© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716234

Biometric Identity, Fiber-Based Data Infrastructures, And the Future of Data Sovereignty: Legal and Infrastructural Implications of Decentralized Digital Id Systems in the United States and Emerging Economies

OLUWATAYO OSODEIN[1], AROME ADAMA[2], OLUWATIMILEYIN OSODEIN[3], AYOMIDE AROWOLO-AYODEJI[4], CLETUS O. OLADIMEJI[5], TEMITOPE OWOEYE[6]

[1]*Legal, Wiseplus Limited*
[2]*Faculty of Law, Kogi State University*
[3]*Cyber Security, Wiseplus Limited*
[4]*Know the Blocks*
[5]*Cyber Security, Olabisi Onabanjo University*
[6]*School of Law, Kogi State University*

I. INTRODUCTION

Today there is no doubt as to the importance of data. It is the bedrock of technology today. It is the means through which identity is established aside from being the source of information. It is used to assert control and sovereignty over personal data. The evolution of technology has created a convergence of three critical elements which are biometric identity verification fibre-based data infrastructures and data sovereignty. The convergence of these three elements has resulted in the creation of powerful tools for governance by both the state and private sector. It is the focus of this essay. As decentralized ID systems are emerging, as a deviation from centralized systems, they create a platform or infrastructure through which decentralized data identity (DDID) systems are built. These infrastructures ensure high speed and secure data exchange as well as a compatible legal and regulatory framework that can navigate complex issues concerning privacy consent cross-border data flows as well as ensuing liabilities. Nonetheless even where these exist serious issues on the legal ownership, governance and sovereignty over data which form part of or establish digital identity arise.

Even us decentralized systems evolve, the legal and infrastructural implications of this emergence diverge from jurisdiction to jurisdiction and are defined by differences in regulatory, and infrastructural capacity as well as the approach of the state to digital governance. In the light of this essay examines the legal and infrastructural implications of decentralized identity systems in the United States and in emerging economies. As a corollary, this essay will consider several key aspects of the topic as it builds towards achieving the aim of the essay. These include biometric identity and DDID systems, Fiber-infrastructure and its implications in the U.S. and emerging economies, the Legal implication of decentralizes systems in the U.S. and emerging economies and the future of data sovereignty.

II. BIOMETRIC IDENTITY AND DECENTRALIZED DIGITAL ID (DDID) SYSTEMS

Biometric identity simply refers to the immutable physical traits such as fingerprints and facial features that are unique to an individual and can be used to identify such an individual.[1] Biometric identity systems use these features for authentication purposes[2] It offers a unique means of authentication which has several advantages when compared to traditional credentials such as passwords or physical cards[3] According to the research by Grand View Research, the biometrics ecosystem is projected to reach approximately $150.58 billion by 2030, its broad adoption and applications in technology and

many aspects of human endeavor. Biometric systems offer significant advantages and address critical vulnerabilities associated with passwords or physical cards.[4] For instance, they cannot be forgotten easily like passwords nor can they be covertly shared like tokens.[5] In fact, when integrated into digital identity systems they tend to be frictionless and secure across applications whether in banking, health care, business etc.

Identity data can be stored and managed either in a centralized system or in a decentralized system. A centralized identity system relies on a single or central authority, such as a private organization, to store and manage identity data and as such is prone to vulnerabilities such as single points of failure and large-scale breaches.[6] They raise concerns about user privacy. Decentralized ID systems on the other hand are built on a decentralized ledger system such as block chains or cryptographic protocols.[7] They are designed to transfer control from a central authority such as a government or corporation to the individual. In this system, the user or individual holds controls and manages their identity credentials which includes biometric data within a personal wallet.[7] The user only presents verifiable proof to third parties without any other intermediary accessing or storing the raw biometric data.[8] The goal here is to attain a self-sovereign identity where the issuance storage and verification of data is decoupled from a central identity and reserved for the user or owner of the data.[9] This enhances privacy and security by minimizing data exposure eliminating honeypots of centralized biometric databases and facilitating user autonomy.

Despite its many advantages embedding biometric data within decentralized identity systems faces several operational challenges emanating from failure to enrol rates, security paradox and operational challenges.

One such challenge emanates from failure-to-enroll (FTE). This refers to a situation where an individual is unable to enrol into a biometric system for the purpose of identification as a result of an insufficient and distinct biometric sample, absence of the required parts of the body that is needed for obtaining the necessary biometric sample, or design in the system making it challenging for an individual to provide a consistent biometric credential etc.[11] This affects manual labourers disproportionately due to the fact that they have worn out fingerprints or fading iris patterns and those with disabilities. A good example of this is the Aadhaar system in India which utilizes a central ID system where each citizen is given a 12-digit ID number issued by the Unique Identification Authority of India (UIDAI).[10] According to Drèze et al., over 1.5 million indigent persons were denied welfare benefits because of biometric authentication failures.[11] In a decentralized identification system, the individual bears responsibility for managing their biometric information or credentials, thus failure to enrol can result in a complete digital exclusion of the individual without recourse to a central authority. [12]
A second issue is what is referred to as the security privacy paradox. The paradox is that while decentralization minimizes the risk of mass breaches that often occur in centralized biometric databases it creates a new attack vector.[13] Due to the fact that biometrics are irrevocable, once they are compromised, they cannot be reset like passwords.[14] Hence, storing these in a decentralized system, means that the burden of security is shifted to the individual who more often than not stores them in a smartphone which is vulnerable. In addition, given that decentralized systems rely on blockchain technology, which is an immutable ledger and is auditable, the individual may become legally liable if his biometric data is breached and utilized for fraudulent purposes which ends up being recorded in the ledger against him.

An operational challenge associated with decentralization occurs when there is a loss of cryptographic keys through which an individual accesses is DDID.[15] Here, the point of creation, storage, and recovery of cryptographic keys becomes a point of vulnerability. Where the keys are lost or forgotten, digital identity may be lost.[16] Recovery may involve the use of some trusted intermediary or complex social recovery protocols which in turn undermines the idea of ‘decentralization’ or ‘self-sovereign’. This also creates another point of failure or coercion. Further, there is the possibility of interoperability as the DDID ecosystem may vary

from place to place particularly between advanced and emerging economies.[17]

III. FIBER INFRASTRUCTURE

As earlier mentioned, centralized digital identity systems offer instant secure and user-controlled verification across borders. However, this is made possible or is contingent on a physical layer of data transmission. This layer is the fiber infrastructure which consists of fiber optic networks with high bandwidth and low latency rates. Compared to other network infrastructures such as wireless it offers extreme speeds of data transfer in huge volumes with even stronger signal integrity over long distances. These features make it an indispensable aspect of decentralized digital identity systems and their cryptographic protocols and real-time biometric authentication. However, there is an uneven distribution of fiber infrastructure globally which creates a huge gap in infrastructural sovereignty which in turn affects the feasibility and security of deploying decentralized identity systems both in the United States and in emerging economies.

Fibre infrastructure is critical for the deployment of DDID for various reasons. First, is that DDID Operations require significant computational resources while also generating significant traffic which consequently results to latency issues and cryptographic overheads. These operations include zero-knowledge proof generation or verification, blockchain consensus mechanisms for credential status checks as well as secure biometric template matching. Wireless networks such as 4G and 5D tend to have higher delays or latency situated around 30-100 milliseconds as opposed to 10 milliseconds provided by fiber optic internet. Given this, biometric authentication through facial recognition across a congested network may experience delays of around 200 milliseconds consequently increasing failure rates by 15 to 22% compared to fiber which delivered a sub-50ms performance which is needed at least for user acceptance. Latency and inconsistency of network quality can result in challenges in the cause of authentication which may take the form of timeouts which may also disrupt users' experience and impede the stimulus delivery of digital services. Another reason is that fibre is more secure as it is harder to tap into undetected compared to others like wireless. This is vital for sensitive ID data as it protects the data in transit from the user's device, verifiers and decentralized ledgers.

a. Infrastructural Implications in the U.S and Emerging Economies

In the United States, there are severe disparities with Respect to the distribution of fibre infrastructure which is necessary for decentralized digital identity systems. For instance, in 2023 it was reported that 92.11% of people living in urban areas had access to high-speed broadband reaching up to 100/mbs download and 20/mbs upload which was largely attained through fiber infrastructure playing a significant role. However, only 77% of rural residents have access to similar quality of service now. The implications of these are twofold. The first one is that it creates a digital divide between the urban areas and the rural areas which is significant. The second implication is that fibre is more reliable and faster compared to mobile and satellite networks therefore limited access to this results in exclusion and limited opportunities for education work healthcare and others. This is then translated directly into DDID the exclusion. It therefore means that states that have large rural populations and are lacking in fiber infrastructure will be unable to access or carry out DDID operations as they will be forced to rely on satellite or other networks.

For many emerging economies, fibre coverage tends to be generally low. In such economies, major cities tend to have fibre infrastructure at least to an extent but in terms of the national penetration of fibre, it is low. For instance, it is usually below 20%. According to the International Telecommunication Union (ITU), only about 35% of the population in the least developed countries can access the Internet let alone fibre-quality broadband. The implication of these for DDI D deployment in such economies will be greatly deficient. DDID systems require a high internet capability that Fiber delivers. Where fibre has been deployed its importance has been felt. For instance, in Rwanda where the KTRN (Kigali Terrestrial Network) has attained about 95% national coverage to administrative sectors, It enabled the roll of the Irembo digital series platform in 2015 which includes key ID and biometric-linked services.

Beyond access ownership of fiber infrastructure and its routing affects data sovereignty which is one of the central aims of DDID. The physical path traveled by fiber cables is significant and determining jurisdiction and control over data. First, on the issue of routing as data travels through fiber optics it is subject to the legal regime of the country where such cables traverse. Consequently, a biometric verification request from Kenya to a decentralized identifier anchored on a blockchain load in Germany may travel through cables that pass through Egypt or Portugal. This then exposes the metadata or content in a situation where, for instance, encryption is compromised, to the surveillance laws of several jurisdictions. This negates the aspiration of DDID systems which is 'user-controlled' data flows and self-sovereignty.

In addition, the ownership of such infrastructure affects data sovereignty. In developed countries and even emerging economies, fibre backbones tend to be built and operated by foreign private companies. Although this makes deployment faster, it creates dependencies and points of leverage for instance, in cases of dispute over licensing fees or geopolitical pressures. This could affect access and quality of service, thus undermining the DDID systems of such nations that are reliant on the infrastructure.

IV. LEGAL IMPLICATIONS OF DECENTRALIZED ID

Systems in the U.S and Emerging Economies

Deploying DDID systems faces a number of conflicts which include a fragmented legal framework, changing regulatory practices and uncertainty in terms of jurisdiction. Although DDID promises sovereignty to the user and borderless verifications, the legal reality of this is a maze of conflicting obligations that may negatively impact innovation undermine security and lead to a significant compliance burden. This situation is more obvious in the US which has a system where laws diverge according to sectors and state. In emerging economies, this takes the form of GDPR-based frameworks. Neither of these addresses the unique challenges of decentralization.

a. Legal Implications in the U.S

The legal implication of biometric data, fibre infrastructure, and data sovereignty on DDID is simple yet complex. For starters, the laws on digital Identity or Biometric data are fragmented. Each state has its laws with varying degrees of differences as will be discussed below. Secondly, there different laws regulating digital identity or biometric data in different sectors. None of these laws at any level or sector makes provisions for DDID. This will become a significant problem that will have an impact on the future of DDID in the U.S.

In the United States, there is no unified federal legislation that governs digital identity or biometric data. The legal terrain is made up of divergent state laws. One of the most common is the Illinois Biometric Information Privacy Act (BIPA) which was enacted in 2008 and is often considered to be one of the strictest.

BIPA, in s.14/15(b) and (c), makes provision requiring explicit and written consent of the data subject or individual before the collection or storage of biometric data and also prohibits entities from selling leasing or profiting from an individual's biometric data. Paragraph (d) of the same section also prevents the disclosure of an individual's biometric information without their consent unless it is required by law. The standard of care required from data controllers in the storage and handling of biometric data is a 'reasonable standard of care'. An important provision is the 'private right of action' in s.14/20 which allows an individual whose data has been violated to sue for statutory damage even in the absence of actual damage with penalties for violations. This was affirmed by the Illinois Supreme Court in Rosenbach v. Six Flags Entertainment Corp., that where there is such a violation, it is sufficient in itself without the need to provide evidence of actual harm under the private right of action. This decision opened the door for a flurry of litigation with respect to BIPA. In Tims v. Black Horse Carriers, Inc., the limitation period of 5 years was extended to all BIPA claims and liability. Also, in Cothron v. White Castle System, Inc., it was held that every scan or transmission of an individual biometric data counts as a distinct and separation violation which multiplies the statutory damages. Penalties for statutory damages are pegged at $1000

per violation, and $5,000 for any intentional or reckless violations.

These strict provisions and application of BIPA meant that cases and penalties were going to be significant, with many of the cases targeted at facial recognition technologies and biometric timekeeping systems. This in turn led to significant financial exposures for organizations. An example is re Facebook Biometric Information Privacy Litigation, where Meta (Facebook) was found guilty of using it photo-tagging feature which is a facial recognition technology to collect and store the data of individuals without their informed consent and had to settle by paying $650 million. In another case involving Google, Rivera v. Google Inc., $100million was paid by Google for similar violations but for its Google photo services which collected and stored facial recognition data without informed consent. This has made BIPA a reference point for national regulation particularly as emerging technologies continue to rely on biometric authentication systems.

Comparatively, the Texas Business & Commerce Code (Tex. Bus. & Com. Code) and the Washington Revised Code (Wash. Rev. Code) are both narrow in scope and enforcement. The Tex. Bus. & Com. Code in S. 503.001 and Wash. Rev. Code in S. 19.375.020 both require notice and consent for biometric data collection and prohibit commercial sales. However, they do not provide for a private right of action. Thus, enforcement rests solely within the discretion of the Attorney General under s.503.001(f) of the Texas law and s.19.375.030 of the Washington Rev. Code. the implication of this is reduced deterrence and minimal litigation against companies in those jurisdictions.

The overall landscape remains fragmented with as much as about 35 States having introduced biometric privacy laws, many of which are modelled after the BIPA but excluding the right to private action which is integral for accountability. At the federal level, there are moves towards regulating biometric data with the proposal of the American Data Privacy and Protection Act (ADPPA) which has failed to go beyond the committee stages.

Aside from the patchwork of biometric identity laws, another legal implication stems from the existence of sectoral differences or limitations in the U.S. legal terrain. There is no cross-sector-specific law that regulates digital identity or biometric data both at the federal and state levels. The laws are fragmented by sector even if they deal with digital identity or biometric data. For instance, the law that regulates health-related data, at the federal level, falls under the Health Insurance Portability and Accountability Act (HIPPA), 2008 which covers only healthcare providers, insurers and their business associates. Under 45 CFR §§ 160 and 164, HIPPA regulates the use of ‘protected health information' which includes biometric identifiers such as fingerprints but applies only in health care settings. This means that other areas where biometric data are collected are outside the scope of HIPPA. Another example is the Gramm-Leach-Bliley Act (GLBA) which applies to regulate how financial institutions handle an individual’s biometric data described as ‘nonpublic personal information’. However, it seems to apply only to traditional financial institutions.

DDID systems deviate from centralized ID systems traditionally used today. Within the U.S, the legal framework on DDID is yet to be developed and as such there is a lacuna. There is a lack of a federal statute that addresses DDID, leading to uncertainty at every level of its adoption and implementation. The U.S. laws quite notably, do not provide a clear allocation of responsibility in the DDID environment. In centralized frameworks such as the GDPR and sector-specific laws like HIPPA and GLBA are based on the presence of an identifiable ‘data controller’ and ‘data processor’. These are individuals or entities that are subject to duties and obligations which can be enforced against them. They are saddled with the responsibility of obtaining informed consent, notifying regulators where there is a breach and protecting the integrity of data. DDID systems are self-sovereign and self-manages as the data subject retains ID credentials locally in a digital wallet and verifications or authentication takes place in a peer-to-peer structure with zero-knowledge proofs (ZKPs). There is no central entity to be held legally accountable as current laws provide where there is a breach. This raises the fundamental question of 'who is the controller' in this context.

This lacuna also extends to the requirement for consent under the law. Current laws require that the data controller must obtain and, a data subject must give a clear and informed consent before their personal data including biometric data can be obtained and used by the controller. This outplay, in a centralized system, takes the form of ticking a box or agreeing to a privacy policy. In a DDID system, this scenario will be different because the system does not rely on such clickwrap agreements or written disclosures because no central authority or data controller is seeking such consent. Rather, authentication is done through cryptographic methods such as by ZKPs or a digital challenge which allows the data subject to prove its identity without using its biometric data. The issue is that this may satisfy the technical requirement in a DDID system but it does not meet the requirement of informed consent under data privacy or biometric laws like BIPA. In this case, does cryptographic proof or digital challenge meet the standard of consent legally? Existing laws do not make any provision regarding this.

Another situation where the current legal framework is inadequate is with regard to the requirement for notification when there is a data breach of personal data. This obligation rests on the data controller and is in favor of the data subject. This applies in a centralized ID system but this may be inadequate or does not properly address a similar scenario in a decentralized ID system. In a DDID system, data is fragmented across verifiers, issuers and user-controlled storage or digital wallet. This structure is devoid of a single point of failure. In a situation where a verifier's system is compromised but no complete biometric profile or credential is breached, does this amount to a 'breach' under data protection/privacy laws? If it does who is obligated to notify whom, given that no single party controls all the data? This creates a lack of clarity regarding who is legally responsible and what qualifies as a breach requiring notification.

This lack of clarity and certainty has a direct impact on investments and innovations in many sectors. Tech companies are hesitant to invest or build new systems for fear of inadvertently violating laws and the ensuing legal actions from that especially when it comes to dealing with sensitive data like biometrics. The absence of clarity means that the U.S. is not yet well adapted to govern the legal and infrastructure complexities of DDID. This not only limits domestic adoption of DDID systems but also its ability to shape the global norms on the subject.

b. Legal implication for emerging economies.

Emerging economies are enacting data protection laws which are based on and similar to the EU GDPR. Emerging economies are not yet fully engrossed in the centralized systems and as such still have room to be flexible enough to adapt and design modern digital frameworks including DDID systems. Nations like Kenya, South Africa, Brazil and even India have either passed or are in the process of finalizing their laws that are heavily reliant on the GDPR. A good example is the Kenya Data Protection Act (2019) which provides for limitations on the purpose of data, data minimization and processing. S. 24 of the Act considers biometric data as 'sensitive personal data' and as such requires stronger protections. Also, there is South Africa's Protection of Personal Information Act (POPIA) 2021 which considers biometric data as sensitive information and prohibits the processing of such data with consent unless a legal obligation or public interest warrants it in s.26. India's Digital Personal Data Protection Act (2023) also tows this line.

However, each emerging nation faces unique challenges. The majority of them struggle with weak enforcement, resources, capacity, limited digital literacy among users and poor cybersecurity infrastructure. In the rural or informal economies, where digital ID systems may be reliant on social welfare schemes or mobile access which requires informed consent, or robust protection, it becomes difficult to obtain. Consequently, while the laws appear to be strong on paper, implementation in terms of DDID systems that rely on biometric data will be challenging. The infrastructural support and legal framework are just non-existent. In Kenya, for instance, the Data Protection Commissioner (ODPC) is responsible for enforcing data protection laws but, it has a small staff to deal with thousands of complaints in addition to other limitations to enforcement. Its effort has led to a series of fines against erring organizations. For instance, it fined a school Ksg500,000 for collecting and using student

data without their consent. The situation is almost the same in Brazil. This situation results in some form of compliance asymmetry where big multinational companies, especially those used to being regulated by European or U.S regulations, spend significantly on legal teams, and audits and instil audit mechanisms to stay compliant while local businesses and institutions tend to not comply. Given that enforcement remains a patchwork and the penalties are low, the chances of being held accountable are significantly low. Sometimes, such violations go under the radar.

Also, data protection laws in emerging economies provide or lean towards data localization which provides that sensitive personal data including biometric and ID data be stored within national borders. The essence is to assert sovereignty over citizen data, minimize the risk of foreign surveillance and imbue local regulatory authorities with jurisdiction over the use and handling of personal data. An example of this is in the Draft Rules 2025 for the Indian Digital Person Data Protection Act 2023 which in Rule 14 made pursuant to Rule 12, required 'significant Data fiduciaries' to store personal and traffic data exclusively in India. Prior to this, its 2022 Draft Data Governance Policy had already classified biometric and digital ID as 'critical personal data' and as such must be exclusively stored on servers located within India. The implication of this is that companies that manage or use such data regardless of whether they are public or private cannot store such data in overseas databases. Similarly, in Nigeria, Nigeria's Data Protection Regulation (NDPR) via its Implementation Framework 2020, article 8 implied such requirement for retention of data within national jurisdiction. It is not express, however, but signifies a move towards localization.

Despite the aim of localization, they may likely pose a challenge to DDID systems. DDID operates on an almost borderless principle such that identity credentials and authentication may be issued in one country and stored in another in a user-controlled wallet and can also be authenticated in another through a distributed ledger or cloud-based services. Localization also has financial implications for DDID systems. According to PIFS (Program on International Financial Systems), digital service providers will face a 30-60% increase in operational costs to comply with localization law. This in turn becomes a financial hurdle for startups or cross-border platforms that want to build scalable and interoperable DDID systems. This is more so if countries adopt laws that conflict with data localization.

Another legal implication comes from the seeming extraterritoriality of data protection laws which create further jurisdictional complexities particularly given the cross-border nature of DDID systems. An example is S.3 of the GDPR which asserts jurisdiction over entities that offer goods and services to EU data subjects or monitor their behaviour regardless of physical location. This is also the case with many emerging economies' data laws styled after the GDPR. This has implications for DDID systems because they use biometric data for authentication and to interact across borders. An example is where a decentralized authenticator based in one country processes a biometric authentication request from an individual by a European citizen, they would be subject to the provisions of the GDPR. This has implications as it increases the compliance burden and legal risk for emerging economies with global users. For example, fines and penalties can reach up to €20 million or 4% of the turnover of that company depending on which is higher. This could be crippling for startups or local companies in emerging economies. But nonetheless, they are exposed to this in a DDID system.

V. THE FUTURE OF DATA SOVEREIGNTY

DDID systems are still in their nascent stage. As they evolve, they will be shaped by the conflict for control between corporate entities and state authorities. Meta's login feature via Facebook which happens to be used to access e-commerce sites is a good example of how systems can subtly erode user sovereignty and transform Identity into a proprietary commodity. On the other hand, systems controlled by the state can become tools for centralized surveillance because laws require or mandate the use of biometric data across welfare, finance, telecommunications and many other spheres. In the midst of these, DDID systems present themselves as an alternative by

allowing the data subject or user to control their credentials and store their biometric data. However, DDID systems remain constrained by infrastructural, legal and even sociotechnical barriers. A lack of digital literacy may limit the speed of adoption in emerging economies.

Geopolitical tensions will also complicate the landscape largely due to the technological rivalry between the U.S and China which has increasingly dictated the standards for ID systems. While the U.S tends to align with Western regulatory frameworks which lean towards decentralized ID systems, China leans towards integrated ID ecosystems embedded with technologies such as facial recognition with state-influenced protocols. The impact of this on emerging economies is that it forces them into making binary choices as they try to navigate the issue. The future of data sovereignty would require considering autonomy as a negotiated interdependence as opposed to isolation. The risk of collusion between the state and corporate bodies remains tangible.

VI. CONCLUSION

The movement towards DDID systems indicates a major interplay between technology, infrastructure and law. While there is the appeal of a user-controlled identity framework, implementing it most definitely sheds light on issues yet to be resolved in the context of biometric governance, infrastructural disparity and legal framework. Currently, the practice faces the risk both legally and infrastructurally. In both the U.S and emerging economies, the legal environment is not yet adapted to meet the demands of a decentralized system. There still exists a lack of clarity in the laws on data ownership, liability and cross-border governance. These are also challenges that neither the centralized nor decentralized systems can ignore. Unless these are addressed, DDID might end up creating significant hurdles for individuals and companies.

Addressing these issues would require more specific legislation, investments in digital infrastructure, and unwavering commitment towards DDID systems. Comparative experience indicates that it is possible to balance both individual autonomy and institutional accountability but through coordinated efforts from states, developers and other stakeholders in the ecosystem. Stakeholders must come to a perception that decentralization is a domain that requires innovative governance.

VII. BIBLIOGRAPHY

Primary Sources
Statutes

[1] Gramm-Leach-Bliley Act (GLBA)
[2] Implementation Framework for the Nigerian Data Protection Regulation 2020,
[3] Indian Digital Personal Data Protection Act (2023)
[4] Kenyan Data Protection Act (2019)
[5] South African Protection of Personal Information Act (POPIA) 2021
[6] The Illinois Biometric Information Privacy Act (BIPA) 2008
[7] The Nigerian Data Protection Regulation (NDPR) 2019
[8] The Texas Business & Commerce Code (Tex. Bus. & Com. Code)
[9] The U.S Health Insurance Portability and Accountability Act (HIPPA), 2008
[10] The Washington Revised Code (Wash. Rev. Code)

Cases

[11] Cothron v White Castle System, Inc, 2023 IL 128004 (Ill Sup Ct).
[12] In re Facebook Biometric Information Privacy Litigation, No 3:15-cv-03747 (ND Cal, 2020).
[13] Rivera v Google Inc, no 2019-CH-00990 (Cir Ct Cook Cty Ill).
[14] Rosenbach v Six Flags Entertainment Corp, 2019 IL 123186 (Ill Sup Ct).
[15] Tims v Black Horse Carriers, Inc, 2023 IL 127801 (Ill Sup Ct).

SECONDARY SOURCES

[1] Allen Munoriyarwa and Admire Mare, 'Mainstreaming Surveillance Through the Biometrification of Everyday Life' in Digital

Surveillance in Southern Africa: Policies, Politics and Practices (Springer International Publishing, 2023) 141.

[2] Ana I Segovia Domingo and Álvaro Martín Enríquez, 'Digital Identity: the current state of affairs' (2018) 1(0) BBVA Research 1.

[3] Andrea Rinaldi, 'Biometrics' new identity—measuring more physical and biological traits' (2016) 17(1) The EMBO Reports 22.

[4] Asmita Mahale, Madhavi Damle, Abhijit Chirputkar, Prasanna Kulkarni, and Trupti Bhosale 'Data Protection Regulation by Personal Data Protection Bill in India: Bearing on Business India' (2023) 11(3) Russian Law Journal 2840.

[5] Aviral Goel and Yogachandran Rahulamathavan, 'A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility' (2024) 17(1) Future Internet 1.

[6] Brooke Norton, 'Navigating the Legal Framework: Implementing a Government-Backed Digital Identity in the United States' (2024) 64(2) Jurimetrics: The Journal of Law, Science & Technology.

[7] C Palmer, 'How Fast Should Your Internet Be? The FCC Now Says 100Mbps' HighSpeedInternet.com (14 March 2024) https://www.highspeedinternet.com/resources/fcc-updates-speed-standards-100mbps#:~:text=According%20to%20the%20latest%20broadband%20map%20published,access%20to%20fixed%20broadband%20speeds%20of%2025/3 accessed 1 June 2025.

[8] Christopher Allen, The Path to Self-Sovereign Identity (Life with Alacrity, 2016).

[9] Christopher Kuner, 'Data and Extraterritoriality' in Research Handbook on Extraterritoriality in International Law (Edward Elgar Publishing, 2023) 356.

[10] Daniel Hodapp and André Hanelt, 'Interoperability in the era of digital innovation: An information systems research agenda' (2022) 37(4) Journal of Information Technology 407.

[11] Daria Schumm, Katharina OE Müller and Burkhard Stiller, 'Are We There Yet? A Study of Decentralized Identity Applications' (2025) arXiv preprint arXiv:2503.15964.

[12] Daria Sukhova, 'E-Government Development in Rwanda' (HSE University, 2022) https://we.hse.ru/en/irs/cas/passrw accessed 17 May 2025.

[13] Deepak Garg and Abhimanyu Nain, 'Next generation optical wireless communication: a comprehensive review' (2023) 44(s1) Journal of Optical Communications s1535.

[14] Drummond Reed and Markus Sabadello, 'Decentralized identifiers' in Alex Preukschat and Drummond Reed (eds), Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials (Shelter Island, NY, 2021) 157.

[15] Edward J Oughton, William Lehr, Konstantinos Katsaros, Ioannis Selinis, Dean Bubley, and Julius Kusuma, 'Revisiting wireless internet connectivity: 5G vs Wi-Fi 6' (2021) 45(5) Telecommunications Policy 102127.

[16] Emily Stackhouse Taetzsch, 'Privacy Purgatory: Why the United States Needs a Comprehensive Federal Data Privacy Law' (2024) 50 Journal of Legislation 121

[17] Eric Udd, Fiber Optic Smart Structures in Fiber Optic Sensors: An Introduction for Engineers and Scientists (2011) 373.

[18] F Onu and SC Ikporo, 'Comparative study of optic fibre and wireless technologies in internet connectivity' (2016) 5 International Journal of Computer Applications Technology and Research 403.

[19] Florentin Blanc and Giuseppa Ottimofiore, 'Regulatory Compliance in a Global Perspective: Developing Countries, Emerging Markets and the Role of International Development Institutions' in The Cambridge Handbook of Compliance (Cambridge University Press, 2021) 158.

[20] Gaurav Malik, 'Biometric Authentication—Risks and advancements in biometric security systems' (2024) 6(3) Journal of Computer Science and Technology Studies 159.

[21] Geoff Goodell and Tomaso Aste, 'A Decentralized Digital Identity Architecture' (2019) 2 Frontiers in Blockchain 17.

[22] Grand View Research, Biometric Technology Market Size & Share Report, 2030 (Grand View Research, 2023) https://www.grandviewresearch.com/industry-analysis/biometrics-industry#:~:text=The%20global%20biometric%20technology%20market,20.4%25%20from%202023%20to%202030 accessed 8 June 2025.

[23] Hasan Syed, 'Power to The People: How Blockchain Based Digital Identity Can Empower Disadvantaged Individuals' (2019).

[24] Heylyung Yun, 'China's Data Sovereignty and Security: Implications for Global Digital Borders and Governance' (2025) 10(2) Chinese Political Science Review 178.

[25] International Telecommunication Union, Measuring the Information Society Report Volume 2. ICT Country Profiles (2017) https://www.itu.int/en/ITU-D/LDCs/Documents/2017/Country%20Profiles/Country%20Profile_Rwanda.pdf.

[26] International Telecommunication Union, 'Press Release' (ITU, 2024) https://www.itu.int/en/mediacentre/Pages/PR-2024-11-27-facts-and-figures.aspx accessed 7 June 2025.

[27] Isaac Juma and Bukola Faturoti, 'Enforcing Data Privacy in Kenya and Nigeria: Towards an African Approach to Regulatory Practice' (2025) International Review of Law, Computers & Technology 1.

[28] Jayaprada Putrevu and Charilaos Mertzanis, 'The Adoption of Digital Payments in Emerging Economies: Challenges and Policy Responses' (2024) 26(5) Digital Policy, Regulation and Governance 476.

[29] Jean Drèze Nazar Khalid, Reetika Khera, and Anmol Somanchi, 'Aadhaar and food security in Jharkhand: Pain without gain?' (2017) Economic and Political Weekly 50.

[30] Juha Saunavaara and Mirva Salminen, 'Geography of the global submarine fiber-optic cable network: The case for Arctic Ocean solutions' (2023) 113(1) Geographical Review 1.

[31] Kamran Siddique, Zahid Akhtar and Yangwoo Kim, 'Biometrics vs passwords: a modern version of the tortoise and the hare' (2017) 2017(1) Computer Fraud & Security 13.

[32] Kenya Times, 'Kenyan School Ordered to Pay Ksh500K Compensation for Sharing Child's Data' The Kenya Times (3 May 2025) https://thekenyatimes.com/latest-kenya-times-news/school-to-pay-ksh500k-compensation-for-sharing-childs-data/ accessed 11 June 2025.

[33] Louise Thomas, Iqbal Gondal, Taiwo Oseni, and Selena Sally Firmin, 'A Framework for Data Privacy and Security Accountability in Data Breach Communications' (2022) 116 Computers & Security 102657.

[34] Marco Bassini, 'Data Controller: A Shifting Paradigm in the Digital Age' (2019) 13 Bocconi Legal Papers 103.

[35] Maria De Marsico, 'Biometric Recognition Errors' in Encyclopedia of Cryptography, Security and Privacy (Springer, 2025) 209.

[36] Md Nazrul Islam Khan, 'Cross-Border Data Privacy and Legal Support: A Systematic Review of International Compliance Standards and Cyber Law Practices' (2025).

[37] Md Rayhan Ahmed, AKM Muzahidul Islam, Swakkhar Shatabda, and Salekul Islam, 'Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey' (2022) 10 IEEE Access 113436.

[38] Megan E Curtis, Sarah E. Clingan, Huiying Guo, Yuhui Zhu, Larissa J. Mooney, and Yih-Ing Hser, 'Disparities in digital access among American rural and urban households and implications for telemedicine-based services' (2022) 38(3) The Journal of Rural Health 512.

[39] Min Ye, 'Security in Context (SiC): A Novel Theoretical and Empirical Approach to the US–China Rivalry' (2025) 83(1) Review of Social Economy 79

[40] Nicolo Bird and Emine Hanedar, Expanding and Improving Social Safety Nets Through Digitalization: Conceptual Framework and Review of Country Experiences (International Monetary Fund, 2023).

[41] Nitin Naik and Paul Jenkins, 'Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology' in 2021 IEEE International Symposium on Systems Engineering (ISSE) (IEEE, 2021) 1.

[42] Omar Dib and Baha Rababah, 'Decentralized identity systems: Architecture, challenges, solutions and future directions' (2020) 4(5) Annals of Emerging Technologies in Computing (AETiC) 19.

[43] Pramod Varma, Rahul Matthan, Rudra Chaudhuri, and C. V. Madhukar, The Future of Digital Public Infrastructure: A Thesis for Rapid Global Adoption (Carnegie Endowment for International Peace, 2024).

[44] Pratyush Ranjan Tiwari, Dhruv Agarwal, Prakhar Jain, Swagam Dasgupta, Preetha Datta, Vineet Reddy, and Debayan Gupta., 'India's "Aadhaar" Biometric ID: Structure, Security, and Vulnerabilities' in International Conference on Financial Cryptography and Data Security (Springer International Publishing, 2022) 672.

[45] Program on International Financial Systems, Data Localization, Cloud Adoption, and the Financial Sector (2024) https://www.pifsinternational.org/wp-content/uploads/2024/07/Report-on-Data-Localization-07.29.2024.pdf.

[46] Rebecca Ong, 'Mandatory Data Breach Notification: Its Role in Protecting Personal Data' (2023) 10 Journal of International and Comparative Law 87.

[47] Sandeep Dommari and Rupesh Kumar Mishra, 'The Role of Biometric Authentication in Securing Personal and Corporate Digital Identities' (2024) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5259335 accessed 26 June 2025.

[48] Supreet Kaur et al., 'Recent trends in wireless and optical fiber communication' (2022) 3(1) Global Transitions Proceedings 343.

[49] Swimpy Pahuja and Navdeep Goel, 'Multimodal biometric authentication: A review' (2024) 37(4) AI Communications 525.

[50] Tajinder Kumar, Shashi Bhushan, Pooja Sharma, and Vishal Garg, 'Examining the vulnerabilities of biometric systems: Privacy and security perspectives' in Leveraging Computer Vision to Biometric Applications (Chapman and Hall/CRC, 2024) 34.

[51] TT Tram Ngo, T. Anh Dang, V. Vuong Huynh, and T. Cong Le, 'A systematic literature mapping on using blockchain technology in identity management' (2023) 11 IEEE Access 26004.

[52] Víctor Rodríguez-Doncel, 'Web Technologies for Decentralised Identity' in Governance and Control of Data and Digital Economy in the European Single Market (2025) 111.

[53] Wie Liang Sim, Hui Na Chua and Mohammad Tahir, 'Blockchain for Identity Management: The Implications to Personal Data Protection' in 2019 IEEE Conference on Application, Information and Network Security (AINS) (IEEE, 2019) 30.