ABHIDHVAJ LAW JOURNAL

[www.abhidhvajlawjournal.com]

The goal of Abhidhvaj Law Journal is to offer an open-access platform where anyone involved in the legal profession can contribute their research on any legal topic and aid in building a quality platform that anyone can use to advance their legal knowledge and experience.

Editor In chief – Assistant Professor Mr. Janmejay Singh

Publisher & Founder – Vaibhav Sangam Mishra

Frequency – Quarterly (4 Issue Per year)

ISSN : 2583-6323 (Online)

Biometric Tech and data privacy

AUTHOR'S NAME – Minjal Sankahla, B.A, LL.B(Hons.), Compl.

INSTITUTION NAME - Indore Institute of Law.

ABSTRACT:

Using biometric technology, a person's distinct identification can be verified. This makes it simpler for the government and other areas of the nation to recognize the person using their distinctive features. Hospitals, banks, schools, nationality certificates, and many more industries all employ this technology. The growing usage of biometric identification has advantages as well as disadvantages, particularly for an individual's personal information. Though not in a technological form, biometric technology has always been a part of life. Due to privacy violations, a lot of people struggle. Businesses must abide by rules and regulations to avoid fines and safeguard customer data and privacy. Making sure that the right safeguards are in place to protect the security and privacy of biometric data is crucial as biometric technology develops further. To safeguard citizens from data breaches, the government is implementing several significant security steps. Biometric data must be protected from misuse or unauthorized access because it is extremely sensitive. In this post, we'll examine a variety of biometric technologies together with security-related rules and regulations.

Keywords: Biometric technology, Breach of data, Impact, laws, and penalties.

Research objective

1. To analyze whether biometric technology is safe and protected worldwide.
2. To analyze what are the provisions in case of violation of privacy and biometric data theft.
3. To figure out whether laws in India are sufficient to curb the problem of breach of data.

INTRODUCTION:

The 21st century is the era of technology. New ways and techniques are discovered to make man's work easier and effortless. But after introducing biometric technology it gets more easier to access the person's data without any confusion because every person is unique so does their biometrics. We can find traces of Biometrics back to ancient times, especially in India handprints were used by kings and important officials for identification purposes. As a method

of authentication, use official documents. Furthermore, thumb impressions were used to identify people. People would frequently stamp their thumbprints on documents to verify their legitimacy and give authorization in legal and administrative circumstances. Even though it wasn't used in the context of technology, facial recognition was used to identify people in ancient India. In ancient Indian society, ancestry and clan affiliation were essential. Families, castes, and clans served as means of communal identification and were frequently utilized to identify an individual's identity. The usage of symbolic symbols or seals as identity markers is acknowledged in certain ancient Indian written works. These marks, which would be exclusive to a person or group, might be used to verify papers or develop ownership. But the incorporation of biometric technology like iris scanning and fingerprint recognition was not present during ancient times.[1] Alphonse Bertillon's endeavors to identify criminals through an anthropometric system marked the beginning of the use of biometrics for recognition and security in the late 19th century.[2] Biometric technologies including voice, iris, and facial identification were created in the second part of the 20th century[3]. The earliest organized collection of hand images for identifying purposes dates back to 1858. The 1960s: innovations in biometric technology lead to high-tech scanners with near-perfect biomarker reading accuracy. 1991: real-time recognition is made feasible by the development of facial detection technologies. Early in the new millennium: biometric authentication started appearing in commonplace uses.[4] Currently: facial recognition on smartphones, fingerprint access to financial apps, and biometric payment cards are examples of how biometric identification has entered the mainstream. The biometric data is used for identification or certification reasons, and the collected data is subsequently compared to a database of previously stored templates or patterns. When compared to standard authentication techniques like passwords or access cards, biometric authentication methods offer convenience and more safeguards. However, it is crucial to address privacy issues and make sure that suitable security measures are in place to protect people's biometric data.[5]

[1] *Capitol Technology University*, https://www.captechu.edu/blog/evolution-of-biometrics , (last visited July. 6, 2023).

[2] *Thales group* https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/history-of-biometric-authentication , (last visited July. 6, 2023)

[3] *Bioconnect*, https://bioconnect.com/2021/12/08/a-brief-history-of-biometrics/ , (last visited July. 6, 2023)

[4] Stephen Mayhew, 'History of Biometrics', *Biometric update.com*, (July. 01, 2023, 9:29 PM), https://www.biometricupdate.com/201802/history-of-biometrics-2

[5] Biometric Technology: A Brief History https://loginid.io/blog/biometric-technology-a-brief-history

Types of biometric technologies

Individuals are identified and authenticated using biometric technologies based on distinctive physical or behavioral attributes. such as-

1. Fingerprint recognition: it is one of the most widely used biometric technology. It functions by identifying the particular ridges and patterns on a person's fingertip. For identification or verification reasons, a fingerprint scanner records the fingerprint image, which is later compared to a database of fingerprints that have been previously stored.[6] With the use of optical scanners it captures a 2D image of the fingerprint and by using algorithms identifies the unique patterns of the prints.[7]
2. Heart-rate sensors- Heart-rate sensors track each person's specific heartbeat rhythms. The user's heart rate can be tracked as part of continuous authentication, which verifies their identity and presence.
3. Voice recognition- the distinctive qualities of a person's voice, such as pitch, tone, and pronunciation, are examined by voice recognition technology. For identification or verification, a voiceprint is created and compared to a voiceprint that has already been saved.[8]
4. Iris recognition- the colored portion of a person's eye's distinctive patterns are recorded by iris identification technology. It takes high-resolution pictures of the iris with specialized cameras and then converts those pictures into a digital template. For identification or verification, this template is compared to a database.[9]
5. Retina scanning- the unique designs of blood vessels in the back of the eye is photographed by retina scanning equipment using infrared light. To identify or verify the pattern, a digital template of it is created and compared to a database.[10]
6. Facial recognition- technology for facial identification examines a person's particular facial characteristics and proportions. It maps face landmarks using algorithms to

[6] Mary Clark, 'Fingerprint Reader Technology Comparison: optical finger scanner, capacitive-based fingerprint reader and multispectral imaging sensor, (*Bayometric)* (July. 01, 2023, 9:29 PM), *https://www.bayometric.com/fingerprint-reader-technology-comparison/*

[7] Zachary Kew-Denniss, 'Optical, capacitive, and ultrasonic fingerprint sensors- how do they work? *Android Police*, (July. 01, 2023, 9:29 PM) https://www.androidpolice.com/optical-capacitive-and-ultrasonic-fingerprint-readers-how-do-they-work/

[8] Biometrics: definition, use cases, latest news, *Thales group*, (July. 01, 2023, 9:29 PM) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

[9] What is biometrics? How is it used in security? https://usa.kaspersky.com/resource-center/definitions/biometrics

[10] Matt Gibson, 'What is Biometric Identification and how does it work?' *M2SYS*, (July. 01, 2023, 9:29 PM), https://www.m2sys.com/blog/biometric-technology/what-is-biometric-identification-and-how-does-it-work/

produce a facial template. To identify or confirm a person, this template is then compared to a database of previously saved templates.[11]

7. Dynamic signature analysis-it is a behavioral biometric tool, that examines a person's signature to determine who they are. To establish a distinctive biometric template, this technology records the speed, pressure, and rhythm of the signature. Utilizing this technology for computer access would allow for ongoing identity verification of computer users.[12]
8. Multimodal biometrics- to create a more reliable and accurate identification and authentication process, multimodal biometrics combines many biometric technologies. For instance, combining speech recognition technology can result in a more secure and dependable identification process.[13]
9. DNA-Based recognition- an individual's DNA is used to confirm their identity vis DNA-based recognition, a sort of physiological biometric technology. The development of this technology is still ongoing, and it is not yet in wide use[14].

Revolutionary biometric technologies and the purpose of Industries adapting it

1. Dynamic Signature Analysis
2. Gait recognition
3. Ear Shape recognition
4. Vein recognition

For identity verification, fraud protection, and safe access to financial services, these businesses use biometric technologies. Government organizations are utilizing biometric technologies for border control, law enforcement, and national security reasons.[15] For patient identification, electronic health records, and safe access to medical data, biometric technologies are being employed in healthcare. For student identification, attendance monitoring, and safe access to

[11] Advantages and disadvantages of biometrics, *Mitek*, (July. 01, 2023, 9:29 PM), https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics

[12] Russ Ryan, Emerging Biometric Technologies, *Security infowatch.com*, (July. 01, 2023, 9:29 PM), https://www.securityinfowatch.com/access-identity/access-control/article/10517342/emerging-biometric-technologies

[13] Biometrics: definition, use cases, latest news, *Thales group*, (July. 01, 2023, 9:29 PM) https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/inspired/biometrics

[14] Biometrics and Privacy-issues and challenges, (*OVIC*) https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/

[15] Russ Ryan, Emerging Biometric Technologies, (*Security infowatch.co*, (July. 01, 2023, 9:29 PM) https://www.securityinfowatch.com/access-identity/access-control/article/10517342/emerging-biometric-technologies

educational resources, biometric technologies are employed in schools and colleges. Secure access to mobile devices and services is made possible by the use of biometric technologies in telecommunications. Wearables like smartwatches and fitness trackers use biometric technologies for secure access to personal information and health monitoring.[16]

How Biometric Tech deals with concerns over data privacy & security

1. Privacy- because biometric information is so private and delicate, there are questions concerning how it should be gathered, saved, and used.
2. Informed consent- before collecting and using a person's biometric data, it is essential to get that person's informed consent.
3. Security and data breaches- once compromised, biometric data cannot be updated, Unlike a password or PIN. Biometric system security is a problem, as is the possibility of data breaches.
4. Discrimination and Bias- the use of biometric technologies could unintentionally reinforce prejudice and discrimination. When biometric systems' algorithms are trained on skewed or underrepresented datasets, unfair results and treatment of particular people or groups may occur.
5. Function creep- biometric information may be used for other reasons without the subjects' knowledge or agreement, which is a problem. The ability of people to regulate their biometric data and the possibility of mission creep in its application are both questioned by this function creep.[17]
6. Encryption and secure storage- during transmission and storage, biometric data is frequently encrypted to prevent unauthorized access.
7. Minimization of data- instead of storing the real raw data, biometric systems often save a template or a mathematical representation of the biometric data.[18]
8. Access control and authentication- only people with permission can access and use the biometric data thanks to the tight access control measures used by biometric systems.

[16] Vincent Bonneau, IDATE and Laurent, Virginie Lefebvre, PwC, 'Biometrics technologies: a key enabler for future digital services', European Commission, (July. 01, 2023, 9:29 PM), https://ati.ec.europa.eu/sites/default/files/2020-07/Biometrics%20technologies%20-%20a%20key%20enabler%20for%20future%20digital%20services%20%28v2%29.pdf

[17] Biometrics and Privacy-issues and challenges, (*OVIC*) https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/ (last visited July. 6, 2023)

An additional security measure is provided by multi-factor authentication, which combines biometrics with a PIN or password.[19]

9. Biometric data protection- many nations have passed laws and rules regarding the protection of biometric information. To ensure that the necessary security measures are in place, these rules specify the rights and obligations of organizations that gather and utilize biometric data.
10. Transparency and informed consent- individuals should receive clear and transparent information from biometric systems about how their biometric data is collected, stored, and used.
11. Regular audits and compliance- companies handling biometric data must regularly audit and evaluate their operations to make sure that privacy and security regulations are being followed.
12. Ethical considerations- the ethical development and application of biometric technology should take into account the potential negative effects on people's privacy and human rights.[20]

Essential components of Biometric technology

The basic components of biometric technology are:

- Input interface (sensors)
    1. a metal oxide semiconductor (CMOS) imager
    2. a charge-coupled device (CCD)

    these sensors are used in the case of face recognition, handprint recognition, or iris/ retinal recognition systems.[21]
- Processing Unit
- Storage unit
- Decision unit

[19] Sterling Miller, 'the basics, usage, and privacy concerns of biometric data', *Thomson Reuter*, (July. 01, 2023, 9:29 PM), https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data

[20] Sterling Miller, 'the basics, usage, and privacy concerns of biometric data', *Thomson Reuter,* (July. 01, 2023, 9:29 PM), https://legal.thomsonreuters.com/en/insights/articles/the-basics-usage-and-privacy-concerns-of-biometric-data

[21] Biometrics- overview, https://www.tutorialspoint.com/biometrics/biometrics_overview.htm , (last visited July. 6, 2023).

Data breach

- **Impact of it on the individual-** a hack of the Biostar 2 biometric database in August 2019 made 28 million records, including the fingerprints of more than 1 million people, publicly available. Researchers found a significant in the Biostar 2 biometric systems used by banks, the UK police, and defense companies in August 2019. The hack disclosed employees' biometric data that weren't secured, along with personal data. Given that the service is available in 1.5 million places worldwide, the breach's sheer size was concerning[22]. The use of fictitious biometric data to obtain unauthorized access to systems or data is known as "biometric spoofing", and it is an increasing hacking threat. False voice recordings, phony facial photos, and fake fingerprints can all be used for spoofing. A breach of biometric data may have a major effect on an individual. Once compromised, biometric information cannot be updated, unlike a password or PIN. This may result in many nefarious crimes.[23]
- **Legal implications-**
    1. Data protection and privacy laws
    2. Regulatory compliance
    3. Civil liability
    4. Regulatory investigations and penalties
    5. Contractual obligations
    6. Criminal liability

- **Consequences for an organization-** An organization that experiences a biometric data breach may face serious and wide-ranging repercussions.[24] Loss of money, costs for the investigation into the breach, alerting those affected, offering credit monitoring services, paying legal fees, paying fines under the law, and probable legal action are some examples. A biometric data leak can seriously harm a company's reputation and

[22] Josh Taylor, 'Major breach found in biometrics system used by banks, UK police, and defense firms', *The Guardian,* (July. 01, 2023, 9:29 PM) https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

[23] Zak Doffman, 'New Data Breach has exposed millions of fingerprint and facial recognition records: report', *Forbes,* (July. 01, 2023, 9:29 PM) https://www.forbes.com/sites/zakdoffman/2019/08/14/new-data-breach-has-exposed-millions-of-fingerprint-and-facial-recognition-records-report/?sh=48388dea46c6

[24] Biometric Data breach: database exposes fingerprints, facial recognition data of 1 million people, *Norton,* (July. 01, 2023, 9:29 PM) https://us.norton.com/blog/emerging-threats/biometric-data-breach-database-exposes-fingerprints-and-facial-recognition-data

reduce client confidence.[25] If organizations don't appropriately protect biometric data, they may be subject to legal and regulatory repercussions. Customers and staff may become less trustworthy as a result of a data leak. Breach of biometric data might put people at risk for fraud and identity theft.[26] An organization's operations may be seriously disrupted as a result of dealing with a data breach's aftermath. Managing the public relations and communication components of the issue, as well as rerouting resources to investigate and address the breach, are all examples of this.

- **Legal obligations on the organization-** there are numerous jurisdictions, including all 50 states in the US and the District of Columbia, that have breached notification laws that call for businesses to alert people when certain categories of personal information, such as biometric data are compromised in a breach[27]. Once a breach is found, organizations are often required to notify the impacted parties as soon as possible. Information concerning the breach, the kinds of biometric data that were exposed, and the risks or harms that people may take to protect themselves should all be included in the notification to impacted persons.[28] Affected individuals may need to be notified by a company via phone, email, or other forms of physical or electronic communication. Organizations may be legally required to notify regulatory bodies, such as data protection authorities or other pertinent government entities, of the breach in addition to notifying the impacted persons.[29]
- **Consequences**
    1. Irreversible damage
    2. Identity theft
    3. Malicious activities
    4. Spoofing

[25] Clare O'Gara, 'What are the consequences of a biometric data breach?' *Secureworld,* (July. 01, 2023, 9:29 PM), https://www.secureworld.io/industry-news/biometric-data-breach-consequences

[26] Josh Taylor, 'Major breach found in biometrics system used by banks, UK police, and defense firms', *The Guardian,* (July. 01, 2023, 9:29 PM), https://www.theguardian.com/technology/2019/aug/14/major-breach-found-in-biometrics-system-used-by-banks-uk-police-and-defence-firms

[27] Requirements of the District's data breach notification law, *office of the Attorney General for the District of Columbia, https://oag.dc.gov/about-oag/laws-legal-opinions/requirements-districts-data-breach-notification*, (last visited July. 6, 2023).

[28] Kirk J. Nahra, Ali A. Jessani, Samuel Kane, 'Biometric Privacy Law Update', *WilmerHale,* (July. 01, 2023, 9:29 PM), https://www.wilmerhale.com/insights/client-alerts/20230224-biometric-privacy-law-updatem

[29] Kyle D. Black, 'Biometric privacy laws create new Avenue for data breach class Actions', *Buchanan,* (July. 01, 2023, 9:29 PM)https://www.bipc.com/biometric-privacy-laws-create-new-avenue-for-data-breach-class-actions

5. Legal and regulatory consequences
6. Ethical concerns

Impact of Biometric Technologies

- **On individual-** The privacy and autonomy of an individual may be impacted by biometric technologies in several ways, raising ethical questions like There are issues with how this data is used and secured when it is collected and stored by biometric technologies[30]. Before collecting and using a person's biometric data, it is essential to get that person's informed consent. Once compromised, biometric information cannot be updated, unlike a password or PIN. There are worries regarding the safety of biometric technologies and the possibility of data breaches. Biometric technologies might unintentionally support prejudice and discrimination. Without the subjects' knowledge or consent, biometric data obtained for one purpose may be utilized for other purposes. This function creep raises concerns about the control people have over their biometric data and the possibility of mission creep in its application. It can be difficult to obtain informed permission from vulnerable groups, such as kids, the elderly, or people who have cognitive disabilities. Accountability and transparency are required when using biometric technologies.[31]
- **Marginalized communities-** In marginalized communities, biometric technology may have an outsized effect. Bias is possible with biometric technologies, especially when it comes to underrepresented groups[32]. Marginalized groups may be more susceptible to privacy invasions as a result of past and present discrimination.[33] People with some disabilities, such as those who are blind or have mobility issues, might not be able to use biometric technologies. Because of this, marginalized communities may have difficulty accessing healthcare[34]. Because they can be expensive to implement, biometric technologies may not be widely used in healthcare facilities that serve

[30] Biometrics and Privacy-issues and challenges, (*OVIC*) https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/ , (last visited July. 6, 2023).
[31] Jonathan Turley, 'Anonymity, Obscurity, and Technology: Reconsidering privacy in the age of Biometrics', pg .no. 2179, Year 2020, https://www.bu.edu/bulawreview/files/2021/01/TURLEY.pdf
[32] Jessica Groopman, 'In biometrics, security concerns span technical, legal and ethical', *TechTarget*, (July. 01, 2023, 9:29 PM), https://www.techtarget.com/searchsecurity/tip/In-biometrics-security-concerns-span-technical-legal-and-ethical
[33] Kais Sfaxi Dip CSMP, 'The Surging Dominance Of Biometric Technology and its Game Changing impact', *Linkedin*, (July. 01, 2023, 9:29 PM), https://www.linkedin.com/pulse/rise-biometric-technology-its-impact-security-kais/
[34] Anna Papadopoulos, 'The Pros and Cons of Biometrics', *CEOWORLD Magazine*, (July. 01, 2023, 9:29 PM), https://ceoworld.biz/2022/05/09/the-pros-and-cons-of-biometrics/

underserved populations. The extensive use of biometric technologies may have ethical repercussions, including increasing surveillance, a loss of anonymity, and possibly declining institutional trust. Because of past and present discrimination, marginalized communities may be more susceptible to these ethical issues[35].

- **Vulnerable populations, refugees, and immigrants-** A vulnerable population, such as refugees or undocumented immigrants, may be particularly affected by the usage of biometric technologies in healthcare. Among the possible effects and factors to take into account are[36]:
    1. Privacy and security concerns
    2. Access and Inclusion
    3. Discrimination and Bias
    4. Data protection and misuse
    5. Legal and Ethical Considerations

Laws to protect biometric data worldwide and penalties

- **New York Biometric privacy act (AB 1362)-** the consequences for breaking the New York Biometric Privacy Act. However, comparable biometric privacy statutes in other jurisdictions, like the Illinois Biometric Information Privacy Act (BIPA), offer a private right of action and permit damages of a certain sum per infringement and reckless disregard for the rule. it attempts to control how biometric data is gathered, used, and kept in the state of New York.[37]
- **Illinois Biometric Information Privacy Act (BIPA)-** With its BIPA, Illinois has led the way in establishing biometric privacy laws. It grants people a private right of action and establishes stringent guidelines for businesses about the authorization, disclosure, and storage of biometric data.[38]

[35] Russ Ryan, Emerging Biometric Technologies, *Security infowatch.com*, (July. 01, 2023, 9:29 PM), https://www.securityinfowatch.com/access-identity/access-control/article/10517342/emerging-biometric-technologies

[36] *Congressional Research Service*, https://crsreports.congress.gov/product/pdf/IF/IF11783 , (last visited July. 6, 2023).

[37] Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, 'The Anatomy of biometric laws: what U.S companies need to know in 2020', (*The National Law Review*, 15 January 2020), (July. 01, 2023, 9:29 PM), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020 \ thelyonfirm, https://www.thelyonfirm.com/class-action/data-privacy/biometrics/, (last visited July. 6, 2023).

[38] Fredric D. Bellamy, 'Looking to the future of biometric data privacy laws', (*Reuters*, 6 April 2022), (July. 01, 2023, 9:29 PM), https://www.reuters.com/legal/legalindustry/looking-future-biometric-data-privacy-laws-2022-04-06/

- **General Data Protection Regulation (GDPR)-** The collection, use, and storage of personal data, including biometric data, is governed by this European Union (EU) privacy regulation.[39]
- **California Consumer Privacy Act (CCPA)-** This statute includes a private right of action and covers biometric data.[40]
- **National Biometric Information Privacy Act of 2020-** This law mandates that any private organization that gets a person's biometric identification or biometric data take specific steps to maintain and ensure[41]
- **Biometric Information Privacy Act (BIPA)-** This Illinois statute gives people a private right of action and safeguards the privacy of biometric data.[42]
- **Other states-** Texas and Washington own biometric privacy laws have been passed, but they don't offer a private right of action. Instead, the attorney general normally handles enforcement.[43]

INDIA

- **Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011[44]-** This rule outlines the exact guidelines that govern personal information, sensitive personal data, and biometric information.
- **The Aadhar Act, 2016-** This act regulates the collection, storage, and use of biometric data for the Aadhaar program.[45]

[39] Biometric data and privacy laws 9GDPR, CCPA/ CPRA), *Thales Group,* (July. 01, 2023, 9:29 PM), https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data
[40] Fredric D. Bellamy, 'Looking to the future of biometric data privacy laws', (*Reuters,* 6 April 2022), (July. 01, 2023, 9:29 PM), https://www.reuters.com/legal/legalindustry/looking-future-biometric-data-privacy-laws-2022-04-06/
[41] National Biometric Information Privacy Act of 2020, *Congress. Gov*, https://www.congress.gov/bill/116th-congress/senate-bill/4400 , (last visited July. 6, 2023).
[42] *Bloomberg Law*, https://pro.bloomberglaw.com/brief/biometric-data-privacy-laws/ , (last visited July. 6, 2023).
[43] Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, 'The Anatomy of biometric laws: what U.S companies need to know in 2020', (*The National Law Review,* 15 January 2020), , (July. 01, 2023, 9:29 PM), https://www.natlawreview.com/article/anatomy-biometric-laws-what-us-companies-need-to-know-2020
[44] Arjun Uppal, 'India: Biometric data: Regime in India', *mondaq*, July. 01, 2023, 9:29 PM), https://www.mondaq.com/india/privacy-protection/857992/biometric-data-regime-in-india
[45] Arjun Uppal, 'India: Biometric data: Regime in India', *mondaq*, (July. 01, 2023, 9:29 PM), https://www.mondaq.com/india/privacy-protection/857992/biometric-data-regime-in-india

- **The Indian Evidence Act, 2005-** This law establishes the admissibility of electronic evidence, including biometric information, in court cases.[46]
- **Personal Data Protection Bill, 2019-** In its current version, the proposed DPDP Bill imposes sanctions for failure to uphold its duties. Depending on the type of non-compliance, the penalty under the DPDP Bill ranges from INR 10,000 (about USD 120.71) to INR 250 Crores (Indian Rupees Two Hundred Fifty Crores) (around USD 30,177,175). Whether individuals have private remedies.[47]
- **Information Technology Act, 2000-** According to Section 43A of the IT Act, a data collector may be required to pay a data subject who has been harmed as a result of their failure to implement reasonable security practices and procedures for the protection of sensitive personal data and personal information. Additionally, the Directions have included a penalty for failing to give information to CERT of a term of imprisonment extendable to 1 year or a fine up to about INR 100,000 (approximately USD 1207.09 as of 29 December 2022), or both.-Compliance with or disregard for the Directions.[48]

Seeking legal recourse

1. To examine their legal alternatives, people can get in touch with an attorney who focuses on data privacy and security. An attorney can offer advice on the best course of action and assist in determining if a claim has a legal basis.[49]
2. People can notify the proper agencies, such as the Federal Trade Commission (FTC) or the state attorney general's office, about the breach. The organisation can be held accountable and further breaches can be avoided by reporting the breach.[50]

[46] The Indian Evidence Act, 2005
[47] Penalties for non-compliance, *Baker Mckenxie*, https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/india/topics/penalties-for-non-compliance , (last visited July. 6, 2023).
[48] Penalties for non-compliance, *Baker Mckenxie*, (July. 01, 2023, 9:29 PM), https://resourcehub.bakermckenzie.com/en/resources/data-privacy-security/asia-pacific/india/topics/penalties-for-non-compliance
[49] Fredric D. Bellamy, 'Looking to the future of biometric data privacy laws', (*Reuters*, 6 April 2022), (July. 01, 2023, 9:29 PM), https://www.reuters.com/legal/legalindustry/looking-future-biometric-data-privacy-laws-2022-04-06/
[50] Jessica Groopman, 'In biometrics, security concerns span technical, legal and ethical', (*TechTarget*, June 2020), (July. 01, 2023, 9:29 PM), https://www.techtarget.com/searchsecurity/tip/In-biometrics-security-concerns-span-technical-legal-and-ethical

3. A class action lawsuit against the entity in charge of the breach may include individuals. Individuals may be able to seek loss reimbursement through class action lawsuits rather than bringing individual claims.[51]
4. A business that perpetrated the breach may be subject to legal action from individuals. This may entail submitting a complaint to a regulatory body—like the FTC or state attorney general's office—and asking for an investigation.[52]

Benefits of biometric technologies

A high level of security and confidence is offered by biometric technology for establishing identity. Unauthorized individuals have a harder time gaining access thanks to biometric verification, which is based on distinctive biological or behavioral traits that are difficult to imitate[53]. Convenient and quick authentication processes are provided by biometric technologies. Users no longer need to keep track of and manage numerous passwords or tokens because they can quickly and simply authenticate using their biometric characteristics. Biometric traits are challenging to fake or steal, making them more resistant to spoofing attacks. Biometric systems often incorporate anti-spoofing measures to detect and prevent fraudulent attempts.[54] Each person has a unique set of biometric characteristics that are difficult to communicate or transfer. As a result, biometric authentication is more secure than conventional procedures that rely on passwords or tokens, which can be lost, stolen, or used by several people.[55]

Lawsuits

1. Rosenbach v. Six Flags- The Illinois Supreme Court declared in 2019 that customers can bring legal claims against businesses for BIPA violations even if they haven't been

[51] Clare O'Gara, 'What are the consequences of a biometric data breach?' (*Secureworld*, 15 August 2019), (July. 01, 2023, 9:29 PM), https://www.secureworld.io/industry-news/biometric-data-breach-consequences
[52] Biometrics Invasion of Privacy, *The Lyon Firm*, https://www.thelyonfirm.com/class-action/data-privacy/biometrics/ , (last visited July. 6, 2023).
[53] Biometrics and Privacy-issues and challenges, (*OVIC*) https://ovic.vic.gov.au/privacy/resources-for-organisations/biometrics-and-privacy-issues-and-challenges/, (last visited July. 6, 2023).
[54] Advantages and disadvantages of biometrics, https://www.miteksystems.com/blog/advantages-and-disadvantages-of-biometrics , (last visited July. 6, 2023).
[55] Russ Ryan, Emerging Biometric Technologies, securityinfowatch, (July. 01, 2023, 9:29 PM), https://www.securityinfowatch.com/access-identity/access-control/article/10517342/emerging-biometric-technologies

harmed. This decision has made it possible for additional data breach class lawsuits including biometric information.[56]

2. Patel v. Facebook- A class-action lawsuit claiming that Facebook had collected and stored users' biometric data without their consent in violation of Illinois' Biometric Information Privacy Act (BIPA) was settled in 2020 with a $650 million payment from Facebook.[57]

CONCLUSION:

As a result, there are no specific laws for biometric technology. There are many benefits as well as drawbacks of biometric technology because it contains personal data of individuals which is at risk if the data get stolen because of lack of security methods. Different nations, including India, have passed several laws and rules to safeguard people's privacy and data from biometric data breaches. Serious penalties, such as civil penalties and damages, can be imposed for breaking these laws. Under the legislation of the IT Act biometric technology is safeguarded. The personal data bill, 2019 in India protects privacy but it also needs some updations. There are still loopholes in the IT Act under which biometric data will suffer threats.

[56] bradley, https://www.bradley.com/insights/publications/2018/05/the-evolution-of-us-biometric-privacy-law, (last visited July. 6, 2023).

[57] Kyle D. Black, CIPP/E, CIPP/US, CIPM, Biometric Privacy Laws Create New Avenue for Data Breach Class Actions, bipc, (July. 01, 2023, 9:29 PM), https://www.bipc.com/biometric-privacy-laws-create-new-avenue-for-data-breach-class-actions