guarantee individuals' rights on private data collection and transfer within the EU and to regulate businesses operating internationally within the EU. GDPR categorizes biometric data as personal data and consists of eleven sections, each focusing on different aspects of data privacy, including protocols, data transfer, storage, maintenance, liability, and compensation. Over 2,000 fines have been issued to date for GDPR enforcement [19]. Similar to CCPA, GDPR mandates that companies must obtain consent before collecting biometric data, inform users about data collection and third-party sharing, and grant users access to their data with the right to request its removal. Violations of GDPR can result in fines of up to 4% of a company's global revenue. Recent research highlights how the strict legal system of GDPR with significant fines affects overall technological development in EU [20, 21]. The most notable case involved Meta resulting in the €1.2 billion fine in May of 2023 for mishandling of user data. The major issue was that Meta shared personal data collected from EU users with companies in US against GDPR prohibiting the transfer of personal data outside of the EU [22]. Data transfer via standard contractual clauses (SCCs) to the US were considered breaches of Europeans data flow agreements. Meta strongly argued that the fines are extreme and the short deadlines to make extensive changes to their data management system, which would adversely affect the user experience for millions of Facebook users not impacted by GDPR. In addition to this case, over 2,000 fines have been levied [19]. As evidenced by these cases, GDPR emphasizes every aspect of the CIAAA framework.
5) ***GDPR of UK***- After the Brexit, the United Kingdom (UK) introduced its own version of GDPR that aimed at providing the equivalent levels of protections to the EU's GDPR [23]. The UK version requires that companies obtain explicit consent for data collection from users and disclose their policies on data handling and processing. While the UK has lowered the age that companies must obtain consent before data collection from 16 years old to 13 years old, most of the regulations remain consistent with the EU's GDPR. Compared to Eu's GDPR, however, it has been rarely used with only 13 fines levied since its inception [19]. Like the EU's GDPR, the UK's version underscores the confidentiality and integrity of biometric data, requiring systems to restrict authorized accesses and prevent from unauthorized modification.
6) ***Privacy Act (PA) 1988 of Australia*** - In Australia, privacy issues are controlled either by common laws or the Privacy Act (PA) 1988, which aims to protect a wide range of personal data, ranging from ethnic and racial information to an individual's IP address [24]. Compared to other laws specifically targeting biometrics, however, the scope of the protection in the PA 1988 is limited and narrow, considering solely fingerprint and face biometrics. This act mandates that both the Australian government and the private-sector entities disclose collected data, allow individuals to refuse to identify themselves, provide access to collected data, and if necessary, correct or destroy data. The PA 1988 prioritizes the confidentiality and integrity of personal data and issues severe fines for violations. According to the act, applications and systems dealing with personal data must obtain user consent, although existing systems do not have to completely overhaul if biometric data is to be stored locally on a user's device.
7) ***Protection of Personal Information Act (POPIA) of South Africa*** - South Africa introduced the initial version of the Protection of Personal Information Act (POPIA) in 2013, with enforcement commencing in 2021 [25]. This act explicitly defines biometric data as personal data to be protected. Similar to other laws mentioned above, POPIA mandates consent-based data collection and grants individuals the right to access and revoke data collected. However, POPIA regulates more severe consequences, not only fines but also the possibility of imprisonment. Citizens have the right to submit complaints under POPIA, but it is the responsibility of the government to investigate and enforce the legislation without granting citizens the right to private action. To facilitate enforcement, the act established the Information Regulator, an office in the South African government dedicated to the enforcement of POPIA. In addition, the act restricts data transfer from outside the country, unless certain security requirements are met. Regarding the CIAAA framework, POPIA is the one that strongly encourages accountability along with

confidentiality, authorization, and integrity. The potential consequences could be severe with up to a decade of imprisonment in case of failure in compliance. As the act is relatively new, the first case was in March 2022.

8) ***General Personal Data Protection (LGPD) Law of Brazil*** - Brazil legislated the General Personal Data Protection (LGPD) Law that establishes foundation for individuals' right on personal data within the country in 2020. This law encompasses a wide range of personal data, from biometric data to ethnicity, sexual preference, religious or political affiliation, and genetic information [26]. The first enforcement action under LGPD occurred in 2023, where the Brazilian government issued two relatively small fines to *Telekall Infoservice* for mishandling of user data. LGPD places significant emphasis on confidentiality to ensure that user data is only collected, shared, and analyzed with explicit user consent. It also specifies certain types of data that are prohibited from collection, such as political affiliation. If the collection of such data is unavoidable, systems must transparently inform users of their full control over data access, retention, and removal.
9) ***Digital Personal Data Protect (DPDP) Act of India*** - In August of 2023, India enacted the Digital Personal Data Protect (DPDP) Act that designed to safeguard a wide range of personal data and regulate its collection and handling practices. Similar to Australia's PA 1988, this act established a government board that tasked with data protection oversight, responsible for handling violations of the data protection laws [27]. The DPDP defines personal data in an extensive manner, as "a representation of information, facts, concepts, opinions or instructions in a manner suitable for communication, interpretation or processing by human beings or by automated means," potentially encompassing biometric data. As the act has been recently implemented, there is no case DPDP is applied to yet, but it is noteworthy that this act focuses on the integrity and accountability of systems. The government enforcement agency will monitor proper data collection and retention practices and ensure systems' accessibility for future audits. In case of severe violations, companies may face fines of up to 2.5 billion rupees.

5. Analysis of Legislative Framework on Biometric Data

In this section, we evaluate existing acts, laws, and regulations based on the following criteria: 1) impact on individuals, business, and governments, 2) the types of enforcement, 3) the right to action of citizens, and 4) the specificity on biometric data, and the result is presented in Table 1. To measure the comprehensiveness of the legal framework for security and privacy of biometrics, we examine their coverage of security aspects defined in the CIAAA framework in Table 2, with check marks to indicate consideration of each aspect. Analysis in Tables 1 and 2 reveals two primary limitations in existing legislation:

- *Insufficient specificity for biometric data* – Many existing laws and regulations treat biometric data as a part of a broad spectrum of personal data, including data such as IP addresses and political alignment. Unlike other types of personal data, biometric data is, however, unique to each individual and irreplaceable, thus the potential risk of data breaches could be tremendous. In addition, biometric data that could be directly tied to an individual's health like facial and iris scans, may constitute highly sensitive information requiring stronger protection than other data types.
- *Limitation on private rights and enforcement mechanisms* – In some jurisdictions, the private right of action on biometric data is still not explicitly outlined in policies, with enforcement falling under the purview of government agencies. Allowing the private right to action could be effective by providing a private incentive to address violations without overburdening law enforcement agencies, as seen in Illinois's BIPA and Texas's CUBI. In addition, while fines remain the major enforcement method across many countries, we need to diversify and strengthen enforcement methods to effectively deal with violations by both government and private sector entities.

To address the limitations identified above, we recommend two approaches:

- *Specialized biometric regulation* – We advocate for the establishment of a clear definition of biometric data and the implementation of dedicated regulations governing mandatory services and violations specific to biometrics to guarantee the *Confidentiality*, *Integrity*, *Availability*, *Authenticity*, and *Accountability* of biometric data. Additionally, implementing protection policies tailored to biometrics are essential to minimize

potential damage. Furthermore, regulations should foster international cooperation while monitoring sharing and transfer of biometric data across borders.

- *Diversification of enforcement methods* – It is imperative to develop a variety of enforcement mechanisms beyond fines, while simultaneously supporting companies in making their profit within regulatory frameworks. The magnitude of fines should be commensurate with the size of the company and the severity of the violation. Exploring options such as barring companies from engaging in certain business practices could be effective. Given the significance of biometric data in everyday life, more stringent methods such as those involving imprisonment, implemented in POPIA, could be considered to protect citizen's rights.

Table 1. Comparison of existing security and privacy regulations on biometric data

Country	Regulations	Impact on			Enforcement Types	Right to Action	Biometric Specificity
		Individuals	Business	Government			
United States (US)	Illinois-BIPA	High (Private right to action)	High (Complete overhaul of existing practices)	High (Significant increase in class actions)	Fines	Yes	Yes
	Texas-CUBI	Low	Medium (Depending on Texas Attorney General)	High (Enforcement task)	Fines	No	Yes
	California-CCPA	High (Private right to action)	High (Complete overhaul of existing practices)	Medium (Not consider data breaches	Fines	Yes	Yes
European Union (EU)	GDPR	High (Private right to action)	High (Complete overhaul of existing practices)	High (Enforcement task)	Fines	Yes	Designates a separate type of data for biometrics
United Kingdom (UK)	GDPR	High (Private right to action)	High (Complete overhaul of existing practices)	High (Enforcement task)	Fines	Yes	Designates a separate type of data for biometrics
Australia	PA 1988	High (Private right to action)	High (For large companies)	High (Enforcement task on all federal data)	Dedicated government office (OAIC)	Indirectly through OAIC	No
South Africa	POPIA	Low	High (Severe overhauls and consequences)	High (With a dedicated government office)	Dedicated government office	No	Indirectly (With wide range of considerations)
Brazil	LGPD	Low	Low (Loose enforcement with small fines)	Low (Enforcement is entirely up to the government)	Fines	No	Designates a separate type of data for biometrics
India	DPDPA	Low	High (Complete overhaul of existing practices)	High (Enforcement task on all federal data)	Dedicated government office (Yet established)	Indirectly through a government office	Yes (With wide range of considerations)

Table 2. Analysis of existing regulations with the CIAAA framework.

√: Covered, Δ: Covered with limitations, X: Not covered

		BIPA	**CUBI**	**CCPA**	**GDPR**	**GDPR**	**PA1988**	**POPIA**	**GPDPL**	**DPDPA**
Confidentiality	Requires consent for data retention	√	√	√	√	√	√	√	√	√
	Allow revocation of consent	√	√	√	√	√	√	√	√	√
	Secure data store	√	√	√	√	√	√	√	√	√
Integrity	Not allow unauthorized modification	√	√	√	√	√	√	√	√	√
Availability	Access to collected data	√	√	√	√	√	√	√	√	√
Authenticity	Not allow unauthorized access to data	√	√	√	√	√	√	√	√	√
	Not allow to share data with unauthorized	√	√	√	√	√	√	√	√	√
Accountability	Financial enforcement	√	Δ	√	√	√	√	√	Δ	N/A
	Enforcement beyond fines	X	X	X	X	X	X	X	X	X
	Biometric-specific data control	√	√	√	X	X	X	√	X	√

6. Conclusion

As biometrics has become an integral part of everyday life, the volume of biometric data collected has surged incredibly with significant risks of data leakage and misuse for malicious purposes. With the advance in big data technology, biometrics-based applications and services have been more widely adapted across various domains. Given the sensitive nature of biometric data, privacy breaches could have severe consequences, impacting individuals' lives. To protect people's security and privacy, it is critical that governments legislate to govern the collection, use, retention, and sharing of biometric data. In this paper, we identify the security and privacy issues on biometric data based on the CIAAA security framework and then conduct a comprehensive analysis of laws, acts, and regulations established in the US, EU, UK, Australia, Brazil, South Africa, and India. Through an assessment of their impacts, enforcement methods, and coverage of security aspects, we discuss the findings including limitations and propose suggestions to enhance the effectiveness of legislation on biometric data. As the next step, we plan to analyze the regulations to assess their impact on domestic and international business, as well as explore methods to prevent and detect international cybercrime related to biometric data. Additionally, we will consider incentive systems to encourage both public and private sectors to comply with the regulatory requirements in the future.

References

[1] Piazza, P.A. (2014). Alphonse Bertillon and the Identification of Persons (1880-1914).
[2] Faundez-Zanuy, M. 2006. "Biometric security technology." *IEEE Aerospace and Electronic Systems Magazine* 21, 6 (2006), 15–26. DOI:http://dx.doi.org/10.1109/maes.2006.1662038
[3] Yang, W., Wang, S., Hu, J., Zheng, G., & Valli, C. (2019). "Security and Accuracy of Fingerprint-Based Biometrics: A Review." *Symmetry,* 11(2):141. https://doi.org/10.3390/sym11020141
[4] Espinoza, M. (2011). "Vulnerabilities of fingerprint reader to fake fingerprints attacks." *Forensic Science International,* 204(1–3), 41-49. DOI: https://doi.org/10.1016/j.forsciint.2010.05.002
[5] Redfern, A.N. (2021). "Face it – The Convenience of a Biometric Password May Mean Forfeiting Your Fifth Amendment Rights." *Penn State Law Review*
[6] L. Lai, S. -W. Ho and H. V. Poor, "Privacy–Security Trade-Offs in Biometric Security Systems—Part I: Single Use Case," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 122-139, March 2011, doi: 10.1109/TIFS.2010.2098872.
[7] M. Faundez-Zanuy. 2004. On the vulnerability of biometric security systems. *IEEE Aerospace and Electronic Systems Magazine* 19, 6 (2004), 3–8. DOI: http://dx.doi.org/10.1109/maes.2004.1308819
[8] Perkowitz, Sidney. 2021. "The Bias in the Machine: Facial Recognition Technology and Racial Disparities." *MIT Case Studies in Social and Ethical Responsibilities of Computing, no. Winter 2021 (February)*. https://doi.org/10.21428/2c646de5.62272586.
[9] Rathgeb, C., Uhl, A. A survey on biometric cryptosystems and cancelable biometrics. *EURASIP J. on Info. Security* **2011**, 3 (2011).
[10] Fenrich, K. (2008, February). Securing your control system: the "CIA triad" is a widely used benchmark for evaluating information system security effectiveness. *Power Engineering*, *112*(2), 44+. https://link.gale.com/apps/doc/A177028777/AONE?u=anon~e1988afb&sid=googleScholar&xid=20af50f0
[11] Illinois General Assembly. 2008. Biometric Information Privacy Act, Public Act 095-0994. 95th General Assembly. Available at: https://www.ilga.gov/legislation/publicacts/fulltext.asp?Name=095-0994
[12] Supreme Court of Illinois. (2019). Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186. Retrieved from https://www.illinoiscourts.gov/Resources/f71510f1-fb2a-43d8-ba14-292c8009dfd9/123186.pdf
[13] ACLU of Illinois. (n.d.). Rosenbach v. Six Flags. Retrieved from https://www.aclu-il.org/en/cases/rosenbach-v-six-flags
[14] S.T.O.P. - The Surveillance Technology Oversight Project. (n.d.). Biometric Information Privacy Act (BIPA) Litigation Tracker. Retrieved from https://www.stopspying. org /bipa-litigation-tracker
[15] Texas Legislature. (2017). Business and Commerce Code Chapter 503. Biometric Identifiers. Retrieved from https://statutes.capitol.texas.gov/Docs/BC/htm/BC.503.htm
[16] Ahlering, Thomas, & Cockroft, Andrew. "All eyes on Texas after filing first enforcement action under State's biometric privacy law." *JDSupra*. Retrieved October 23, 2023, from https://www.jdsupra.com/legalnews/all-eyes-on-texas-after-filing-first-1933187/.
[17] Granitz, P. 2022. Texas sues Meta, saying it misused facial recognition data. *NPR*. (February 2022). Retrieved October 23, 2023 from https://www.npr.org/2022/02/15/1080769555/texas-sues-meta-for-misusing-facial-recognition-data
[18] Navarro, S and Korn, A. An overview of why class action privacy lawsuits may have just gotten bigger – yet again. *Mintz*. Retrieved October 23, 2023 from https://www.mintz.com/insights-center/viewpoints/2826/2023-03-01-overview-why-class-action-privacy-lawsuits-may-have-just
[19] GDPR Enforcement Tracker. Retrieved October 23, 2023b from https://www.enforcementtracker.com/
[20] Li, He, Yu, Lu, & He, Wu. (2019). "The impact of GDPR on Global Technology Development." *Journal of Global Information Technology Management,* 22(1), 1–6. DOI: http://dx.doi.org/10.1080/1097198x.2019.1569186.
[21] Albrecht, J.P. (2016). "How the GDPR will change the world." *European Data Protection Law Review,* 2(3), 287–289. DOI: http://dx.doi.org/10.21552/edpl/2016/3/4.
[22] Goujard, Clothilde & Scott, Mark. (2023). "EU hits Meta with record €1.2B privacy fine." *Politico.* https://www.politico.eu/article/eu-hits-meta-with-record-e1-2b-privacy-fine/.
[23] Government Digital Service UK. 2015. Data protection. (September 2015). Retrieved October 23, 2023. from https://www.gov.uk/data-protection
[24] Australian Government, 'Privacy Act 1988,' 1988. [Online]. Available: https://www.oaic.gov.au/privacy/privacy-legislation/the-privacy-act
[25] POPIA, "Protection of Personal Information Act (POPI Act)," *POPIA*, 2021. https://popia.co.za/
[26] J Isaza, John J. & Katshir, Hannah. (2020). "Brazil Passes Landmark Privacy Law: The General Law for the Protection of Privacy," *American Bar Association.* April 2020.
[27] "The Digital Personal Data Protection Bill, 2023," *PRS Legislative Research*. https://prsindia.org/billtrack/digital-personal-data-protection-bill-2023