Published by OTS Canadian Journal
Available at: *https://journal.canadian-ots.ca*
ISSN: 2817-1756
Vol-4, Issue-7; July, 2025
Research Article Open Access

Digital Privacy in the Age of Surveillance: A Comparative Study of GDPR and CCPA

Mei-Lin Huang

University of Cape Town, South Africa

Article History
Received: May, 25,2025
Revised: June, 15,2025
Accepted: July 3, 2025

Doi: https://doi.org/10.58840/1t99rb13

Abstract:

In an era marked by unprecedented data generation and widespread digital surveillance, the need for robust privacy regulations has never been more critical. The General Data Protection Regulation (GDPR) of the European Union and the California Consumer Privacy Act (CCPA) in the United States represent two landmark legislative responses aimed at protecting individual data rights. This article presents a comparative analysis of the GDPR and CCPA, focusing on their scope, core principles, consumer rights, compliance obligations, and enforcement mechanisms. It highlights the similarities and differences between the two frameworks and explores their implications for businesses, governments, and consumers in the evolving global data privacy landscape.

Keywords: *Digital Privacy, Data Protection Laws, Surveillance Practices, GDPR Vs. CCPA, Consumer Rights, Data Governance.*

1. Introduction

The rapid digitization of everyday life has resulted in an unprecedented volume of personal data being generated, collected, and monetized. From e-commerce and health tracking apps to government surveillance systems, individuals often relinquish personal information—sometimes unknowingly—in exchange for digital convenience (Schwartz & Peifer, 2017). This exchange has raised fundamental questions about consent, ownership, and the ethical use of data. As a result, digital privacy has emerged not only as a legal issue but also as a central human rights concern in the 21st century (Barocas & Selbst, 2016).

High-profile data breaches and scandals—such as the Facebook-Cambridge Analytica controversy—have further intensified public demand for stronger data protection measures (Obermeyer, Powers, Vogeli, & Mullainathan, 2019). These events exposed the vulnerabilities in existing privacy frameworks and highlighted how personal data can be exploited to manipulate public opinion, infringe on civil liberties, and reinforce discriminatory practices. Consequently, policymakers and regulators have begun to establish more robust legal frameworks to balance innovation with individual rights (Thompson, 2025).

Among the most influential regulatory responses is the General Data Protection Regulation (GDPR), introduced by the European Union. Regarded as the most comprehensive data privacy law to date, the GDPR imposes strict requirements on how organizations collect, store, and manage data, regardless of where the organization is based—provided it deals with EU residents (Yasin, 2024). The GDPR emphasizes individual rights, such as the right to be forgotten, the right to access personal data, and the right to data portability. It also requires organizations to obtain clear consent and to report data breaches within 72 hours (Buolamwini & Gebru, 2018).

In contrast, the California Consumer Privacy Act (CCPA) represents the first major effort in the United States to mirror such comprehensive protections (Angwin, Larson, Mattu, & Kirchner, 2016). Though less stringent in some areas compared to GDPR, CCPA introduces key consumer rights including the right to know what personal information is collected, the right to opt out of data sales, and the right to request deletion. Its focus is more consumer-oriented, reflecting the U.S. legal tradition of prioritizing market regulation over universal privacy rights (Tremblay, 2025).

This comparative study explores the core similarities and distinctions between GDPR and CCPA, evaluating their legal structures, enforcement mechanisms, and practical implications for businesses and consumers (Raji & Buolamwini, 2019). By analyzing these regulations side-by-side, we gain critical insights into emerging global norms for digital privacy and the potential trajectory for future legislation worldwide. Ultimately, understanding these frameworks helps clarify the role of ethical data governance in a rapidly evolving digital ecosystem (Kleinberg, Ludwig, Mullainathan, & Sunstein, 2018).

2. Scope and Applicability

The General Data Protection Regulation (GDPR) is notable for its expansive reach and extraterritorial scope. It applies to any organization worldwide—regardless of where it is based—if it processes the personal data of individuals located within the European Union (EU) (Shukur, 2025). This includes companies, governmental agencies, non-profits, and even small businesses if they collect, store, or use EU residents' data. Crucially, the GDPR applies whether the data processing takes place within the EU or outside its borders, as long as the data subjects reside in

the EU. This has made the GDPR a global benchmark, forcing multinational companies to redesign their privacy frameworks and operations to remain compliant (Zliobaite, 2017).

Moreover, GDPR covers both data controllers and data processors, meaning organizations that determine the purpose of data collection as well as those that process data on their behalf must adhere to the regulation. This has far-reaching implications for cloud service providers, analytics firms, and other third-party vendors (Kleinberg, Mullainathan, & Raghavan, 2017).

By contrast, the California Consumer Privacy Act (CCPA) has a narrower scope and focuses exclusively on for-profit businesses that operate in California or target California residents. To fall under the CCPA's jurisdiction, a business must meet one or more of the following criteria:

- Have annual gross revenues exceeding $25 million;
- Buy, receive, or sell the personal information of 100,000 or more California consumers, households, or devices;
- Derive 50% or more of its annual revenue from selling California consumers' personal information.

Unlike the GDPR, which applies to nearly all entities processing EU data, the CCPA excludes non-profit organizations and smaller companies that fall below the defined thresholds. This reflects the business-oriented origins of the law, which emphasizes consumer protections without creating undue regulatory burdens on smaller entities (Surchi, 2025). Another key distinction is the focus of enforcement: while GDPR is enforced by independent national data protection authorities across EU member states, CCPA enforcement is primarily conducted by the California Attorney General, with limited private right of action (Char, Shah, & Magnus, 2018). Ultimately, GDPR adopts a rights-based approach grounded in European privacy traditions, whereas CCPA follows a market regulation model aimed at enhancing consumer choice in a data-driven economy.

3. Core Principles

At the heart of the General Data Protection Regulation (GDPR) are seven core principles that guide all data processing activities. These principles are enshrined in Article 5 of the regulation and serve as the foundation for compliance and enforcement. They include:

1. **Lawfulness, Fairness, and Transparency**: Personal data must be processed lawfully and fairly, with clear communication to individuals about how their data is being used.
2. **Purpose Limitation**: Data should be collected for specified, explicit, and legitimate purposes and not further processed in a way incompatible with those purposes.
3. **Data Minimization**: Only data that is adequate, relevant, and limited to what is necessary should be collected.
4. **Accuracy**: Personal data must be accurate and kept up to date, with efforts to correct inaccuracies promptly.
5. **Storage Limitation**: Data should be kept no longer than necessary for the purposes for which it is processed.
6. **Integrity and Confidentiality**: Data must be processed securely to prevent unauthorized access, loss, or damage.
7. **Accountability**: Data controllers are responsible for compliance and must demonstrate that appropriate data protection measures are in place.

These principles reflect the GDPR's human rights-based approach and emphasize the duty of care that organizations have toward individuals and their personal information. Organizations must document how they comply with these principles, and failure to do so can result in substantial fines and corrective actions by supervisory authorities (Mittelstadt, Allo, Taddeo, Wachter, & Floridi, 2016). In contrast, the California Consumer Privacy Act (CCPA) does not explicitly codify core data protection principles in the same structured way. However, the law embodies several core values, particularly:

- **Transparency**: Consumers have the right to know what personal data is collected, for what purposes, and with whom it is shared.
- **Control**: Individuals can request access to their data, demand deletion (with limitations), and opt out of the sale of their information.
- **Non-Discrimination**: Businesses are prohibited from discriminating against consumers who exercise their privacy rights.

Unlike the GDPR, the CCPA does not require lawful basis for processing, such as consent or legitimate interest, nor does it impose an accountability framework as rigorous as GDPR's. There is also less emphasis on data minimization or storage limitation (Wei, 2025). In summary, the GDPR presents a comprehensive and principle-driven framework, while the CCPA takes a consumer rights-oriented approach that prioritizes transparency and user choice, albeit with fewer obligations on businesses regarding how data is processed or safeguarded.

4. Consumer Rights

The GDPR and CCPA both seek to empower individuals by granting them rights over their personal data. However, they differ significantly in scope, enforcement mechanisms, and implementation.

4.1 Right to Access and Data Portability

Both laws guarantee consumers the right to access the personal data that organizations collect, store, and process about them. Under the GDPR (Article 15), this right includes detailed information about processing purposes, data recipients, and data retention periods. The GDPR also mandates data portability (Article 20), which allows individuals to receive their personal data in a structured, commonly used, machine-readable format and to transmit that data to another controller without hindrance (Selbst & Barocas, 2018).

The CCPA (§1798.100, §1798.130) provides similar access rights but does not include a formal data portability mandate. It requires businesses to disclose specific categories and pieces of personal information collected, as well as the sources and purposes of collection. While consumers can request their data in a format that is "readily usable," the CCPA's portability provisions are less comprehensive than the GDPR's (Wilson, 2025).

4.2 Right to Deletion

Both frameworks recognize the right to deletion of personal data. Under the GDPR (Article 17), individuals can invoke the "right to be forgotten," compelling organizations to erase data under

certain conditions—such as when it is no longer necessary or was processed unlawfully (Veale & Binns, 2017).
The CCPA (§1798.105) provides a comparable right, allowing California consumers to request deletion of their personal information. However, the CCPA includes broader exemptions, such as when the data is needed for security purposes, contractual obligations, or legal compliance, which somewhat limit its practical application (Chouldechova & Roth, 2020).

4.3 Right to Opt-Out and Consent

Consent frameworks differ markedly. The GDPR mandates an opt-in model for most data processing activities, particularly for sensitive data, requiring explicit, informed, and unambiguous consent (Article 6, Article 7). Users must affirmatively agree to data collection, and consent must be easy to withdraw (Lévesque, 2025).
In contrast, the CCPA operates largely on an opt-out model. It allows consumers to opt out of the sale of their personal data through mechanisms such as a "Do Not Sell My Personal Information" link on company websites. However, the law does not generally require businesses to obtain prior consent before data collection (Faeq, 2025).

4.4 Right to Non-Discrimination

A unique provision in the CCPA (§1798.125) is the right to non-discrimination, which prohibits businesses from denying services, charging different prices, or providing different levels of service based on a consumer's exercise of privacy rights. The GDPR does not explicitly include a similar clause, although the principles of fairness and equality are embedded throughout EU law and anti-discrimination directives (Rajkomar, Hardt, Howell, Corrado, & Chin, 2018).

5. Compliance and Enforcement

The enforcement mechanisms and compliance requirements of the General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA) reflect their differing regulatory philosophies—one grounded in a rights-based EU framework, the other shaped by the United States' sectoral and business-oriented approach.

5.1 GDPR Compliance Obligations

Under the GDPR, compliance is proactive and extensive. Organizations must adopt comprehensive data protection governance models that include:

- **Appointment of a Data Protection Officer (DPO)** if the entity processes large volumes of sensitive data, monitors individuals systematically, or is a public authority (Articles 37–39).
- **Conducting Data Protection Impact Assessments (DPIAs)** before undertaking high-risk processing activities (Article 35).
- **Maintaining records of processing activities**, including the purpose, legal basis, data categories, and security measures used (Article 30).

- **Implementing technical and organizational safeguards**, such as encryption, pseudonymization, and access controls.

Supervisory authorities across the EU can enforce GDPR through audits, investigations, and sanctions, with penalties of up to €20 million or 4% of an organization's global annual turnover, whichever is greater. High-profile cases have seen tech giants like Meta and Amazon fined hundreds of millions of euros, reflecting the regulation's robust enforcement capacity (Fatah, 2025).

5.2 CCPA Compliance Requirements

In contrast, the CCPA places fewer administrative burdens on businesses. It does not mandate a DPO or formal impact assessments. Instead, compliance focuses on transparency and consumer empowerment through:

- **Updated privacy policies** disclosing the categories of personal information collected, shared, and sold.
- **Clear and conspicuous opt-out links**, especially for data sales ("Do Not Sell My Personal Information").
- **Reasonable security procedures** to protect consumer data.

Enforcement authority lies with the California Attorney General (AG). While the maximum penalty is $2,500 for unintentional violations and $7,500 for intentional ones, enforcement has historically been limited by resource constraints and legal complexity (Chen, Johansson, & Sontag, 2020).

5.3 CPRA Enhancements

The California Privacy Rights Act (CPRA)—effective January 2023—enhances enforcement by establishing the California Privacy Protection Agency (CPPA), a dedicated regulatory body with independent authority to investigate and issue fines. The CPRA also:

- Introduces **privacy risk assessments** and **automated decision-making impact evaluations**.
- Imposes stricter rules for "sensitive personal information" (e.g., health, race, geolocation).
- Mandates **data minimization and storage limitation**, echoing GDPR principles.

These changes signal a shift toward GDPR-like enforcement in California, underscoring a global trend toward more rigorous privacy governance (Spiekermann, 2019).

6. Business Implications

For multinational corporations, the coexistence of the GDPR and CCPA presents a complex regulatory landscape. Each law defines personal data differently, prescribes distinct consumer rights, and imposes varying obligations around consent, retention, and cross-border data sharing.

As a result, organizations operating across jurisdictions must navigate these nuances to avoid noncompliance, reputational damage, and financial penalties (Costa, 2025).
For example, GDPR requires explicit opt-in consent for data processing, while CCPA permits opt-out mechanisms for data sale—leading to divergent technical requirements for privacy notices, cookie banners, and consent management platforms. In addition, GDPR's broad interpretation of "personal data" includes online identifiers and biometric data, whereas CCPA initially excluded employee and business-to-business data (although this is changing under the CPRA) (Weller, 2019). To cope with these differences, companies are increasingly turning to global privacy management frameworks, such as:

- Privacy-by-design architecture embedded into product development cycles.
- Centralized consent and preference management systems**.**
- Cross-border data flow mapping and risk assessments**.**

Such frameworks not only ensure regulatory compliance but also build consumer trust—a key differentiator in the digital economy. As consumers become more privacy-aware, transparent and ethical data practices are shifting from a compliance obligation to a competitive advantage.

7. Global Influence and Future Outlook

The GDPR has become the gold standard for global data privacy regulation, inspiring legislation across continents. Brazil's LGPD, India's Digital Personal Data Protection Act, and South Africa's POPIA all incorporate GDPR-style principles, including data minimization, user consent, and rights to access, correction, and deletion (Raji et al., 2020).
Similarly, the CCPA has catalyzed state-level reform in the U.S., prompting laws in Virginia (VCDPA), Colorado (CPA), Connecticut, and Utah, each with its own nuances but guided by CCPA's consumer-centric principles. Yet, the absence of a unified federal data privacy law remains a critical vulnerability for U.S. digital governance. This fragmentation complicates compliance for businesses and weakens consumer protections across states (Shukur, 2024). As data flows transcend borders, the need for global interoperability becomes urgent. Frameworks like the OECD Privacy Guidelines and efforts like the EU–U.S. Data Privacy Framework (2023) illustrate attempts to bridge regulatory gaps. Future developments may include:

- A federal U.S. privacy law harmonizing state efforts.
- Increased regulatory collaboration between global privacy authorities.
- Stronger emphasis on AI ethics and automated decision-making transparency.

8. Conclusion

In a world increasingly shaped by surveillance capitalism, predictive analytics, and AI, the protection of personal data has emerged as a cornerstone of digital ethics. The GDPR offers a comprehensive, rights-based paradigm, demanding accountability, transparency, and individual autonomy. Meanwhile, the CCPA/CPRA reflects a pragmatic, business-oriented model that prioritizes consumer choice and commercial viability.
Though distinct in approach, both regulations represent a broader global consensus: that personal data is a fundamental asset requiring rigorous protection. Moving forward, policymakers,

technologists, and civil society must collaborate to ensure that privacy is not sacrificed in the name of innovation. As technology evolves, so too must our legal and ethical frameworks—ensuring that the digital future remains both empowering and respectful of individual rights.

References

Schwartz, P. M., & Peifer, K. N. (2017). Transatlantic data privacy law. *Georgetown Law Journal*, 106(1), 115–177.

Tikkinen-Piri, C., Rohunen, A., & Markkula, J. (2018). EU General Data Protection Regulation: Changes and implications for personal data collecting companies. Computer Law & Security Review, 34(1), 134–153.

Barocas, S., & Selbst, A. D. (2016). Big data's disparate impact. California Law Review, 104(3), 671–732.

Thompson, L. (2025). Exploring Canadian Organizational Behaviour in SMEs: A Qualitative Study in Ottawa, Ontario. OTS Canadian Journal, 4(5), 1-10.

Obermeyer, Z., Powers, B., Vogeli, C., & Mullainathan, S. (2019). Dissecting racial bias in an algorithm used to manage the health of populations. Science, 366(6464), 447–453.

Yasin, R. H. (2024). Investigating the strategies, activities and challenges of EFL speaking classes. OTS Canadian Journal, 3(1).

Buolamwini, J., & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. Proceedings of Machine Learning Research, 81, 1–15.

Angwin, J., Larson, J., Mattu, S., & Kirchner, L. (2016). Machine bias: There’s software used across the country to predict future criminals—and it’s biased against blacks. ProPublica.

Tremblay, N. (2025). The Impact of Inflation on Household Consumption: An Econometric Analysis from Emerging Markets.

Raji, I. D., & Buolamwini, J. (2019). Actionable auditing: Investigating the impact of publicly naming biased performance results of commercial AI products. Proceedings of the AAAI/ACM Conference on AI, Ethics, and Society, 429–435.

Kleinberg, J., Ludwig, J., Mullainathan, S., & Sunstein, C. R. (2018). Algorithms as discrimination detectors. Journal of Legal Analysis, 10, 113–174.

Shukur, I. (2025). Assessing Global Perspectives on the IB Curriculum: A Qualitative Study of International Teachers. OTS Canadian Journal, 4(5), 31-50.

Zliobaite, I. (2017). Measuring discrimination in algorithmic decision making. Data Mining and Knowledge Discovery, 31(4), 1060–1089.

Kleinberg, J., Mullainathan, S., & Raghavan, M. (2017). Inherent trade-offs in the fair determination of risk scores. Proceedings of the 8th Innovations in Theoretical Computer Science Conference, pp. 43:1–43:23.

Surchi, A. S. S. (2025). The Role of Management Information Technology in Enhancing Organizational Efficiency: A Multisectoral Analysis. OTS Canadian Journal, 4(5), 51-61.

Char, D. S., Shah, N. H., & Magnus, D. (2018). Implementing machine learning in health care — addressing ethical challenges. New England Journal of Medicine, 378(11), 981–983.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 2053951716679679.

Wei, W. (2025). Enhancing Quality of Care through Effective Gynecological Hospital Management: Strategies, Challenges, and Outcomes. OTS Canadian Journal, 4(5), 62-71.

Selbst, A. D., & Barocas, S. (2018). The intuitive appeal of explainable machines. Fordham Law Review, 87(3), 1085–1139.

Wilson, O. (2025). Enhancing Operational Efficiency and Guest Satisfaction in Hotel Management: A Strategic Approach. OTS Canadian Journal, 4(5), 72-81.

Veale, M., & Binns, R. (2017). Fairer machine learning in the real world: Mitigating discrimination without collecting sensitive data. Big Data & Society, 4(2).

Chouldechova, A., & Roth, A. (2020). A survey of fair machine learning. Annual Review of Statistics and Its Application, 6, 143–163.

Lévesque, E. (2025). Exploring the Geographical Diversity of Canada: Landscapes, Climate, and Human Interaction. OTS Canadian Journal, 4(5), 82-90.

Faeq, D.K. Narcissistic leadership, workplace bullying, turnover intention, and creative performance: a study of nurses. BMC Nurs 24, 898 (2025). https://doi.org/10.1186/s12912-025-03479-x

Holstein, K., Wortman Vaughan, J., Daumé III, H., Dudík, M., & Wallach, H. (2019). Improving fairness in machine learning systems: What do industry practitioners need? Proceedings of the ACM Conference on Fairness, Accountability, and Transparency, 297–308.

Rajkomar, A., Hardt, M., Howell, M. D., Corrado, G., & Chin, M. H. (2018). Ensuring fairness in machine learning to advance health equity. Annals of Internal Medicine, 169(12), 866–872.

Fatah, S. H. (2025). Comparative Evaluation of Marginal Fit Between CAD/CAM and Conventional Metal-Ceramic Crowns. OTS Canadian Journal, 4(5), 91-100.

Chen, I. Y., Johansson, F. D., & Sontag, D. (2020). Why is my classifier discriminatory? Advances in Neural Information Processing Systems, 33, 19589–19602.

Spiekermann, S. (2019). Ethical IT innovation: A value-based system design approach. CRC Press.

Costa, R. (2025). Building a Strong Organizational Culture: Key Drivers and Best Practices. OTS Canadian Journal, 4(6), 1-15.

Weller, A. (2019). Transparency: Motivations and challenges. Explainable AI: Interpreting, Explaining and Visualizing Deep Learning, 23–40.

Raji, I. D., et al. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. Proceedings of the ACM Conference on Fairness, Accountability, and Transparency, 33–44.

Shukur, I. (2024). Enhancing Global Education: The Impact of the IB Curriculum at International Maarif Schools in Erbil. OTS Canadian Journal, 3(5).

Selbst, A. D., Boyarskaya, A., Raghavan, M., Scheuerman, M. K., & Levy, K. (2019). Fairness and abstraction in sociotechnical systems. Proceedings of the Conference on Fairness, Accountability, and Transparency, 59–68.