Gulf Journal of Advance Business Research
ISSN 3078-5294 (Online), ISSN 3078-5286 (Print)
FE Gulf Publishers
https://fegulf.com

Cross-Jurisdictional data privacy compliance in the U.S.: developing a new model for managing AI data across state and federal laws

Grace Annie Chintoh[1], Osinachi Deborah Segun-Falade[2], Chinekwu Somtochukwu Odionu[3], & Amazing Hope Ekeh[4]

[1]Gulfstream Aerospace Corporation, USA
[2]TD Bank, Toronto, Canada
[3]Independent Researcher, Texas, USA
[4]Cubed Partners LLC, Oregon, USA

Corresponding Author: Grace Annie Chintoh
Corresponding Author Email: gchintoh6@gmail.com

Article Info

Volume No: 3 **Issue No:** 2 **Page No:** 537-548

Received: 15-10-24 **Accepted:** 21-12-24 **Published:** 09-02-25

DOI: 10.51594/gjabr.v3i2.96
DOI URL: https://doi.org/10.51594/gjabr.v3i2.96

Abstract

The fragmented landscape of data privacy laws in the United States poses significant challenges for organizations utilizing artificial intelligence (AI) systems that process sensitive and large-scale data. Variations in state laws and the absence of a comprehensive federal framework exacerbate compliance complexities, limiting AI innovation and creating legal uncertainties. This paper proposes a conceptual model to harmonize privacy compliance across U.S. jurisdictions, integrating key interoperability principles, consistency, transparency, and scalability. The framework emphasizes standardized practices for data classification, consent management, risk assessment, and enforcement mechanisms supported by technological enablers such as privacy-enhancing technologies and AI compliance tools. Through case studies in healthcare, e-commerce, and finance, the paper demonstrates the framework's practical application and effectiveness in resolving multi-jurisdictional compliance challenges. Actionable recommendations for policymakers, organizations, and AI developers are provided to facilitate implementation alongside future research directions to refine the model and address emerging privacy risks. This study offers a roadmap for navigating the complexities of U.S. privacy laws, promoting trust, accountability, and responsible AI innovation.

Keywords: AI data governance, U.S. privacy laws, Cross-jurisdictional compliance, Privacy-enhancing technologies, Data protection framework, Ethical AI.

INTRODUCTION

Artificial intelligence (AI) has revolutionized industries, transforming how data is collected, analyzed, and utilized. Data privacy has emerged as a critical concern in this digital age, particularly in AI-driven systems that process vast amounts of personal and sensitive information (Settibathini, Kothuru, Vadlamudi, Thammreddi, & Rangineni, 2023). The rapid adoption of AI technologies has amplified the need for robust data governance frameworks that protect individuals' privacy while enabling innovation. However, the U.S. faces significant challenges due to its fragmented legal landscape (Dwivedi et al., 2021).

Unlike jurisdictions like the European Union, which has implemented a comprehensive regulatory framework under the General Data Protection Regulation (GDPR), the U.S. lacks a unified federal law governing data privacy (S. S. Bakare, Adeniyi, Akpuokwe, & Eneh, 2024). Instead, a patchwork of state-level laws, such as the California Consumer Privacy Act (CCPA) and Virginia Consumer Data Protection Act (VCDPA), coexists with sector-specific federal regulations like the Health Insurance Portability and Accountability Act (HIPAA). This fragmentation creates a complex and often inconsistent compliance environment, particularly for organizations deploying AI systems that operate across multiple jurisdictions (Perumal, 2022).

The interplay between state and federal laws further complicates compliance efforts. While state laws may provide comprehensive protections, their requirements can vary significantly, leading to regulatory uncertainty for businesses (Rudden, 2025). For example, the CCPA imposes specific obligations on data controllers and processors, which may not align seamlessly with requirements under other state laws. Additionally, federal laws such as HIPAA are often narrowly tailored to specific industries, leaving significant gaps in addressing broader data privacy concerns in the AI context (Evans, 2022).

This paper aims to address these challenges by developing a conceptual model that harmonizes data privacy compliance across state and federal laws in the U.S. The proposed framework seeks to create consistent standards for managing AI data, ensuring compliance and innovation. By streamlining legal obligations and fostering interoperability between jurisdictions, the model aspires to enhance trust in AI systems while reducing the regulatory burden on organizations.

The paper is structured as follows. First, an overview of key U.S. data privacy laws and the unique challenges AI systems face in adhering to them is provided. Next, the proposed conceptual framework is introduced, detailing its principles and objectives. This is followed by discussion of the methodology used to develop the model and its key components. Practical applications of the model are then illustrated through case studies, highlighting its effectiveness in addressing real-world compliance challenges. Finally, the paper concludes with recommendations for policymakers, businesses, and researchers, emphasizing the importance of collaboration in advancing data privacy governance in the U.S. Through this structured approach, the paper aims to contribute meaningfully to the ongoing discourse on data privacy in the AI era, offering practical solutions to bridge the regulatory gaps in the U.S. and fostering a future where innovation and privacy coexist harmoniously.

OVERVIEW OF U.S. DATA PRIVACY LAWS AND AI CHALLENGES

Major U.S. Privacy Laws

Without a comprehensive federal data privacy law, the U.S. relies on state-level legislation and sector-specific rules to regulate data privacy. Among the most prominent state laws is the California Consumer Privacy Act (CCPA), which grants residents rights such as access to personal information, the ability to opt out of data sales, and the right to request data deletion.

The California Privacy Rights Act (CPRA), an amendment to the CCPA, further expands these rights, introducing provisions for sensitive data handling and establishing the California Privacy Protection Agency to enforce compliance (Renuka, RadhaKrishnan, Priya, Jhansy, & Ezekiel, 2025).

Virginia's Consumer Data Protection Act (VCDPA) and Colorado's Privacy Act (CPA) offer additional examples of state-level legislation. While these laws share similarities with the CCPA, they also introduce unique provisions, such as opt-in consent requirements for sensitive data processing under the VCDPA and detailed rights for data portability under the CPA. These differences illustrate the variability in state laws, complicating compliance for organizations operating in multiple jurisdictions (Austin-Gabriel, Monsalve, & Varde, 2024; Hanson, Okonkwo, & Orakwe).

At the federal level, sector-specific laws such as the Health Insurance Portability and Accountability Act (HIPAA) regulate data within defined domains. HIPAA focuses on safeguarding protected health information (PHI) and imposes strict standards for data handling by covered entities and their associates. Similarly, the Gramm-Leach-Bliley Act (GLBA) governs the financial sector, ensuring the confidentiality and security of consumer financial data. While effective within their respective domains, these laws fail to address broader privacy concerns or offer guidance for the unique challenges AI systems pose (Emmanuel, Aria, Jose, & Diego, 2025).

Challenges for AI Systems

AI systems depend on extensive datasets to train algorithms, develop models, and make predictions. This dependency introduces numerous compliance challenges, particularly in a fragmented regulatory environment. First, variations in state-level laws require organizations to adapt their data handling practices to meet different legal obligations, increasing administrative burdens and costs. For example, the definition of "sensitive data" and the requirements for consent differ significantly between the CCPA, CPRA, and VCDPA, creating uncertainty for businesses (Hanson, Okonkwo, & Orakwe).

Second, AI systems often involve cross-border data transfers between states and, in some cases, countries. This complicates compliance further, as organizations must navigate conflicting legal requirements, such as differing data anonymization or encryption thresholds. The lack of uniformity in these standards undermines efforts to create consistent data governance practices.

Third, AI introduces unique privacy risks that current laws do not adequately address. Issues such as algorithmic bias, automated decision-making, and data inferencing challenge the traditional definitions of personal data and consent. For instance, AI systems can generate new insights about individuals by analyzing non-sensitive data, effectively creating sensitive information that existing regulations may not explicitly cover. These emerging risks highlight the limitations of current laws in capturing the full scope of AI-driven data processing (P. A. Adepoju et al., 2022; Austin-Gabriel, Afolabi, Ike, & Hussain, 2024).

Gaps and Inconsistencies

The absence of a unified federal privacy framework leaves significant gaps in U.S. data privacy governance. One notable gap is the inconsistent protection of individuals' rights across states. While residents of California enjoy robust privacy rights under the CCPA and CPRA, those in states without comprehensive privacy laws are left with limited protections. This disparity creates inequities and complicates the deployment of nationwide AI systems.

Another inconsistency lies in the scope and applicability of federal laws. HIPAA and the GLBA are narrowly tailored to specific industries, leaving many sectors unregulated or subject only to general tort principles. This sectoral approach fails to account for the cross-industry nature of AI, where data from various domains is often combined and analyzed (A.

H. Adepoju, Hamza, Collins, & Austin-Gabriel, 2025; Austin-Gabriel, Hussain, Adepoju, & Afolabi).

Moreover, enforcement mechanisms vary widely between jurisdictions. While the CPRA establishes a dedicated enforcement agency, other states rely on underfunded regulatory bodies or private litigation to uphold compliance. This lack of uniformity weakens overall accountability and creates uncertainty for businesses. Finally, the existing regulatory framework does not adequately account for the global nature of AI systems. Many U.S.-based organizations must also comply with international regulations such as the GDPR, which often imposes stricter requirements. Reconciling these conflicting obligations adds another layer of complexity for organizations seeking to remain competitive in a global market (Oyegbade, Igwe, Ofodile, & C, 2021).

In summary, U.S. data privacy laws' fragmented nature and limited scope create significant challenges for AI systems. These challenges are compounded by inconsistencies in enforcement, variations in state-level requirements, and the inability of current regulations to address the unique risks associated with AI technologies. Addressing these issues requires a cohesive and comprehensive approach that harmonizes privacy standards across jurisdictions while accommodating the transformative potential of AI.

CONCEPTUAL FRAMEWORK FOR HARMONIZING PRIVACY COMPLIANCE

Interoperability

The principle of interoperability ensures that the framework facilitates seamless compliance with varying legal requirements across jurisdictions. The model allows organizations to adopt standardized practices while respecting regional differences by enabling compatibility between state-specific laws and federal regulations. This can be achieved by developing a common compliance protocol, which outlines baseline requirements derived from shared elements of existing laws. For example, most state privacy laws grant individuals rights to access, delete, or opt out of data sharing. These rights can serve as a foundation for the protocol, with additional layers tailored to specific state-level requirements.

Interoperability also involves the integration of privacy-enhancing technologies (PETs), such as differential privacy and federated learning, which can help organizations manage data in compliance with diverse regulations. These technologies enable the processing and analysis of data without exposing sensitive information, ensuring that privacy requirements are upheld even in complex AI workflows (Hanson, Okonkwo, & Orakwe; Okedele, Aziza, Oduro, & Ishola, 2024b).

Consistency

Consistency within the framework addresses the need for uniform application of privacy principles across all jurisdictions. This principle seeks to eliminate the confusion caused by conflicting legal definitions, obligations, and enforcement mechanisms, creating a stable and predictable regulatory environment.

A unified taxonomy of key terms and concepts—such as "personal data," "data processing," and "consent"—is essential for achieving consistency. The framework proposes aligning these definitions to minimize ambiguities and ensure clarity for organizations and individuals. Additionally, it advocates for consistent enforcement standards, such as uniform penalties for non-compliance, which reduce disparities between states and foster a level playing field. By providing universal guidelines, the framework empowers organizations to design and implement AI systems with greater confidence. This reduces compliance costs and encourages innovation by removing legal uncertainties that often hinder the deployment of new technologies (Afolabi, Hussain, Austin-Gabriel, Ige, & Adepoju, 2023; O. A. Bakare, Aziza, Uzougbo, & Oduro, 2024b).

Transparency

Transparency is critical to trust in AI systems and data privacy practices. The framework emphasizes the need for organizations to communicate their data collection, usage, and sharing practices to regulators and individuals. Transparent practices enable individuals to make informed decisions about their data while helping regulators assess compliance more effectively.

To operationalize transparency, the framework recommends the adoption of standardized privacy notices that provide concise and comprehensible information about data practices. These notices should be designed to meet the needs of diverse audiences, including individuals without legal or technical expertise. Furthermore, transparency extends to AI-specific challenges, such as algorithmic decision-making. The framework advocates for the inclusion of explainability mechanisms that allow individuals to understand how their data is used in AI processes and the outcomes it generates. This enhances accountability and mitigates the risks of bias and discrimination in AI systems (Hanson, Okonkwo, & Orakwe; Hussain, Austin-Gabriel, Ige, Adepoju, & Afolabi, 2023).

Scalability

Scalability ensures that the framework can adapt to the evolving landscape of data privacy and AI technologies. As new privacy laws emerge and AI capabilities expand, the model must remain flexible to accommodate these changes without imposing undue burdens on organizations.

The framework incorporates modular components that can be updated or expanded as needed. For instance, a baseline compliance protocol can be augmented with new provisions to address emerging risks, such as the use of biometric data or generative AI models. This modularity allows organizations to maintain compliance without overhauling their existing systems. Scalability also involves leveraging AI-driven compliance tools, such as automated auditing systems and real-time monitoring software. These tools enable organizations to efficiently track and manage their obligations, ensuring that compliance processes can scale alongside their operations (Apata, Falana, Hanson, Oderhohwo, & Oyewole, 2023; Hanson & Sanusi, 2023).

The proposed framework balances regulatory compliance and AI innovation by reducing complexity and fostering a conducive environment for technological advancement. The model simplifies the regulatory landscape by harmonizing privacy laws, enabling organizations to allocate more resources to innovation rather than legal navigation.

Additionally, integrating PETs and explainability mechanisms aligns with ethical AI principles, promoting responsible innovation. Organizations can leverage these tools to design systems that comply with legal requirements and address societal concerns, such as bias and discrimination. The framework further supports innovation by encouraging collaboration between regulators, industry stakeholders, and civil society. The model fosters dialogue and knowledge-sharing by establishing advisory boards and public-private partnerships, ensuring that privacy regulations keep pace with technological advancements (O. A. Bakare, Aziza, Uzougbo, & Oduro, 2024a).

METHODOLOGY AND KEY COMPONENTS OF THE MODEL

Developing a conceptual framework to harmonize privacy compliance across U.S. jurisdictions requires a structured approach to ensure practicality and effectiveness. This section outlines the methodology employed to design the model and details its key components. The framework leverages existing legal principles, incorporates best practices from comparative studies, and integrates technological advancements to address the complexities of cross-jurisdictional AI data governance.

Methodology

The model was developed through a multi-step process that combined theoretical research with practical analysis. The process began with an extensive review of academic studies, policy papers, and industry reports to identify the core challenges associated with privacy compliance in AI. This step also highlighted successful strategies from other regulatory frameworks, such as the GDPR, that could inform the design of the proposed model.

A detailed examination of key U.S. state and federal privacy laws was conducted to identify commonalities and differences. This analysis revealed overlapping provisions, such as individual rights to data access and deletion, as well as divergent requirements, such as variations in the definition of sensitive data. These insights informed the development of a unified protocol that accommodates state-specific nuances while providing consistency. Input from stakeholders—including policymakers, industry representatives, and privacy advocates—was incorporated to ensure the model is balanced and pragmatic. Feedback from these groups helped refine the framework's components, ensuring they address real-world challenges while promoting compliance and innovation.

Hypothetical scenarios were used to test the model's applicability in different contexts, such as healthcare, finance, and e-commerce. These case studies validated the framework's ability to handle diverse data governance needs across sectors.

Key Components of the Model

The proposed framework is composed of four interdependent components, each addressing a critical aspect of privacy compliance:

Data Classification

Data classification serves as the framework's foundation, enabling organizations to manage their data assets in a structured and compliant manner. The model introduces a tiered classification system that categorizes data based on its sensitivity and intended use. Non-sensitive data, such as aggregated statistics, includes information that poses minimal privacy risks. Sensitive data requires heightened protection, such as health records, financial information, and biometric identifiers. The model also accounts for derived data, including insights generated by AI models, such as inferred or predictive attributes about individuals. By clearly defining these categories, the framework helps organizations implement appropriate safeguards tailored to the nature of the data. This structure facilitates compliance with varying legal requirements and improves the efficiency of data management practices.

Consent Management

Consent lies at the heart of privacy compliance, and the framework underscores its critical importance in AI data governance. The model incorporates several advanced mechanisms for managing consent to accommodate diverse regulatory landscapes. Dynamic consent mechanisms allow individuals to provide, modify, or withdraw their consent for specific data uses in real time, giving them greater control over their personal information. Granular control enables users to specify consent preferences at a detailed level, such as consenting to data collection for one purpose but not another. The framework also proposes a unified consent protocol to standardize consent management across jurisdictions. This ensures consistency for organizations operating in multiple states, enhancing transparency and empowering users to make informed decisions about their data.

Risk Assessment

Proactively identifying and mitigating privacy risks are central to the framework's approach to compliance. Organizations must conduct privacy impact assessments (PIAs) for AI projects, identifying potential risks to individuals and outlining strategies to address them. Regular algorithmic audits are another key element, providing evaluations of AI models to ensure they meet ethical and legal standards. These audits address bias, discrimination, and lack of transparency, fostering trust in AI systems. A quantifiable risk scoring system is introduced to

help organizations prioritize their resources. This enables a focused approach, directing attention to the most critical risks and ensuring efficient risk management. By embedding these practices into the framework, organizations can maintain compliance while minimizing potential harms associated with AI technologies.

Enforcement Mechanisms

Effective enforcement ensures that the framework operates as intended and achieves its objectives. The model establishes standardized reporting requirements, obligating organizations to submit regular compliance reports to regulatory authorities. These reports provide transparency into data governance practices and risk management efforts, facilitating oversight and accountability. Collaborative enforcement models are also encouraged, fostering cooperation between state and federal agencies to reduce redundancies and inconsistencies in enforcement efforts. Additionally, the framework includes clear remediation protocols for addressing non-compliance. These guidelines outline timelines for corrective actions and specify penalties for repeated violations, ensuring that organizations remain accountable for their practices.

By integrating data classification, consent management, risk assessment, and enforcement mechanisms, the proposed framework provides a robust solution for harmonizing privacy compliance across jurisdictions. This comprehensive approach helps organizations navigate the complexities of U.S. privacy laws and promotes trust, transparency, and innovation in the rapidly evolving field of AI.

Technological Enablers

The integration of advanced technologies plays a pivotal role in bringing the proposed framework into practice. These technologies are key enablers, streamlining compliance processes and enhancing the framework's effectiveness. By leveraging these tools, organizations can operationalize the framework with greater precision and efficiency, addressing complex privacy challenges in AI data governance.

- AI Compliance Tools: AI compliance tools are indispensable for automating critical compliance tasks, significantly reducing the administrative burden on organizations. These tools facilitate data mapping, consent management, and monitoring of legal updates, ensuring that organizations remain aligned with evolving regulatory requirements. For instance, natural language processing algorithms can analyze complex privacy policies to verify compliance with applicable laws and standards. Such tools enhance operational efficiency and minimize the risk of human error, ensuring that compliance measures are robust and consistent across various jurisdictions.
- Privacy-Enhancing Technologies (PETs): Privacy-enhancing technologies enable organizations to process data responsibly while safeguarding individual privacy. Techniques such as differential privacy ensure that aggregate data can be analyzed without exposing specific individuals' information. Homomorphic encryption allows computations on encrypted data, eliminating the need to decrypt sensitive information during processing. Secure multi-party computation further enhances privacy by enabling collaborative data analysis without revealing raw data to any party. These technologies are particularly valuable for AI applications that rely on large-scale data analysis, ensuring that privacy remains intact even as data is leveraged for innovation and insights.
- Blockchain for Audit Trails: Blockchain technology offers an immutable and transparent means of recording data processing activities, bolstering accountability and trust. By creating secure, time-stamped records of how data is collected, stored, and processed, blockchain serves as an effective audit trail for compliance verification. This capability is especially useful during regulatory audits, providing clear evidence of adherence to privacy laws and organizational policies. Additionally, blockchain's decentralized nature

ensures that records cannot be tampered with, further enhancing the reliability of compliance documentation.

- Real-Time Monitoring Systems: AI-driven real-time monitoring systems are crucial for identifying potential privacy violations or compliance risks as they occur. These systems leverage machine learning algorithms to continuously assess data processing activities, flagging anomalies or deviations from established protocols. By addressing issues proactively, organizations can mitigate risks before they escalate into significant violations. Real-time monitoring also enables adaptive compliance, allowing organizations to respond swiftly to changes in legal requirements or emerging threats in the data landscape (Austin-Gabriel, Afolabi, Ike, & Yemi, 2024; Oyegbade, Igwe, Ofodile, & C, 2022).

In summary, the methodology and components of the proposed framework are designed to address the unique challenges of harmonizing privacy compliance in the U.S. By combining rigorous research, stakeholder input, and advanced technologies, and the model offers a practical solution that balances legal obligations with the demands of AI innovation. Its tiered approach to data classification, robust consent mechanisms, proactive risk assessment, and scalable enforcement strategies ensure that organizations can navigate the complexities of cross-jurisdictional compliance effectively. With the integration of technological enablers, the framework simplifies compliance and promotes ethical and responsible AI development.

CASE STUDIES AND PRACTICAL APPLICATIONS

This section explores real-world and hypothetical scenarios to demonstrate the functionality and effectiveness of the proposed framework for harmonizing privacy compliance in the U.S. These examples illustrate how the framework addresses multi-state and federal compliance challenges, fostering AI innovation while upholding individual privacy.

Healthcare Data Governance

A healthcare technology company operates across California, Virginia, and New York, offering AI-powered telemedicine services. Its platform collects sensitive patient data, such as medical histories, biometric information, and real-time health metrics, to provide personalized treatment recommendations. The company faces compliance challenges due to varying privacy laws. For instance, it must adhere to sector-specific federal regulations such as HIPAA while complying with the California Consumer Privacy Act and Virginia's Consumer Data Protection Act. Differences in consent requirements, definitions of sensitive data, and enforcement mechanisms complicate efforts to ensure compliance (Hussain, Austin-Gabriel, Adepoju, & Afolabi).

The proposed framework addresses these challenges effectively. The company categorizes data into sensitive and non-sensitive categories through its tiered classification system, applying stricter safeguards to biometric information. A unified consent framework allows patients to manage granular data-sharing preferences, with dynamic consent mechanisms enabling real-time modifications. Privacy impact assessments mitigate risks associated with AI algorithms, while blockchain technology creates immutable records of consent-related transactions. This approach harmonizes compliance practices across jurisdictions, ensuring legal adherence without compromising the company's ability to innovate. Patients gain transparency and greater control over their data, enhancing trust in the platform (Okedele, Aziza, Oduro, & Ishola, 2024a).

E-Commerce and Personalized Advertising

A nationwide e-commerce retailer uses AI to analyze customer behavior, delivering personalized product recommendations. The platform collects browsing history, purchase patterns, and geolocation data. The retailer must navigate compliance with state laws such as the California Privacy Rights Act and Colorado Privacy Act, which impose varying

requirements for data transparency, opt-out rights, and targeted advertising. Managing consent for millions of users across multiple states further complicates compliance efforts.

The framework streamlines these processes by classifying customer data into non-sensitive and sensitive categories, with geolocation data subject to stricter protections. A standardized consent protocol enables users to opt out of data collection for targeted advertising, ensuring compliance with state laws. Redesigned privacy notices clearly explain data usage and user rights, supported by explainability tools for transparency in AI-driven recommendations. Differential privacy anonymizes customer data, mitigating re-identification risks while maintaining the effectiveness of personalized insights. This approach fosters regulatory compliance, customer trust, and brand loyalty (Latilo, Uzougbo, Ugwu, Oduro, & Aziza, 2024).

Financial Fraud Detection

A financial services firm employs AI to detect fraudulent transactions, analyzing vast customer data such as transaction histories and account activity patterns. The firm faces dual challenges: compliance with the Gramm-Leach-Bliley Act at the federal level and adherence to state-specific privacy laws governing financial data. Balancing data privacy with the need for real-time fraud detection adds further complexity.

Under the framework, transaction histories are classified as sensitive data, subject to stringent access controls. Algorithmic audits ensure that fraud detection models comply with ethical and legal standards while addressing potential biases. Customers receive clear explanations of how AI algorithms flag fraudulent activities, enhancing transparency. Real-time monitoring systems track data usage, ensuring compliance with federal and state regulations. This approach enables effective fraud detection while maintaining robust privacy protections, strengthening customer confidence in the firm.

A startup develops an AI-powered platform for smart cities, integrating data from traffic sensors, public transportation systems, and citizen feedback. Operating in multiple states with distinct privacy laws, the platform faces challenges in harmonizing data handling practices. The framework's interoperable compliance protocol allows the startup to standardize governance practices across jurisdictions, ensuring consistency. Its scalability enables the platform to adapt seamlessly to new privacy regulations as they emerge. Privacy-enhancing technologies such as secure multi-party computation facilitate data analysis without compromising individual privacy. By operationalizing these elements, the framework supports the efficient rollout of the platform across states, balancing data-driven innovation with strong privacy protections (P. A. Adepoju, Hussain, Austin-Gabriel, & Afolabi; Durojaiye, Ewim, & Igwe; Hussain).

CONCLUSION AND RECOMMENDATIONS

Summary of Key Findings

This paper identified critical challenges associated with cross-jurisdictional compliance in the U.S., rooted in the fragmented nature of state privacy laws and the absence of a comprehensive federal framework. The proposed model addresses these challenges through a unified compliance protocol that balances regional differences while establishing consistent standards nationwide. The framework simplifies the complex compliance process by leveraging technological enablers such as privacy-enhancing tools, automated compliance solutions, and explainability mechanisms while enhancing transparency and accountability. Furthermore, it supports AI-driven innovation by mitigating legal uncertainties and reducing operational inefficiencies often hindering technological advancement.

The case studies demonstrated the framework's practical applications across diverse sectors, including healthcare, e-commerce, and financial services. These examples showcased its flexibility in resolving compliance challenges, harmonizing privacy practices, and safeguarding individual rights without stifling innovation. The results confirm that the model

is a viable solution for navigating the complexities of AI data governance while promoting trust and transparency.

Recommendations

For the framework to achieve widespread adoption and efficacy, several steps must be taken by policymakers, organizations, and AI developers. Policymakers should prioritize the creation of a comprehensive federal privacy standard that incorporates the principles outlined in this paper. Such a law would bridge the gaps between state-level regulations, ensuring consistency and clarity for organizations. Collaboration between state and federal authorities is essential to harmonize enforcement mechanisms, reduce conflicts, and streamline compliance processes. To further encourage adoption, governments could incentivize using advanced privacy-preserving tools by offering financial benefits such as tax credits or grants.

Organizations play a vital role in implementing this framework. Investment in robust compliance infrastructure is crucial for managing data classification, consent mechanisms, and real-time monitoring. Training programs should be introduced to educate employees about AI data usage's ethical and legal implications, fostering a culture of accountability. Regular risk assessments, including privacy impact evaluations and algorithmic audits, are necessary to identify vulnerabilities and ensure ethical and legal standards adherence.

AI developers are equally responsible for ensuring their systems align with privacy and transparency requirements. Incorporating privacy-by-design principles is critical for embedding compliance mechanisms into the core architecture of AI systems. Explainable AI should be prioritized to enhance user understanding of AI-driven decisions, fostering trust and meeting regulatory requirements. Additionally, modular and scalable system designs will enable AI technologies to adapt to changing legal landscapes and new privacy laws as they emerge.

Future Research Directions

While the proposed framework offers a robust solution for harmonizing privacy compliance, further research is essential to refine its components and address new challenges. One important area of study involves adapting the framework for global compliance, particularly about international standards like GDPR. As AI technologies evolve, researchers must address the privacy risks associated with generative models and autonomous systems, which may present unique challenges not covered by existing frameworks.

Evaluating the effectiveness of enforcement mechanisms is another critical area for exploration. Studies should examine how penalties, audits, and collaborative oversight influence organizational behavior and compliance outcomes. Additionally, understanding public perceptions of AI systems and data governance practices can inform the development of policies that protect privacy and enhance user trust and engagement.

References

Adepoju, A. H., Hamza, O., Collins, A., & Austin-Gabriel, B. (2025). Integrating Risk Management and Communication Strategies in Technical Research Programs to Secure High-Value Investments. *Gulf Journal of Advance Business Research, 3*(1), 105-127.

Adepoju, P. A., Austin-Gabriel, B., Ige, A. B., Hussain, N. Y., Amoo, O. O., & Afolabi, A. I. (2022). Machine learning innovations for enhancing quantum-resistant cryptographic protocols in secure communication.

Adepoju, P. A., Hussain, N. Y., Austin-Gabriel, B., & Afolabi, A. I. Data Science Approaches to Enhancing Decision-Making in Sustainable Development and Resource Optimization.

Afolabi, A. I., Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., & Adepoju, P. A. (2023). Geospatial AI and data analytics for satellite-based disaster prediction and risk

assessment.

Apata, O. E., Falana, O. E., Hanson, U., Oderhohwo, E., & Oyewole, P. O. (2023). Exploring the Effects of Divorce on Children's Psychological and Physiological Wellbeing. *Asian Journal of Education and Social Studies, 49*(4), 124-133.

Austin-Gabriel, B., Afolabi, A. I., Ike, C. C., & Hussain, N. Y. (2024). Machine learning for preventing cyber-attacks on entrepreneurial crowdfunding platforms. *Open Access Research Journal of Science and Technology, 12*(02), 146-154. doi:https://doi.org/10.53022/oarjst.2024.12.2.0148

Austin-Gabriel, B., Afolabi, A. I., Ike, C. C., & Yemi, N. (2024). AI and machine learning for detecting social media-based fraud targeting small businesses.

Austin-Gabriel, B., Hussain, N. Y., Adepoju, P. A., & Afolabi, A. I. Large Language Models for Automating Data Insights and Enhancing Business Process Improvements.

Austin-Gabriel, B., Monsalve, C. N., & Varde, A. S. (2024). Power Plant Detection for Energy Estimation using GIS with Remote Sensing, CNN & Vision Transformers. *arXiv preprint arXiv:2412.04986*.

Bakare, O. A., Aziza, O. R., Uzougbo, N. S., & Oduro, P. (2024a). Ethical and legal project management framework for the oil and gas industry. *International Journal of Applied Research in Social Sciences, 6*(10).

Bakare, O. A., Aziza, O. R., Uzougbo, N. S., & Oduro, P. (2024b). A governance and risk management framework for project management in the oil and gas industry. *Open Access Research Journal of Science and Technology, 12*(01), 121-130.

Bakare, S. S., Adeniyi, A. O., Akpuokwe, C. U., & Eneh, N. E. (2024). Data privacy laws and compliance: a comparative review of the EU GDPR and USA regulations. *Computer Science & IT Research Journal, 5*(3), 528-543.

Durojaiye, A. T., Ewim, C. P.-M., & Igwe, A. N. Designing a machine learning-based lending model to enhance access to capital for small and medium enterprises.

Dwivedi, Y. K., Hughes, L., Ismagilova, E., Aarts, G., Coombs, C., Crick, T., . . . Eirug, A. (2021). Artificial Intelligence (AI): Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 57*, 101994.

Emmanuel, O., Aria, J., Jose, D., & Diego, C. (2025). The Impact of Cybersecurity Laws on Legal Procedures and Case Law.

Evans, B. J. (2022). The HIPAA privacy rule at age 25: privacy for equitable AI.

Hanson, U., Okonkwo, C. A., & Orakwe, C. U. Fostering Mental Health Awareness and Academic Success Through Educational Psychology and Telehealth Programs Retrieved from https://www.irejournals.com/paper-details/1706745

Hanson, U., Okonkwo, C. A., & Orakwe, C. U. Implementing AI-Enhanced Learning Analytics to Improve Educational Outcomes Using Psychological Insights. Retrieved from https://www.irejournals.com/formatedpaper/1706747.pdf

Hanson, U., Okonkwo, C. A., & Orakwe, C. U. Leveraging educational psychology to transform leadership in underserved schools.

Hanson, U., Okonkwo, C. A., & Orakwe, C. U. Promoting inclusive education and special needs support through psychological and educational frameworks. doi:https://www.irejournals.com/paper-details/1706746

Hanson, U., & Sanusi, P. (2023). *Examining determinants for eligibility in special needs education through the lens of race and ethnicity: A scoping review of the literature.* Paper presented at the APHA 2023 Annual Meeting and Expo.

Hussain, N. Y. (N.D.). Deep Learning Architectures Enabling Sophisticated Feature Extraction and Representation for Complex Data Analysis.

Hussain, N. Y., Austin-Gabriel, B., Adepoju, P. A., & Afolabi, A. I. AI and Predictive

Modeling for Pharmaceutical Supply Chain Optimization and Market Analysis.

Hussain, N. Y., Austin-Gabriel, B., Ige, A. B., Adepoju, P. A., & Afolabi, A. I. (2023). Generative AI advances for data-driven insights in IoT, cloud technologies, and big data challenges.

Latilo, A., Uzougbo, N. S., Ugwu, M. C., Oduro, P., & Aziza, O. R. (2024). Developing legal frameworks for successful engineering, procurement, and construction projects.

Okedele, P. O., Aziza, O. R., Oduro, P., & Ishola, A. O. (2024a). Climate change litigation as a tool for global environmental policy reform: A comparative study of international case law. *Global Environmental Policy Review*.

Okedele, P. O., Aziza, O. R., Oduro, P., & Ishola, A. O. (2024b). Human Rights, Climate Justice, and Environmental Law: Bridging International Legal Standards for Social Equity. *Human Rights, 20*(12), 232-241.

Oyegbade, I. K., Igwe, A. N., Ofodile, O. C., & C, A. (2021). Innovative financial planning and governance models for emerging markets: Insights from startups and banking audits. . *open Access Research Journal of Multidisciplinary Studies, 01*(02), 108-116.

Oyegbade, I. K., Igwe, A. N., Ofodile, O. C., & C, A. (2022). Advancing SME Financing Through Public-Private Partnerships and Low-Cost Lending: A Framework for Inclusive Growth. *Iconic Research and Engineering Journals, 6*(2), 289-302.

Perumal, V. (2022). The future of US data privacy: Lessons from the GDPR and State Legislation.

Renuka, O., RadhaKrishnan, N., Priya, B. S., Jhansy, A., & Ezekiel, S. (2025). Data Privacy and Protection: Legal and Ethical Challenges. *Emerging Threats and Countermeasures in Cybersecurity*, 433-465.

Rudden, L. (2025). *Fragmented Data Privacy Laws: Time for Federal Legislation.* Paper presented at the Boston College Intellectual Property and Technology Forum.

Settibathini, V., Kothuru, S. K., Vadlamudi, A. K., Thammreddi, L., & Rangineni, S. (2023). Strategic analysis review of data analytics with the help of artificial intelligence. *International Journal of Advances in Engineering Research, 26*, 1-10.