International Journal of Scientific Research and Management (IJSRM)
||Volume||12||Issue||12||Pages||573-584||2024||
Website: https://ijsrm.net ISSN (e): 2321-3418
DOI: 10.18535/ijsrm/v12i12.lla01

Data Privacy and Regulatory Compliance: A Call for a Centralized Regulatory Framework

Olumide Ajayi Timothy

Graduate Programs: University of Illinois, Urbana Champaign, University of Cumberlands.

Abstract
Considering the recent technological advancements, the study examines the need for centralized data privacy and compliance regulation in the United States of America (USA). There is no centralized data privacy landscape in the USA other than decentralized regulations across various states. This has hindered the development of a standardized approach to data protection. Therefore, this study examined the key challenges associated with the current data privacy landscape in the USA and how a centralized data privacy and compliance regulation can address these challenges.
Objective: The study's primary purpose was to examine the plausibility of a unified framework on data privacy within the US and how data can be well-managed.
Method: The study employed a theoretical approach, analyzing existing literature, case studies, and current legal framework to assess the extent of data protection within the United States and make a case for a prompt federal law that would be all-encompassing in the subject matter of data, data privacy, and security.
Results: The study found no centralized data privacy landscape in the USA other than decentralized regulations across various states, which can lead to inconsistencies and business compliance burdens. Additionally, the existing laws may not adequately address emerging privacy challenges, such as those related to artificial intelligence and big data.
Conclusion: The study concluded that centralized data privacy and compliance regulation could significantly enhance data protection in the USA. Thus, such a regulation could provide a more robust, consistent, and effective framework for safeguarding personal data.

Keywords: Data, Data Privacy, Rights, Legislations, Compliance, Regulations.

Introduction

Today's digital age boasts that collecting, processing, and sharing personal data have become ubiquitous, transforming how businesses operate, interact with customers, and drive innovation. However, this rapid growth in data-driven activities has also raised significant concerns about data privacy, security, and compliance (Faster Capital, 2004). Debates on human rights, data protection, and confidentiality are rising.

This is especially true regarding pervasive automatic computing, mass surveillance, and related threats to privacy (Murphy, 2015). Data is fast becoming one of the most valuable and resourceful resources in the modern world. It drives innovation, insights, and opportunities for individuals, organizations, and societies. However, despite the excellent value data offers, it has significant risks and challenges, including ethical issues, privacy concerns, security, and governance (Faster Capital, 2004).

Considering this 21st-century issue, and while there have been various efforts across jurisdictions to ensure a proper background and framework to regulate problems arising from data privacy and concerns duly, it is worth noting that the United States does not have a single comprehensive principal data protection legislation. Instead, what is obtainable is a plethora of laws enacted at both the federal and state levels to protect the personal data of US residents. (Pittman et al, 2024).

At the federal level, the Federal Trade Commission Act (FTC Act) grants the U.S. Federal Trade Commission (FTC) broad authority to take legal action against unfair or deceptive practices that harm consumers and enforce federal regulations designed to protect privacy and data. In addition to the FTC Act, several other federal laws address specific aspects of data privacy. For instance, the Driver's Privacy Protection Act of 1994 safeguards the confidentiality of personal information collected by state Departments of Motor Vehicles. The Children's Online Privacy Protection Act (COPPA) prohibits online information collection from children under 13. It mandates the publication of privacy notices and the acquisition of verifiable parental consent before collecting such information. The Video Privacy Protection Act restricts the disclosure of rental or sales records for videos or similar audio-visual materials, including online streaming services. While these laws provide some protection, they are often limited in scope and may not adequately address the evolving landscape of data privacy challenges (Pittman et al., 2024).

While some states are more active and engaging in data privacy issues, some are reluctant to ensure proper regulation, and there is indeed no unifying legislation that brings all the states together regarding data privacy. This has formed the basis for this paper, which seeks to gather insights into the conceptual understanding of data, data privacy, and compliance. It also provides an understanding of how far the US has gone in terms of legal and regulatory framework coupled with institutions that have been available to regulate data concerns, as well as the need for a unifying federal law that would ensure uniformity in the protection of data, ensuring data privacy across the board within the states and recommendations.

The following research question guides this study:

1. What is the relationship between data, privacy, and compliance?
2. How well does the conceptual clarification of data, data privacy, and compliance resonate with cyber-security and protecting confidential information?
3. What legal frameworks regulate data and data privacy within the US jurisdiction, both at the federal and state level, and how well has compliance been achieved?
4. What gaps can be identified with the availability of sector-specific legislation on data privacy and state laws on data sharing regulation?
5. What is the implication(s) for proposing federal/unified data privacy laws for the United States, and what impact would such legislation have, considering prevailing circumstances?

Understanding Data, Data Privacy and Compliance

A working knowledge of what constitutes Data, Data Privacy, and Compliance is necessary for a comprehensive understanding of the thematic concerns in this study.

Data means "recorded information, regardless of the form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost, pricing, or management information (Law Insider, 2024). It also entails all results, technical information, and materials developed and obtained in the performance of the Services hereunder, including but not limited to all reports, survey and evaluation tools, surveys and assessments, plans, charts, recordings (video and sound), pictures, curricula, electronically prepared presentations, public awareness or prevention campaign materials, drawings, analyses, graphic representations, computer programs and printouts, notes and memoranda, and documents, whether finished or unfinished, which result from or are prepared in connection with the Services performed hereunder; electronic representation of information in any form; digital representation of facts, acts or information and any compilation of such acts, facts or information, including the form of sound, visual or audio-visual recording (Law Insider, 2024).

Data Privacy is a branch of data security concerned with properly handling data – consent, notice, and regulatory obligations. More specifically, practical data privacy concerns often revolve around whether or how data is shared with third parties, how data is legally collected or stored, and regulatory restrictions such as general data privacy regulations and the Health Insurance Portability and Accountability Act, among others. Data privacy, also referred to as information privacy, is said to be that area of data protection that

concerns the proper handling of sensitive data, including personal data, to meet regulatory requirements and protect the confidentiality and immutability of the data. Data protection spans three broad categories: traditional data protection (such as backup and restore copies), data security, and data privacy (SNIA, 2004).

Privacy can also be said to be the right of an individual to be free from uninvited surveillance; safely existing in one's space and freely expressing one's opinions behind closed doors is critical to living in a democratic society (Buckbee, 2024). Compliance means doing something according to the required obligations, yielding or carrying it into effect, or accommodating something (The Law Dictionary, 2024).

Given the above, it can be safely said that data privacy and compliance regulations are the set of practices, policies, and regulations/ procedures that an organization/firm implements to ensure they adhere to all legal regulations and standards concerning their users' private information; which creates a balance between the need for the collection of such data and the individual's right to control their personal information (Davis, 2024).

Legal and Regulatory Framework and Institutions on Data Privacy and Compliance Regulations in the United States of America

As stated in the introductory part of this study, there is no unified law on data protection in the United States. Instead, what is obtainable is a variety of laws enacted at both state and federal levels to protect the personal data of the person(s) residing in the United States. Here, we shall be examining selected applicable laws at both state and federal levels to gain a proper understanding of the subject matter concerning the study. In the United States, legislations ranging from the Driver's Privacy Protection Act of 1994 (18 U.S. Code § 2721 *et seq.,* Children's Online Privacy Protection Act (COPPA) (15 U.S. Code § 6501), The Video Privacy Protection Act (18 U.S. Code § 2710 *et seq.*), the Cable Communications Policy Act of 1984 and the Biden-Harris Executive order on National Cyber Security Strategy will be examined *in seriatim.*

<u>The Driver's Privacy Protection Act of 1994 (18 U.S. Code § 2721</u>

The Driver's Privacy Protection Act of 1994 is one of the relevant legislations related to data protection. This legalization, passed in 1994, ensures the privacy and disclosure of personal information gathered by the State Department of Motor Vehicles (Gorin, 2023).

What led to the passage of this legislation, introduced by Jim Moran from Virginia in 1992, was premised on the fact that after an increase in some opponents of abortion, relevant authorities were using public driving license databases to track down and harass abortion providers and patients. Prominent among such cases was physician Susan Wicklund, who faced protests and harassment, including her house being picketed for a month. The law is codified in Chapter 123 of Title 18 of the United States Code (Gorin, 2023).

This legislation is to the effect that the government has a legal obligation to protect this information from misuse. These rules are laid out specifically in Title 18 U.S. Code Section 2721 (the Drivers Privacy Protection Act or DPPA). Thus, when an officer or agent of a DMV mishandles this, it is considered a federal offense and may be punishable by fines (Gorin, 2023).

Also, the government must ensure the safekeeping of the collected data and private information while seeking vehicle licenses and protecting the information from misuse. By Section 2721 of the law,

> "*A State Department of Motor Vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity:*
> *(1) personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section; or*
> *(2) highly restricted personal information, as defined in 18 U.S.C. 2725(4), about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9): Provided, That subsection (a)(2) shall not in any way affect the use of organ*

donation information on an individual's driver's license or affect the administration of organ donation initiatives in the States."

The piece of legislation, while protecting personal information as it relates to information within the confines of the Department of Motor Vehicles, is not without exceptions. Personal information that the legislation seeks to protect includes the names and addresses, photographs, phone numbers, Social Security Numbers, Driver's License Numbers, and Health, Medical, or Disability Information and, in some circumstances, permits the use and disclosure of some information without the express consent of the owner.

These situations include legal proceedings in connection to any civil, criminal, administrative, or arbitral proceeding in any federal, state, or local court or agency or before any self-regulatory body, permission to disclose individual's personal information for motor vehicle product alterations, recalls, or advisories related to the vehicle's performance and safety, release of information about towed or impounded vehicles, investigations by a licensed private investigator, and in the case of the express consent of the owner of such information. A federal offense is committed in the event of violating this legislation, but there is no assigned prison time for such an offense. (D. Gorin, 2023). It is only punishable with fines of up to $5,000 (Five Thousand United States Dollars)

Children's Online Privacy Protection Act (COPPA) (15 U.S. Code § 6501)

Another piece of legislation addressing data privacy concerns in the United States is the Children's Online Privacy Protection Act (COPPA). The legislation, enacted in 1998 but became effective April 21, 2000, applies to the online collection of personal information by persons or entities under U.S. jurisdiction about children under 13 years of age, including children outside the U.S., if the website or service is U.S.-based. It details what a website operator must include in a privacy policy, when and how to seek verifiable consent from a parent or guardian, and what responsibilities an operator must protect children's privacy and safety online, including restrictions on the marketing of those under 13 (Gates 2022) The law which was after that revised in 2013 guides the implementation of COPPA.

The 2013 revisions to this rule "address[ed] changes in the way children use and access the internet, including the increased use of mobile devices and social networking" and "widen[ed] the definition of children's personal information to include persistent identifiers such as cookies that track a child's activity online, as well as geo-location information, photos, videos, and audio recordings (Gates 2022) As part of ensuring compliance with data protection rule and a leap, this legislation covering younger subjects ensures that they are not vulnerable to the public through the misuse of their respective data.

The Video Privacy Protection Act (18 U.S. Code § 2710

This legislation, which was enacted in pursuance of the prevention of wrongful disclosure of video tape rental or sale records or similar audio-visual materials, makes any "video tape service provider" that discloses rental information outside the ordinary course of business liable for up to $2,500 in actual damages unless the consumer has consented, the consumer had the opportunity to consent, or the data was subject to a court order or warrant. This piece of legislation enacted in 1988 ensures data protection to the extent of limiting a video service provider, as defined in the statute, from knowingly disclosing a consumer's personally identifiable information derived from their rental or purchase of, or subscription to, pre-recorded audiovisual materials or services without the consumer's informed, written consent. (Westlaw, 1988)

The Cable Communications Policy Act of 1984

The Cable Communications Policy Act of 1984 is another Federal legislation in the United States geared towards protecting sensitive data within the US Cable/Television industry. Enacted in 1984, it intends to promote competition and deregulate cable television by establishing the National Policy for regulating cable television communications by federal, state, and local authorities. By ensuring this, the distribution of data is at an optimal level, ensuring compliance with the extant laws.

The Biden-Harris Executive Order on National Cyber-security Strategy

To ensure further regulation and protection of data and sensitive information, the Biden-Harris administration developed the 2021 executive order to improve the nation's cyber-security (White House Government, 2021). The key facts about the policy are the need to ensure a re-balancing of the responsibility in defending cyberspace and realigning incentives to favor long-term investments through a more intentional, coordinated, and resourced approach to cyber-defense. Similarly, the executive order lays out principles for privacy and security in developing and deploying artificial intelligence.

- **TABLE 1- Federal Legislations on Data Privacy in the US**

S/N	NAME OF LEGISLATION	YEAR OF ENACTMENT	OBJECTIVES
1	Cable Communications Policy Act	1984	Establishment of regulations regarding franchise standards and proceeds that would attempt to strengthen the development of cable systems
2	Children's Online Privacy Protection Act (COPPA) (15 U.S. Code § 6501)	1998	give parents control over what information websites can collect from their kids
3	Drivers Privacy Protection Act 1994	1994	protect the privacy of personal information contained in an individual's motor vehicle records
4	Health Insurance Portability and Accountability Act of 1996	1996	protect the confidentiality and security of healthcare information and help the healthcare industry control administrative costs
5	The Controlling the Assault of Non-Solicited Pornography and Marketing Act (CAN-SPAM Act) (15 U.S. Code § 7701 *et seq*.)	2003	establishes requirements for those who send unsolicited commercial email. The Act bans false or misleading header information and prohibits deceptive information.
6	The Fair Credit Reporting Act (FCRA), (amended by the Fair and Accurate Credit Transactions Act (15 U.S. Code § 1681),	1618, Revised 2018	consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit
7	The Family Educational Rights and Privacy Act (20 U.S.C. § 1232g)	1974	federal law that affords parents the right to have access to their children's education records
8	The Gramm Leach Bliley Act (GLBA) (15 U.S. Code § 6802(a) *et seq*.)	1999	financial institutions – companies offering consumers financial products or services like loans, financial or investment advice, or

			insurance – must explain their information-sharing practices to their customers and safeguard sensitive data.
9	The Telephone Consumer Protection Act (TCPA) (47 U.S. Code § 227)	1991	Restricts telephone solicitations (i.e., telemarketing) and automated telephone equipment.
10	The Video Privacy Protection Act (18 U.S. Code § 2710 *et seq.*)	1988	In certain circumstances, video service providers are prohibited from disclosing personally identifiable information.

It is imperative to mention that the discussed federal legislations are all geared at ensuring sanity within the social space, coupled with the problem of abuse within the sector regarding compliance and regulations, hence the need to appreciate these legislations. However, there is a need to briefly appraise some state-related legislation on data privacy and compliance within the United States.

McAuliffe and Powers (2024) highlight various state-related legislation on privacy. As of June 2024, 19 states - California, Colorado, Connecticut, Delaware, Florida, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia - have enacted privacy laws. Many U.S. states have passed or will soon enact comprehensive privacy laws. Examples of state legislation are as follows:

- California's California Privacy Rights Act (CPRA) and Virginia's Virginia Consumer Data Protection Act (VA CDPA) became effective on January 1, 2023.
- Colorado's Colorado Privacy Act (ColoPA),
- Connecticut's Connecticut Act Concerning Personal Data Privacy and Online Monitoring (CT DPA)
- Utah's Utah Consumer Privacy Act (UCPA) followed suit on July 1, 2023.
- Texas's Texas Data Privacy and Security Act (TDPSA), Florida's Florida Digital Bill of Rights (FDBR)
- Oregon's Oregon Consumer Data Privacy Act (OCDPA) took effect for most businesses on July 1, 2024.
- Montana's Montana Consumer Data Privacy Act (MCDPA) also became effective on October 1, 2024.

In 2025, Iowa, Delaware, Nebraska, New Hampshire, New Jersey, Tennessee, and Minnesota will implement their respective privacy laws. Indiana, Kentucky, and Maryland will follow suit on January 1, 2025.

- **Table 2 states with Data Privacy Laws compared with states with no legislation in the US**

S/N	STATES	LEGISLATIONS & YEAR OF ENACTMENT	OBJECTIVES
1	Massachusetts	Massachusetts Data Privacy Act 2022	
2	New York	i. New York's Stop Hacks and Improve Electronic Data Security Act (N.Y. Gen Bus.	

		Law § 899-bb (Enacted 2019) ii. Revised Cyber-security Requirements for Financial Services Companies	
3	Illinois	Illinois Biometric Privacy Act (BIPA),	
4	Washington	The Washington My Health My Data Law (WMHMYDA)	aims to safeguard consumer health data beyond the scope of the federal Health Insurance Portability and Accountability Act (HIPAA) by regulating the collection, sharing, and selling of consumer health data by any entity conducting business or controlling or processing consumer health data in Washington.
4	California	i. California Consumer Privacy Act (CCPA) 2018, which became effective on January 1, 2020 ii. California Privacy Rights Act (CPRA) amended 2020	The law introduced new obligations on covered businesses, including requirements to disclose the categories of personal information the company collects about consumers.
5	Virginia	Consumer Data Protection Act (Virginia CDPA), 2021	
6	Colorado	Colorado Privacy Act 2021	
7	Utah	Utah Consumer Privacy Act 2022	
8	Connecticut	Connecticut Privacy Act 2022	
9	Delaware	Delaware Personal Data Privacy Act (DPDPA) 2023 (Takes effect January 1, 2025)	
10	Florida	Consumer Data Privacy Act 2023	
11	Indiana	Consumer Data Privacy Act 2023	
12	Iowa	Consumer Data Privacy Act 2023 (Takes Effect 1 January 2025)	
13	Montana	Consumer Data Privacy Act 2023	
14	Oregon	Consumer Data Privacy Act 2023	
15	Tennessee,	Consumer Data Privacy Act 2023	
16	Texas	Consumer Data Privacy Act 2023	
17	Kentucky	Consumer Data Privacy Act 2024	

18	New Hampshire	Consumer Data Privacy Act 2024	
19	New Jersey	Consumer Data Privacy Act 2024	
20	Montana	Consumer Data Privacy Act (MTCDPA)	
21	Tennessee	Tennessee Information Protection Act 2023 (Takes effect 2025)	
22	Minnesota	Minnesota Data Privacy Act (MCDPA)	
23	Maryland	i. Maryland Online Data Privacy Act (MODPA) ii. Maryland Online and Biometrics Data Privacy Act (SB698/HB 807)	
24	Nebraska	Nebraska Data Privacy Act (takes effect 2025)	
25	Rhodes Island	Rhodes Island Data Transparency and Privacy Protection Act (RIDTPPA) Enacted June 29, 2024,	

Extent and Applicability of Available Frameworks Governing Data Privacy and Compliance Regulations in the US

An assessment of extant legislation across the United States shows that, unlike many other countries, the United States lacks a single, unifying federal data protection law. At best, we have numerous federal and state laws, industry-specific legislations, and common law principles to regulate data privacy and security. While it is on record that these legislations present unique challenges for operations, the following are take-homes from the extent and applicability of these instruments as to their relevance within the data and privacy space.

The Health Insurance Portability and Accountability Act (HIPAA) governs the privacy and security of health information. There has been an impressive level of its application, as seen in the case involving the *American Medical Response (AMR),* a private ambulance company paid a $115,200 civil monetary penalty to the HHS' Office for Civil Rights (OCR) to resolve a violation of the HIPAA Right of Access. AMR failed to provide patients timely access to their medical records, taking more than a year to provide the requested documents (Alder:2024).

In another case of the violation of HIPAA involving Optum Medical Care of New Jersey, Optum Medical Care of New Jersey, formerly known as Riverside Medical Group and Riverside Pediatric Group, was a private multi-specialty physician group with approximately 150 locations in New Jersey and Southern Connecticut. In the Fall of 2021, OCR received six complaints from individuals who had not been provided with their records after sending a request to Optum Medical Care. The requests were to obtain a copy of an individual's records or requests from parents for their minor children's records. The HIPAA Privacy Rule gives individuals the right to obtain copies of their medical and minor children's medical records. When a HIPAA-covered entity receives a request, the records must be provided within 30 calendar days, although under certain limited circumstances, a 30-day extension is possible. OCR launched an investigation in February 2022 in response to the complaints and determined that Optum Medical Care had exceeded the allowed timeframe for providing those records. The complainants had to wait between 84 and 231 days to receive their requested records. Optum Medical Care chose to settle the alleged violations and agreed to pay a $160,000 financial penalty and adopt a corrective action plan (CAP) that includes reviewing and revising its policies and procedures for individual access to PHI, providing training to the workforce on those new procedures, and ensuring that all patients are provided with their requested records within 30 days. If a right of access request is denied, OCR must be informed and provided with documentation to support that denial. OCR will monitor Optum Medical Care for compliance with the CAP for one year. (S. Alder: 2024).

Secondly, the Gram-Leach Billey Act (GLBA) addresses protecting personal information with financial institutions such as banks, insurance houses, and other companies in the financial services industries (Pittman et al., 2024). This statute addresses "Non-Public Personal Information" (NPI), which includes any information that a financial service company collects from its customers concerning the provision of its services. It imposes requirements on financial service industry companies for securing NPI, restricting disclosure and use of NPI, and notifying customers when NPI is improperly exposed to unauthorized persons. (Pittman et al, 2024).

While the Federal Trade Commission is the primary body regulating and enforcing actions related to unfair and deceptive practices in the use of data, there is a need to point out salient issues. The relevant legislations have, through transparency, a lawful basis for processing and purpose limitation, ensuring that the use of data is well-regulated. Further, most statutes are delimited in terms of the rights spelled out. The HIPPA allows individuals to request copies of their medical information held by a health service provider. Still, then at the state level, the state of California, through the California Consumer Privacy Act of 2018 (CCPA), allows the resident's right to access personal information held by a business within that axis. This is further provided for by the privacy laws of Virginia, the same replicated in the Colorado Privacy Act, Utah Consumer Privacy Act, and Connecticut Privacy Act (Pittman et al., 2024).

There is also the need to mention that some sector-specific statutes address the right to deletion and the right to be forgotten. This is well illustrated in the Children's Online Privacy Protection Act (COPPA) (15 U.S. Code § 6501), which prohibits the collection of any information from a child under the age of 13 online and from digitally connected devices and requires publication of privacy notices and collection of verifiable parental consent when information from children is being collected. This legislation further addresses and allows parents to review rights and delete their children's information on public databases. (Pittman et al, 2024).

Many states have enacted laws to protect consumer privacy. For example, California's CCPA and Nevada's Privacy Law allow residents to stop businesses from selling their personal information. Recent laws in Virginia, Colorado, and Connecticut allow consumers to limit how their data is used for targeted ads, personalized profiles, and sales. California's CCPA also will enable consumers to opt out of processing sensitive data, like health or financial information, except in specific cases. Utah's law is more limited, focusing on preventing the sale of personal information and using data for targeted ads. (Pittman et al, 2024). The U.S. lacks a centralized data protection authority.

As a result, enforcement mechanisms vary by statute. Some laws are enforced solely by the federal government, while others involve federal and state officials or private lawsuits. Penalties can be civil, criminal, or both. For example, HIPAA violations can lead to civil and criminal sanctions enforced by the HHS, state Attorneys General, and the DOJ. The CPPA, on the other hand, empowers the California Privacy Protection Agency (CPPA) to enforce consumer rights and business obligations under the CPRA. Further, depending on the applicable data protection laws, regulators in the U.S. may have the authority to conduct investigations into potential violations of data protection requirements.

The Need for Centralised Data Privacy and Compliance Regulations within the United States

The need for centralized data privacy and compliance regulation within the United States is a complex issue with solid arguments on both sides. Arguments have favored a centralized data protection regulation, which will be addressed below.

One of them is the need for consistency and predictability. The need for a comprehensive federal data privacy law cannot be overemphasized. It would provide a clear, consistent, and regular framework for businesses and institutions, reducing compliance costs and legal uncertainty. As government response to data collection creates concerns and breaches continue, contemporary US data privacy regulations, starting with California's ground-breaking CCPA, have pushed from an enterprise-as-owner-of-data approach to a consumer rights-centric model (Bower, 2020).

This adds a massive list of new processes to the already stressed compliance budget. The right to deletion, the consumer right to data, children's data handling, new data safeguards and de-identification, data minimization, and retention policy loom large on the compliance roadmap. With each state creating its respective "CCPA" variation, the regulatory matrix for compliance gets more expensive to meet. A central enforcement body could bring a cohesive approach to compliance that could ease its implementation, assuming laws remain strong and in line with threats – which is critical. Avoiding State-by-State privacy compliance is desirable and potentially a way to fuel more straightforward privacy budget requests for CISOs. However, that cannot come at the expense of dilution of intent and, ultimately, protecting the weary and oft-breached American consumer (Bower, 2020).

Flowing from this, it is in place to say that a centralized approach could lead to more robust consumer protections and greater accountability for companies that mishandle personal data, and a unified U.S. data privacy law could help American businesses compete more effectively in the global market, where many countries have already adopted comprehensive data protection regulations (Reis et al., 2024). The United States, for instance, relies on a sectoral approach, with different laws governing specific industries and no overarching federal privacy law. This diversity in approaches creates challenges for multinational businesses and raises questions about the consistency and adequacy of privacy protection globally (Reis et al., 2024).

Similarly, a unified U.S. data privacy law could help American businesses compete more effectively in the global market, where many countries have already adopted comprehensive data protection regulations. This is necessary to ensure uniformity and a certain level of joint consensus on data privacy rights among various states in the United States. The intricate web of state laws, often contradictory and burdensome, coupled with the sheer volume of legal and regulatory requirements in the United States, imposes significant financial strain on enterprises. This leads to increased operational costs and may indirectly impact consumers through potential non-compliance penalties or the transfer of these costs onto them. Moreover, this complex regulatory landscape hinders the achievement of crucial objectives such as safeguarding end-user privacy, empowering individuals with control over their data, promoting transparency and education regarding data usage, and ensuring that privacy laws and policies remain adaptable to the ever-evolving technological landscape. The disparate nature of these state privacy laws further exacerbates the issue, resulting in inconsistent standards and controls. To address these challenges, the United States urgently requires a unified, federal-level approach that supersedes state laws, bringing clarity, simplification, and a common-sense solution to the data privacy environment. (Nix, 2020)

Notwithstanding the need for a centralized data privacy law within the United States, arguments have also been against centralized legislation. One of the leading arguments boils down to halting the innovation that various states have deployed in the model of their data privacy laws, and any states have been at the forefront of data privacy legislation, creating innovative solutions that may not be captured in a one-size-fits-all federal law (Nix, 2020). The debate over the need for centralized data privacy and compliance regulation in the United States is ongoing. While strong arguments exist on both sides, the current patchwork of laws presents challenges for businesses and consumers alike. A well-crafted federal law could provide much-needed clarity and consistency. Still, ensuring that such a law strikes the right balance between protecting consumer privacy and promoting innovation is essential.

However, there are steps to be taken to ensure that the United States creates a comprehensive national framework for data privacy, which is to be known as the American Privacy Rights Act. The Proposed American Privacy Rights Act of 2024 seeks to establish national consumer data privacy rights, govern Artificial Intelligence and automated decision-making, impose additional obligations on high-impact social media companies and large data holders, supersede state privacy laws, and allow a private right of action (Anderson et al., 2024)

The proposed law (ARPA) is to apply to business, health sectors, and other areas in charge of data. The APRA aims to establish a uniform national data privacy and security standard and "expressly pre-empt laws of a State or political subdivision. Under the APRA, subject to limited exceptions, no state could adopt,

maintain, or enforce any law, regulation, rule, or requirement covered or promulgated by the APRA. The APRA clarifies that specific state laws or provisions would be exempt from pre-emption, for example, consumer protection laws of general applicability, civil rights laws, provisions that address (a) the privacy rights or other protections of employees or students, or (b) notification requirements in the event of a data breach, contract or tort law; specific criminal and civil laws (e.g., on blackmail, cyberbullying, child abuse); (vi) public safety laws; and laws that protect the privacy of health information. (Anderson et al, 2024)

This piece of legislation is expected to have a unifying characteristic and replace a plethora of legislation that has made its way into the data regulation sector.

Conclusions and Recommendations

The United States lacks a unified, comprehensive data privacy law, resulting in a complex patchwork of federal and state regulations. This fragmented approach poses challenges for businesses, consumers, and regulators alike. While state-level innovation has driven advancements in data privacy, a centralized federal framework could offer several benefits, including greater consistency, stronger consumer protections, and improved international competitiveness. However, such a framework must be carefully designed to avoid excessive burdens on businesses and ensure it aligns with innovation and economic growth principles.

The following recommendations are made:

- Comprehensive Framework: Enact a comprehensive federal data privacy law that provides a clear and consistent regulatory framework for businesses
- Strong Consumer Protections: Prioritize substantial consumer privacy rights, including the right to access, correct, and delete personal data.
- Robust Enforcement Mechanisms: Establish effective enforcement mechanisms, such as civil penalties and criminal sanctions, to deter non-compliance.
- Data Breach Notification Requirements: Mandate timely notification of data breaches to affected individuals and regulatory authorities.
- Privacy by Design: Encourage the adoption of privacy-by-design principles to embed privacy protections into developing and deploying technologies.
- State-Federal Collaboration:
- Harmonization: Foster collaboration between federal and state regulators to harmonize regulations and avoid conflicting requirements.
- Shared Best Practices: Facilitate sharing best practices and lessons learned among different jurisdictions.
- International Cooperation:
- Global Standards: Engage with international partners to develop common data privacy standards and facilitate cross-border data flows.
- Mutual Recognition Agreements: Explore opportunities for mutual recognition of compliance with data privacy regulations between the U.S. and other countries.
- Industry Self-Regulation:
- Industry Codes of Conduct: Encourage industry self-regulation by developing and adopting robust industry codes of conduct.
- Privacy Certifications: Support the development of privacy certification programs to recognize organizations that demonstrate strong privacy practices.

References

1. Alder S, (2024) *American Medical Response Pays $115k Civil Monetary Penalty for HIPPA Violation*, The HIPPA Journal, (2024)
2. Bower M. (2020), Is the US Ready for Centralized Data Privacy Enforcement? (Comforte Blog-February 18, 2020) Retrieved from https://insights.comforte.com/is-the-us-ready-for-centralized-data-privacy-enforcement

3. Buckbee M. (2024), Data Privacy Guide: Definitions, Explanations, and Legislations, Retrieved from https://www.varonis.com/blog/data-privacy
4. Davis M. (2024) What is Data Privacy Compliance and How can you Achieve it? Retrieved from https://www.osano.com/articles/data-privacy-compliance#:~:text=Data%20privacy%20compliance%20refers%20to,concerning%20their%20users'%20private%20information.
5. Faster Capital (2024). "Data Explosion: Fuelling Exponential Growth in the Digital Age" Retrieved from https://fastercapital.com/content/Data-Explosion--Fueling-Exponential-Growth-in-the-Digital-Age.html
6. Gates K & l, (2022) Children's Online Privacy Protection Act (COPPA) of 1998: Protection for the US's Youngest Data Subjects, Retrieved from https://www.ediscoverylaw.com/2022/12/09/childrens-online-privacy-protection-act-coppa-of-1998-protection-for-the-uss-youngest-data-subjects/
7. Gorin D, (2023) Drivers Privacy Protection Act 18 U. S. Code § 2721 Available at https://www.thefederalcriminalattorneys.com/drivers-privacy-protection-act#:~:text=18%20U.S.C.,in%20manners%20permissible%20by%20law. Accessed 29th November, 2024
8. Law Insider, *Data Definition,* Retrieved from https://www.lawinsider.com/dictionary/data?cursor=ClESS2oVc35sYXdpbnNpZGVyY29udHJhY3Rzci0LEhpEZWZpbml0aW9uU25pcHBldEdyb3VwX3Y1MSINZGF0YSMwMDAwMDAwYQyiAQJlbhgAIAA%3D
9. McAuliffe B. E. & Powers M. G., (Lewis Rice LLC: 2024) Data Protection: U.S. State Privacy Laws, Retrieved from https://www.lewisrice.com/u-s-state-privacy-laws/
10. Murphy U. M., (2015) United States: Privacy and Data Protection, (Masters Thesis: University College Cork)
11. Pittman F. P., Hafiz A. & Hamm A (White & Case LLP),(2024), Data Protection Laws and Regulations USA 2024, Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
12. Pittman F. P., Hafiz A. & Hamm A.,(2024), Data Protection Laws and Regulations USA 2024, Retrieved from https://iclg.com/practice-areas/data-protection-laws-and-regulations/usa
13. SNIA- Experts on Data (2024), What is Data Privacy? Retrieved from https://www.snia.org/education/what-is-data-privacy
14. The Law Dictionary, (2024), Retrieved from https://thelawdictionary.org/comply/
15. WestLaw (1988), Video Privacy Protection Act of 1988 (VPPA), Retrieved at https://content.next.westlaw.com/Glossary/PracticalLaw/I21063f17ef0811e28578f7ccc38dcbee?transitionType=Default&contextData=(sc.Default)
16. White House Government (2021), *Executive Order on Improving the Nation's Cyber-Security*, Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/

Author Profile

Olumide Ajayi is a data privacy and regulatory compliance expert with a strong professional and academic background in data privacy, regulatory compliance, intellectual property, and corporate practice. He is a dual-qualified attorney licensed to practice law in the Federal Republic of Nigeria and New York, USA. He obtained his master's degree with a concentration in Corporate Commercial and International Trade from the University of Illinois, Urbana-Champaign, with high honors. He has practiced data privacy and regulatory compliance in reputable institutions.