WEP Warwick Evans Publishing

International Journal of Social Sciences and Public Administration

ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 6, Number 1, Year 2025
DOI: https://doi.org/10.62051/ijsspa.v6n1.22
Journal homepage: https://wepub.org/index.php/IJSSPA/index

Regulatory Responses to Data Breaches: Evaluating the Effectiveness of GDPR and CCPA in Consumer Protection

Leonardo W Ou

University of California, Irvine, California, USA

ABSTRACT

In the digital age, data breaches have become a significant threat to consumer privacy, prompting the implementation of stringent data protection regulations worldwide. This paper evaluates the effectiveness of two prominent regulatory frameworks, the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in the United States, in safeguarding consumer data and responding to data breaches. Through a comparative analysis of their key provisions, enforcement mechanisms, and real-world impacts, the study examines how these regulations address consumer rights, data access, and control. The research employs a mixed-methods approach, analyzing case studies of major data breaches under each framework, including the 2018 British Airways breach (GDPR) and the 2020 Zoom breach (CCPA). Findings reveal that GDPR, with its broader scope, stringent enforcement, and higher penalties, offers a more comprehensive and proactive approach to data protection compared to the CCPA, which is more localized and reactive. The study highlights the challenges and limitations of each framework, emphasizing the need for ongoing refinement to address emerging technological and cybersecurity threats. The paper concludes that GDPR serves as a global benchmark for data protection, while the CCPA represents a significant but narrower step toward enhancing consumer privacy in the U.S. Future research should explore the adaptability of these regulations to new technologies and their socio-economic impacts on businesses, particularly small and medium-sized enterprises.

KEYWORDS

Privacy Regulations; Data Breaches; Consumer Protection; Data Privacy; Enforcement Mechanisms.

1. INTRODUCTION

In the digital age, data-driven technologies have significantly changed the global economy, placing personal data at the core of business strategies across multiple sectors. This has led to the importance of established data protection policies, as breaches in personal data can cause serious privacy violations that affect millions of people around the world every year. Recognizing the potential risks associated with mishandling personal data, regions around the world have instituted different data protection laws aimed at safeguarding personal information and contributing public trust in digital systems.(Souza et al., 2020) The most representative of these are the General Data Protection Regulation (GDPR) in the European Union and the California Consumer Privacy Act (CCPA) in California, United States. These regulations aim to re-empower consumers, strengthen their control over personal data, and impose obligations on entities that collect, process and store personal data.(Georgiou & Lambrinoudakis, 2020).

The GDPR, implemented across all EU member states, has set a high benchmark for data protection worldwide. On the other side of the Atlantic, the CCPA provides similar protections for residents of

California with more general requirements.(Mazumdar et al., 2023) The enactment of the CCPA has triggered broader discussions within the United States, encouraging other states to consider or enact similar legislation.

Despite these two originating from different legislative environments, one as a supranational regulation and the other as a state-specific law within the United States, but both the GDPR and the CCPA are aimed to address the critical issue. Analyzing these regulations side by side not only because of their global impact but also helps in understanding how localized legislation like the CCPA can influence and perhaps set a precedent for other states or even federal data protection laws in the U.S., which they both also lead in the world. Both the GDPR and CCPA represent different approaches in the evolution of data protection regulations.(Naqvi & Batool, 2023)(Voss et al., 2023) However, despite their importance, questions remain about their effectiveness in practice, especially in relation to enforcement and compliance after data breaches. This paper will look into these regulations, comparing their enforcement mechanisms, and the real-world examples to show the implications on businesses and consumers, and will focus on investigate to following key questions:

- What are the key provisions of GDPR and CCPA? How do they differ in terms of consumer rights, data access, and control?
- Since the implementation of GDPR and CCPA, what tangible impacts have been observed on consumer protection? What are the reported outcomes or breaches, and how have these laws addressed them?
- How do the mechanisms of enforcement and compliance under GDPR compare with those under CCPA? Which has shown more effectiveness in real-world scenarios?
- What are the primary challenges or limitations faced by each regulatory framework in fully protecting consumer rights during data breaches?

Through the review of current literature, analysis of case studies, and synthesis opinions to answer these research questions, the research can provide valuable insights for policymakers, businesses, and consumers.

2. METHODOLOGY

Table 1. The comparison of CCPA and GDPR in regulations and key provisions

Dimension of Efficacy	Indicator (Already in Place)	Assessment Criteria	Which Policy is More Effective?
Data Protection Coverage	Scope of application; Types of data covered	Coverage comparison with global data protection standards	GDPR has broader coverage than CCPA provides more extensive data protection, especially in terms of global reach and types of data covered.
Machanism	Number and nature of enforcement actions; Fines imposed	Analysis of enforcement actions and their outcomes	GDPR due to higher fines and stricter enforcement
Compliance Ease	Survey of organizational efforts and costs for compliance	CCPA requires less stringent compliance efforts	CCPA offers easier compliance for business due to its more focused scope within California.
Consumer Empowerment	Number of cons and control mechanisms	Consumer feedback on data control and rights	GDPR, with more comprehensive consumer rights

This research will utilize two approaches to assess the effectiveness of regulatory responses to data breaches under the GDPR and the CCPA. The study will conduct a general comparison of the two regulations and their key provisions, followed by an analysis of two major data breach cases under each regulatory framework to elaborate outcome indicators and output indicators. Outcome indicators measure the ultimate effectiveness of the policies in achieving their objectives, such as reducing the number of data breaches, increasing the security of consumer data, and improving overall consumer confidence in digital transactions. The research also designed a set of metrics to be used to evaluate the scope and impact of these breaches, as well as the effectiveness of regulatory enforcement in enhancing consumer protection.

2.1. Comparative Analysis

This section will also be divided into two key parts to analyze the regulatory frameworks of GDPR and CCPA, focusing on real-world impacts such as breach frequency, fines, financial losses, and corporate investment in compliance.

2.1.1. Comparative Policy Analysis

The following indicators are selected to show the fundamental differences and similarities in the provisions of each regulation and include:

(1)Indicators for comparing provisions:

- Scope of Application
- Rights Granted to Individuals
- Obligations for Businesses
- Enforcement and Fines

This section of the methodology is structured to analyze and compare the impacts of GDPR and CCPA, focusing on the differences in their effectiveness in dealing with data breaches. The comparison will focus on how frequently breaches are reported, the magnitude of those breaches, the size of fines imposed, the financial losses companies experience, and type of data affected.

2.1.2. Comparison of Investment and Losses Across Companies

To further understand the effectiveness between GDPR and CCPA, the study examined the frequency of incident types reported, focusing on identifying patterns in data breaches and regulatory non-compliance. The analysis was conducted using a structured approach to ensure consistency and comparability across both frameworks. Reports were selected based on their relevance to GDPR and CCPA enforcement actions, prioritizing those that provided detailed descriptions of incidents, regulatory responses, and outcomes. Metrics were carefully defined to capture the nature and scope of incidents, allowing for meaningful comparisons. These companies will be chosen from different sectors, technology, finance, education, communication, and healthcare.

The primary metric analyzed was the type of incident, categorized into groups such as "Unauthorized Processing," "Data Breach," "Phishing," and "Ransomware." Each report was reviewed to extract this information, along with supporting metrics such as the number of individuals affected, the timeline from discovery to notification, fines imposed, and reported misuse of data.

The dataset was organized into fields for regulation type (GDPR or CCPA), incident type, and frequency of occurrence. Cases were grouped by regulation, and the frequency of each incident type was counted. For GDPR, the data included categories such as "Consent Violation" and "Insufficient Security," while CCPA cases featured incidents like "Unauthorized Access" and "Ransomware." This organization ensured that diverse incident types were consistently categorized for comparison.

The analysis focuses on the key differences between GDPR and CCPA enforcement priorities, as reflected in the types and frequencies of incidents. Although the findings are limited to the scope and granularity of the reports reviewed, the selection and processing of data ensured the reliability and relevance of the results.

2.2. Comparison of Two Major Data Breach Cases under Different Regulatory Frameworks

The cases will be selected based on several criteria, including the size of the breach, the severity of the breach, and the regulatory response. This analysis is also based on the assumption that their differences are attributable to policy. The following cases will be analyzed:

- GDPR Case:
    - **British Airways Data Breach (2018)**: Involving the theft of personal and financial information of approximately 500,000 customers. This case is notable for the £183 million fine imposed by the UK's Information Commissioner's Office (ICO) under the GDPR.
- CCPA Case:
    - Zoom Data Breach (2020): Impacting millions of users, this case involved the exposure of personal information due to security flaws. The California Attorney General's office pursued penalties under CCPA.

For each case, the following data will be collected:

- Level of breach: Size of the breach in terms of the number of individuals affected, the sensitivity of the compromised data.
- Regulatory response: Speed and effectiveness of the regulatory authorities in responding to the breach, including the timeliness of breach notification, investigations, and the imposition of fines or corrective actions.
- Consumer protection input: The actions taken by the companies to comply with GDPR or CCPA requirements.
- Fines and penalties: The size of the fines imposed, either as a percentage of the company's global turnover or a flat statutory fine.
- Compliance efforts post-breach: The corrective post-breach actions taken by the companies to comply with GDPR or CCPA requirements.

3. LITERATURE REVIEW DISCUSSION AND ANALYSIS

The implementation of the GDPR and the CCPA represents a significant shift in the paradigm of data protection globally. These regulations not only aim to enhance consumer privacy but also impose standards and practices for data handling by organizations, large and small.(Voss et al., 2023)

The GDPR, particularly, has set a high benchmark globally with its comprehensive and stringent requirements. One of its most impactful provisions is the requirement for explicit consent before personal data can be processed.(General Data Protection Regulation (GDPR), 2024) This has fundamentally changed how organizations interact with EU citizens, requiring transparent communication about the use and purpose of data collection. Furthermore, GDPR introduced the 'right to be forgotten,' empowering individuals to have their data erased from a company's records under specific conditions.(Naqvi & Batool, 2023) This provision is crucial in an age where digital footprints are expansive and potentially everlasting.

The regulation also mandates that businesses implement data protection by design and by default, meaning that privacy settings must be set at high levels by default, and data protection measures must be integrated into the development phase of products and services. This proactive approach is a departure from the more reactive stances seen in earlier regulations.

On the other hand, the CCPA, while not as broad in scope as GDPR, has introduced significant changes within the U.S., particularly affecting companies that deal with large volumes of personal data.(James et al., 2023) It provides California residents with the right to know what personal data is being collected about them, whether it is being sold or disclosed, and to whom. Additionally, the CCPA allows consumers to opt-out of the sale of their personal data, a provision that has prompted businesses to modify their data practices substantially.(California Consumer Privacy Act (CCPA), 2023)

Both regulations also share a focus on children's data, with strict rules governing the processing of information belonging to minors. The GDPR sets the age of consent for data processing at 16 (which can be lowered to 13 by member country), requiring parental consent for data processing activities involving younger children.(Article 8 EU General Data Protection Regulation (EU-GDPR). Privacy/Privazy According to Plan., 2023) Similarly, the CCPA prohibits the sale of children's information (for minors under 16) without explicit consent, reflecting growing concerns about the vulnerability of young individuals online.

The effectiveness of these regulations, however, has been mixed. In Europe, GDPR has been critiqued for its uneven enforcement. While some countries have pursued vigorous enforcement, others have been less active, which undermines the uniformity and overall efficacy of the regulation across the EU.(Naqvi & Batool, 2023) Similarly, in the U.S., the CCPA's impact is evolving, with businesses and regulators still navigating the complexities of its implementation. Some critics argue that the lack of federal regulation leads to a patchwork of state laws that may hinder comprehensive consumer protection.

Moreover, the financial implications for non-compliance under these regulations are significant, designed to incentivize organizations to prioritize data protection. Under GDPR, fines can reach up to 4% of an organization's global annual turnover or €20 million, whichever is greater. In practice, some of the largest fines have reached hundreds of millions of euros, reflecting serious violations and the importance the EU places on protecting personal data.(GDPR Enforcement Tracker Report, 2024) In contrast, the CCPA's penalties are less severe but still represent a considerable financial risk for businesses, particularly in instances of intentional breaches and mishandling of data.

As data continues to be an essential asset in the digital economy, the ongoing development and refinement of these laws will be crucial in addressing emerging challenges such as advancements in artificial intelligence, machine learning, and the increasing sophistication of cyber threats. Both GDPR and CCPA are likely to serve as templates for future legislation globally, influencing how personal data is protected and managed around the world.

4. REGULATORY IMPACTS THROUGH QUANTITATIVE ANALYSIS

This section presents findings on the impact of GDPR and CCPA on business practices, using a mixed-methods approach to compare key metrics like breach frequency, data sensitivity, fines, and financial losses, as well as regulatory scope and data coverage. It includes analyses of two major breaches, the 2018 British Airways breach (GDPR) and the 2020 Zoom breach (CCPA), focusing on breach scale, regulatory response, and consumer protection.

4.1. Comparative Analysis

4.1.1. Comparative Policy Analysis

The analysis of the GDPR and the CCPA shows there are significant differences in their scope, rights afforded to individuals, obligations for businesses, and enforcement mechanisms, all of which contribute to a pronounced disparity in their effectiveness in protecting consumer data and managing data breaches.

The GDPR grants a broader array of rights to individuals, including data portability and stringent controls on automated decision-making, which are pivotal in today's data-driven landscape. These provisions not only enhance consumer control over personal data but also reinforce the accountability of data processors and controllers, thereby fostering greater transparency and trust between consumers and companies.

On the obligations front, GDPR imposes rigorous requirements on businesses to integrate data protection measures from the inception of design processes, thereby embedding data privacy into the fabric of organizational operations. This proactive approach is more robust compared to the CCPA's more reactive measures, which primarily focus on post-data-collection disclosures and maintaining reasonable security practices.

Enforcement under GDPR is notably more stringent, with penalties that can be crippling for businesses that fail to comply. The potential fines under GDPR, which is up to 4% of annual global turnover or €20 million, far exceed those under the CCPA, thereby underscoring the seriousness with which data protection is regarded in the EU.

Indicators for comparing provisions:

Table 2. Similarities and differences between CCPA and GDPR features

Feature	GDPR	CCPA	Similarities	Differences
Scope of Application	Applies to all companies processing the data of EU citizens, regardless of the company's location.	Applies to for-profit entities doing business in California and meeting specific criteria.	Both apply to entities outside their jurisdictions if they process data of covered individuals.	GDPR is broader in terms of the type of entities covered and has a global reach.
Rights Granted to Individuals	Rights to access, rectify, erase data; restrict processing; data portability; object to processing; rights related to automated decision making including profiling.	Rights to know about personal data collected, disclosed, or sold; access and delete personal data; opt-out of the sale of personal data.	Both grant rights to access and delete personal data.	GDPR offers more comprehensive rights, including data portability and restrictions on automated decision making.
Obligations for Businesses	Must implement measures that meet principles of data protection by design and default; conduct impact assessments; ensure data protection across data transfers outside the EU.	Must provide disclosures at the point of collection and maintain reasonable security procedures and practices.	Requirement for proactive data protection measures and transparency.	GDPR has stricter requirements for data protection measures and detailed impact assessments.
Enforcement and Fines	Fines up to 4% of annual global turnover or €20 million, whichever is higher, for the most serious infringements.	Maximum fine of $7,500 per violation in cases of intentional violation and $2,500 per violation otherwise.	Both enforce significant fines and penalties to ensure compliance.	GDPR imposes far higher penalties, reflecting its broader scope and emphasis on compliance.

Source: CCPA and GDPR

4.1.2. Comparison of Investment and Losses Across Companies

The comparison between GDPR and CCPA highlights significant differences in the scale of impact, enforcement mechanisms, and regulatory outcomes. GDPR cases, on average, involve a far greater number of individuals affected (502,536 compared to 6,950 under CCPA).

GDPR's enforcement is marked by substantial financial penalties, with an average fine of €12,134,600 and a total of €60,673,000 across cases. These fines serve as a powerful deterrent, emphasizing GDPR's focus on holding organizations accountable for large-scale non-compliance. By comparison, no fines were reported in the analyzed CCPA cases, suggesting a less punitive approach that may rely more on encouraging remedial measures than imposing financial sanctions.

While GDPR's average notification time is longer (76.67 days compared to 26.4 days for CCPA), this may reflect the complexity of the larger incidents it addresses. However, both frameworks share a maximum notification time of 183 days in extreme cases.

Table 3. Comparison of GDPR and CCPA by Incident Metrics

Metric	GDPR	CCPA
Avg Individuals Affected	502,536	6,950
Total Individuals Affected	2,512,678	69,500
Avg Fines (EUR)	€12,134,600	Not Applicable
Total Fines (EUR)	€60,673,000	0
Avg Time to Notify (Days)	76.67	26.4
Max Time to Notify (Days)	183	183
Total Reported Misuse	1	4
Unique Incident Types	Unauthorized Processing, Insufficient Security, Data Loss, Consent Violation, Data Breach	Unauthorized Access, Ransomware, Data Exposure, Phishing

Overall, GDPR's emphasis on significant fines, its application to large-scale incidents, and its rigorous standards for data protection underscore its strong enforcement capabilities and global reach. This positions GDPR as a leading model for data privacy regulation, particularly for addressing complex, high-impact cases. In contrast, CCPA's faster notification and focus on economic growth may be more suited to addressing local or medium-scale issues, albeit with less emphasis on financial deterrence.

4.2. Comparison of Two Major Data Breach Cases under Different Regulatory Frameworks

The data breaches involving Zoom Video Communications and British Airways reveal distinct patterns in terms of severity, regulatory response, and post-breach compliance. Zoom's breach, which

gained public attention in early 2020, affected an estimated millions of users and involved unauthorized data sharing with third parties and misrepresentation of encryption standards. In contrast, British Airways' 2018 breach compromised the sensitive personal and financial information of 500,000 customers, including payment card data with CVV numbers, highlighting a greater focus on financial data in the latter case. Regulatory responses differed significantly; the Federal Trade Commission (FTC) investigated Zoom, resulting in an $85 million settlement and commitments to improve security practices by November 2020. Meanwhile, the UK's Information Commissioner's Office (ICO) promptly investigated British Airways, ultimately issuing a £20 million fine in October 2020, reduced from an initially proposed £183 million.

The speed of notification was a crucial differentiator, with British Airways notifying the ICO promptly after discovery, while timelines for Zoom's breach disclosures remain unclear. In terms of consumer protection, both companies took significant measures post-breach. Zoom implemented enhanced encryption, initiated regular security reviews, and provided employee training, reflecting a broader focus on user trust. British Airways concentrated on network security upgrades, real-time monitoring, and response systems to prevent future incidents. The financial penalties also underscore the impact: Zoom's $85 million settlement was accompanied by substantial legal fees, while British Airways' £20 million fine represented approximately 1.5% of its global turnover in 2017, emphasizing the scalability of GDPR-enforced fines. Collectively, these cases highlight the varying nature of data breaches and the tailored regulatory and corporate responses required to address the unique challenges posed by different types of data compromise.

Table 4. Comparison of different aspects of the two cases

Aspect	Zoom Video Communications	British Airways (BA)
Level of Breach	Estimated millions affected; unauthorized data sharing with third parties; lack of encryption	500,000 customers affected; names, addresses, emails, and payment card data (including CVV) exposed
Date Reported	Early 2020; privacy and security issues gained public attention	September 6, 2018; promptly reported to ICO
Regulatory Response	FTC investigation; $85M settlement announced in November 2020; commitment to improve security practices	ICO investigation; initially proposed £183M fine reduced to £20M in October 2020
Speed of Notification	Timelines not disclosed in available sources	Promptly notified ICO upon discovery of the breach
Consumer Protection Actions	Commitments to enhanced end-to-end encryption, regular security reviews, and employee training on data handling	Implemented stronger network security measures, real-time monitoring, and response systems
Fines and Penalties	$85M settlement, with up to $21.25M allocated for attorneys' fees	£20M fine, representing about 1.5% of BA’s global turnover in 2017
Post-Breach Compliance	Launched a comprehensive security program, including transparency on third-party data sharing and enhanced encryption	Upgraded infrastructure; introduced ongoing security assessments and regular audits to prevent recurrence

Source: British Airways Penalty Notice and In re: Zoom Video Communications, Inc. Privacy Litigation, N.D. Cal. Master Case No. 3:20-cv-02155-LB.

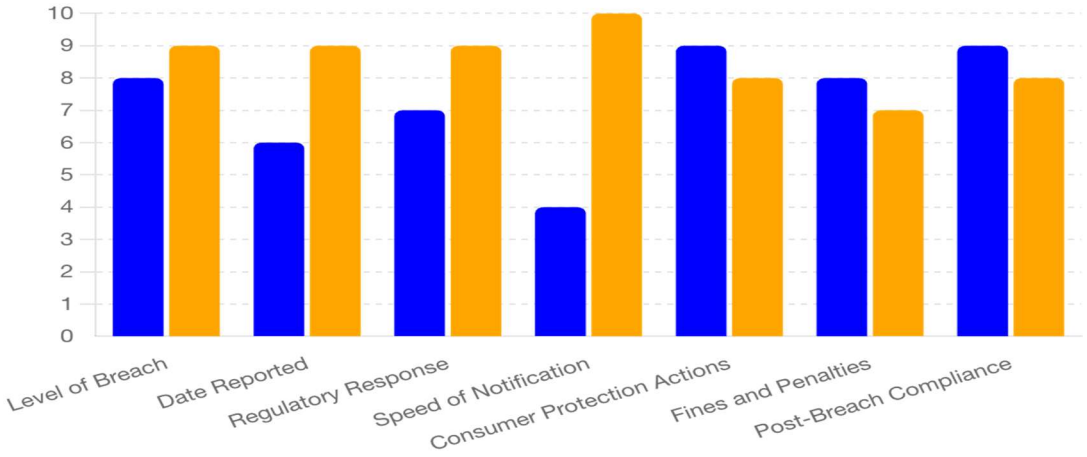

Figure 1. Comparison of different indicators in two cases

Source: Author's illustration based on data from British Airways Penalty Notice and In re: Zoom Video Communications, Inc. Privacy Litigation, N.D. Cal. Master Case No. 3:20-cv-02155-LB

5. CONCLUSION

The analysis between the GDPR and the CCPA with substantial differences in their approach to data protection, with GDPR establishing a more stringent and comprehensive framework. The GDPR's broader scope and rigorous enforcement mechanisms offer a higher level of consumer protection and compliance consistency across the European Union. Its provisions for explicit consent, rights to data portability, and the right to be forgotten are crucial in empowering individuals, ensuring they have significant control over their personal data. Additionally, the obligation for organizations to integrate data protection from the design phase of products and services shows GDPR's proactive approach towards data security.

On the other hand, the CCPA, while advancing consumer privacy rights within California, exhibits a narrower focus. It primarily enhances transparency and control over personal data after collection, particularly targeting the sale of personal information. The CCPA's penalties and targeted applicability to certain for-profit entities suggest a more localized and less severe regulatory impact compared to the GDPR. This difference in the scale and depth of provisions underlines the CCPA's role as a significant but less comprehensive approach to data protection.

The analyses in sections 4.1.2 and 4.2 reveal that GDPR and CCPA result in distinct corporate practices driven by their regulatory frameworks. Under GDPR, organizations are compelled to adopt robust, proactive data protection measures due to its comprehensive scope, stringent penalties, and requirements for compliance by design. Businesses often embed privacy mechanisms at the initial stages of product and service development, invest heavily in security infrastructure, and conduct regular audits to ensure adherence to the regulation's demands.

Conversely, the CCPA's more targeted and reactive focus influences companies to concentrate on data transparency and consumer opt-out mechanisms. For example, businesses subject to CCPA are primarily concerned with maintaining reasonable security practices and providing clear data collection disclosures. This often leads to investments in user interfaces that facilitate consumer control over data, such as "Do Not Sell My Information" options, rather than the broader systemic changes encouraged under GDPR.

However, this study may be subject to several limitations that should be acknowledged. Firstly, the analyzed cases might lack representativeness, given the limited selection of incidents and the scope of available data. This restriction could hinder the generalizability of the findings, as the selected breaches might not encompass the full range of scenarios encountered under GDPR or CCPA.

Secondly, the reliance on publicly available enforcement reports and regulatory responses may introduce biases, as these sources might not comprehensively capture all enforcement actions or corporate compliance efforts. Additionally, the study focuses on measurable outcomes such as fines and notification timelines, which, while important, might overlook less tangible impacts like shifts in organizational culture or consumer trust.

In conclusion, the GDPR provides a more high standard model for data protection legislation globally due to its extensive consumer rights, stringent compliance requirements, and severe penalties for violations. These factors contribute to a more secure and trustworthy data environment.

Future research should explore the adaptability of data protection regulations like GDPR and CCPA to emerging technologies such as artificial intelligence, blockchain, and quantum computing, as these advancements could pose new challenges to data privacy. Additionally, examining the socio-economic impact of compliance on small and medium-sized enterprises (SMEs) can shed light on the balance between regulatory requirements and operational feasibility. Comparative studies across diverse jurisdictions, including Asia, South America, and Africa, could offer valuable insights into global best practices and inform the development of harmonized international standards.

REFERENCES

[1] "California Consumer Privacy Act (CCPA)." State of California - Department of Justice - Office of the Attorney General, 15 Oct. 2018, https://oag.ca.gov/privacy/ccpa.

[2] de Souza, Jonatas S., et al. "The General Law Principles for Protection the Personal Data and Their Importance." Computer Science & Information Technology (CS & IT), AIRCC Publishing Corporation, 2020, pp. 109–20, https://aircconline.com/csit/papers/vol10/csit101110.pdf.

[3] European Parliament and Council of the European Union. "General Data Protection Regulation (GDPR) – Legal Text." General Data Protection Regulation (GDPR), 13 July 2016, https://gdpr-info.eu.

[4] Georgiou, Dimitra, and Costas Lambrinoudakis. "Compatibility of a Security Policy for a Cloud-Based Healthcare System with the EU General Data Protection Regulation (GDPR)." Information, vol. 11, no. 12, Dec. 2020, https://doi.org/10.3390/info11120586.

[5] Information Commissioner's Office. British Airways Penalty Notice. 16 Oct. 2020, https://ico.org.uk/media/action-weve-taken/mpns/2618421/ba-penalty-20201016.pdf.

[6] Joren, Hailey, et al. "Participatory Personalization in Classification." arXiv.Org, 8 Feb. 2023, https://arxiv.org/abs/2302.03874.

[7] Mazumdar, Torsha, et al. "Are Current CCPA Compliant Banners Conveying User's Desired Opt-Out Decisions? An Empirical Study of Cookie Consent Banners." arXiv.Org, 2 Sept. 2023, https://arxiv.org/abs/2309.00776.

[8] Naqvi, Syed Khurram Hussain, and Komal Batool. "A Comparative Analysis between General Data Protection Regulations and California Consumer Privacy Act." Journal of Computer Science, Information Technology and Telecommunication Engineering, vol. 4, no. 1, Mar. 2023, pp. 326–32, https://doi.org/10.30596/jcositte.v4i1.13330.

[9] Runte, Christian, et al. "GDPR Enforcement Tracker Report." CMS Law.Tax, 2024, https://cms.law/en/int/publication/gdpr-enforcement-tracker-report.

[10] Vollmer, Nicholas. "Article 8 EU General Data Protection Regulation (EU-GDPR)." Nicholas Vollmer, 4 Apr. 2023, https://www.privacy-regulation.eu/en/8.htm.

[11] Voss, W. Gregory, and Kimberly A. Houser. "Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies." American Business Law Journal, vol. 56, no. 2, May 2029, pp. 287–344, https://doi.org/10.1111/ablj.12139.

[12] Zoom. In Re: Zoom Video Communications, Inc. Privacy Litigation, N.D. Cal. Master Case No. 5:20-Cv-02155-LHK. 7 Apr. 2022, https://www.zoommeetingsclassaction.com/Content/Documents/Notice.pdf.