The Impact of Data Privacy Laws on Small Business Operations: A Comparative Study of GDPR and CCPA.

MASON V. KOECHER, University of California, Merced, USA

Abstract:

An increase in the prevalence of information privacy laws, such as the European Union General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA), has significantly impacted businesses internationally(6). This study will explore comparisons between GDPR and CCPA/CPRA, which will be used synonymously for the sake of simplicity, on small businesses within the US, focusing on crucial aspects such as compliance costs, forced operational modifications, and possible limitations in small-business expansion(9). These regulations can cause additional trouble for small businesses through obligatory resource allocation, technological upgrade expenses, and legal responsibilities(9).

Findings reveal that while GDPR and CCPA aim to enhance consumer data protection, their distinct scopes and enforcement mechanisms create different levels of complexity for small businesses(12). This study underscores the importance of tailored compliance strategies and suggests policy recommendations to ease the regulatory burden on small enterprises(9). The aggregate of a multiplicity of research provides a comprehensive understanding of the real-world implications of data privacy laws on small business operations. It offers insights into how businesses can adapt to this evolving regulatory landscape.

1. Introduction

The GDPR was passed in order to replace the 1995 Data Protection Directive, which had flaws concerning (1) lack of uniform policy within the E.U., (2) not providing legal protection from inadequate personal processing data outside of the E.U., (3) dated language allowing for ambiguous practices concerning validation of a users consent to share information[1]. For comparison, the CCPA (2018) was the first comprehensive consumer privacy legislation enacted in the U.S.[2]; this legislation corrected prior flaws in the U.S. legal system, extended shortly after by the CPRA (2020)[5], which corrected (1) inaccurate personal data, (2) limited businesses' usage of sensitive personal information, (3) removing the set period in which businesses can correct violations without penalty, (4) prohibits businesses from holding onto personal data for longer than necessary, (5) triples maximum fines for violations involving children under the age of 16 (up to $7,500)[10]. However, it still needs to be determined to what extent these laws have affected small businesses financially, legally, and socially. Thus, this paper identifies these laws' effects through a statistical analysis of the abovementioned categories.

In order to analyze the overall effect of these regulations on small businesses within the United States, we must examine the advantages that larger corporations have in the process implementing GDPR privacy laws in comparison to smaller businesses with less fluid capital to spend on updating systems, processes, and policies[12]. Larger corporations hold a significant advantage in their ability to implement these aforementioned systems, processes, and policies. As larger companies are able to adhere to these privacy laws faster and more effectively than small businesses, they face a

significantly lower probability of facing the hefty fines implemented by the GDPR which totalled more than €2.92 billion in 2022[8].

Some of the most common GDPR violations are as follows: (1) Non-compliance with general data processes, (2) Insufficient fulfillment of data subjects rights, (3) Insufficient legal basis for data processing, (4) Insufficient cooperation with supervisory authorities, (5) Insufficient technical and organizational measures to ensure information security[8]. While some of the most common CCPA violations are as follows: (1) Failing to provide consumers with a privacy notice, (2) Failing to comply with "Do Not Sell My Personal Information" requests, (3) Failing to obtain consent for child's data, (4) Failing to comply with consumer access or deletion requests, (5) Not reporting unauthorized access to consumer data or another form of a data breach, etc[15].

This study underscores the importance of developing tailored compliance strategies that account for the unique limitations of small businesses while proposing actionable policy recommendations to ease their regulatory burden. By focusing on practical and equitable solutions, policymakers and industry leaders can create a more level playing field, ensuring that businesses of all sizes can navigate privacy regulations effectively without stifling innovation or growth.

2. Comparative Analysis

When searching for accurate estimates from which to pull exact costs of compliance for GDPR and CCPA from, the data sets have no consistent metric. A study that took place in 2019 from the International Association of Privacy Professionals (IAPP) in conjunction with Ernst & Young, a global professional service network, found

that among its survey participants, the mean privacy expenditures were in the range of $1 million in 2018, the year in which GDPR was enacted. In the following year, 2019, the mean cost lowered to approximately $622,000[16]. Another study conducted by Ponemon Institute in 2019 on behalf of international law firm McDermott Will & Emery (MW&E) which focused on GDPR compliance budgets, found substantially higher figures than the previous study conducted in the same year. The average budget set aside in order to comply with GDPR regulations was $13.2 million in 2018 and slightly higher in 2019, coming in at around $13.6 million[16]. However, these studies don't seem to survey or cover the costs that smaller businesses incur; for the most part, these data points cover large firms attempts to comply with GDPR as the way in which the studies were conducted were through limited access surveys through Linkedin.

The estimated costs of compliance for the CCPA/CPRA are slightly more accurate then estimates concerning cost of compliance for the GDPR. Table 1, created by Berkeley Economic Advising and Research, LLC, covers the estimated compliance cost by industry for the year 2019. However, a disclaimer used by the Berkeley Economic Advising and Research, LLC, to describe the type of data estimates represented in the table is as follows: "the novel nature of the CCPA and uncertainty regarding the expected compliance actions by firms across a diverse set of sectors should

Table 1: Total Estimated Compliance Costs (million 2019$)

NAICS Code	Description	>$25 million revenue threshold	50% Threshold	75% Threshold
11				40.5
21	Mining, Quarrying, and Oil and Gas Extraction	2.1	9.0	12.6
22	Utilities	1.4	8.3	11.8
23	Construction	16.9	1,026.8	1,536.1
31-33	Manufacturing	48.1	530.8	780.7
42	Wholesale Trade	49.5	755.3	1,116.5
44-45	Retail Trade	32.2	1,021.3	1,522.0
48-49	Transportation & Warehousing	25.0	293.8	431.3
51	Information	20.3	248.1	365.1
52	Finance and Insurance	24.6	429.0	634.3
53	Real Estate, Rental, Leasing	13.8	624.2	931.6
54	Professional, Scientific, and Technical Services	51.6	1,686.0	2,511.6
55	Management of Companies and Enterprises	46.2	65.2	80.0
56	Administrative/Support/Waste Mgmt. Svs.	33.5	551.9	816.9
61	Educational Services	12.2	184.5	273.7
62	Health Care and Social Assistance	34.5	1,329.6	1,986.0
71	Arts, Entertainment, and Recreation	8.3	340.7	508.7
72	Accommodation and Food Services	29.2	953.0	1,422.4
81	Other Services (except Public Administration)	16.4	984.8	1,472.5
Total		466.9	11,069.4	16,454.2

cause the reader to interpret these compliance costs estimates with caution.[17]" Further analysis on the CCPA's effects of small businesses state that larger businesses are better suited to deal with up-front compliance costs while smaller businesses, who may be already behind on compliance with GDPR, will struggle to manage the costs of compliance from both privacy laws. However, the impact on small businesses will be mostly negative in the short-term; long-term, these businesses will possibly outsource this work to dedicated firms and through direct competition, costs will fall[17].

The CCPA, alongside the additional CPRA, goes beyond the scope of the GDPR; including, but not limited to, data relating to a household or device. However, the GDPR has more detailed requirements and contains stricter penalties pertaining to data misuse[19]. Where the CCPA falls short is its narrow scope of just covering California residents and does not extend outside of the US, also the CCPA cannot apply to businesses that gross less than $25 million in annual revenue or have 50,000 Californian users.[19] On one hand, this provision would allow smaller businesses to function while misusing user data which damages the general public's access to their freedom of privacy. On the other hand, this provision puts a soft cap on how much a small business can develop and creates a barrier to entry by introducing new regulations after the business gets to a certain size; possibly causing diminished growth to rising businesses.

The GDPR's aforementioned strict policies[19] do make policy compliance more difficult than the CCPA's. This would present difficulties for any business that falls within the scope of the GDPR which is significantly more than the CCPA. With more than 23 million businesses affected by GDPR regulation[21], the main difficulty shown by a 2019 survey done by GDPR.EU, is that around half of small businesses are failing to

comply with the GDPR because of two particular regulations that state: (1) The GDPR requires companies to describe data processing activities in clear, plain language to data subjects and (2) the requirement for businesses to identify a lawful basis for using someone's data.[20] According to this survey, around half of the respondents were unsure whether or not they complied with either of those two provisions listed above[20]. With a privacy law that carries a difficult compliance factor such as the GDPR, many small business owners within the study done in 2019 by GDPR.EU believe that these laws prey on smaller businesses more than larger corporations. The reasoning being, "We are the easy hits. Big companies can afford lawyers to fight in their corner. We can't so we are seen as easy targets.[20]"

3. Challenges Faced By Small Businesses

In order to keep these standards met and avoid fines, companies that deal with personal data, which in today's market is extremely commonplace with 73% of US companies collecting personal data from consumers who access their services as of 2021[13], must keep in compliance with particularly GDPR regulations at all times which requires time and resources that some small-businesses can't afford, either immediately or at all. As mentioned in the previous section, many challenges faced by these businesses will be shown mostly in the short-term. While compliance costs remain high for all businesses, smaller ones will have less existing capital to soften the financial blow. However, as compliance shifts towards developing an industry surrounding these regulations, the cost of compliance will most likely decrease over time. This, alongside the difficulty of maintaining compliance as a larger company, will shift the difficulty

over to the intended group, large corporations who take advantage of consumer information and use it in ways that are considered a betrayal of the average consumer's trust.

When we take into account the CCPA's high barrier to entry, it actually limits small businesses very little and impacts larger firms far more. The only existing downside of the CCPA is a hypothetical possibility of limiting business growth beyond $25 million or if an app/business becomes too popular (>50,000 users).

4. Benefits of Compliance

The CCPA's benefits to consumers are derived from privacy protections under law. These protections give consumers the right to maintain control over the use of their personal information. These rights determine that any consumer protected under this law will have the ability to prevent the sale or collection of any personal information, along with the ability to delete any of their personal information from potential databases controlled by any business that operates within legal jurisdiction. To further emphasize the importance of individual control over personal data, this market of California consumer data, while difficult to accurately measure, contains $1.6 billion - $5.4 billion USD on the app marketplace alone[17]. For additional context, a study done by Berkeley Economic Advising and Research, LLC, finds that the aggregate value of personal information used for advertising in California is over $12 Billion annually[17]. The obvious benefits for businesses complying to the CCPA regulations are simply not being hit with fines presented in table (2)[22], all of which are updated with the most recent monetary changes.

Updated Monetary Thresholds in CCPA (Figure 2)

Civil Code §	Updated 2025 Amount	Previous Amount
Civil Code § 1798.140(d)(1)(A): *Annual gross revenue amount within the definition of "business"*	$26,625,000	$25,000,000
Civil Code § 1798.150(a)(1)(A): *Monetary damages range per consumer per incident*	*Not less than **$107** and not greater than **$799** per consumer per incident or actual damages, whichever is greater.*	*Not less than **$100** and not greater than **$750** per consumer per incident or actual damages, whichever is greater.*
Civil Code § 1798.155(a): *Administrative fine amounts*	*Not more than **$2,663** for each violation or **$7,988** for each intentional violation and violations involving the personal information of consumers whom the violator has actual knowledge are under 16 years of age.*	*Not more than **$2,500** for each violation or **$7,500** for each intentional violation and violations involving the personal information of consumers whom the violator has actual knowledge are under 16 years of age.*
Civil Code § 1978.199.90(a): *Civil penalty amounts*	*Not more than **$2,663** for each violation or **$7,988** for each intentional violation and violations involving the personal information of consumers whom the violator has actual knowledge are under 16 years of age.*	*Not more than **$2,500** for each violation or **$7,500** for each intentional violation and violations involving the personal information of consumers whom the violator has actual knowledge are under 16 years of age.*
Civil Code § 1798.199.25: *Daily compensation rate for Board members*	*$107*	*$100*

(California Privacy Protection Agency. (2024, December 17). Announcement: Civil Code § 1978.199.90(a) and Penalty Amounts. Retrieved January 11, 2025[22])

The benefits of compliance to the GDPR for consumers are similar to the benefits of the CCPA regarding consumers rights to control over their information. The GDPR is an accumulation of 28 separate laws into one larger legal umbrella, granting extensive protection to consumers in the following ways: (1) The requirement of opt-in consent given by consumers to use data as agreed upon, (2) consumers are given the right to remove their information, (3) data transfers keep privacy in tact as the information moves globally, (4) organizations are explicitly required to protect personal identifiable information (PII) of all "data subjects[2]." The benefits for firms complying to the GDPR is that they won't incur hefty fines that can range from €20,000,000 to 4% of annual worldwide revenue, whichever is higher. Companies like Tiktok, which faced a €345 million fine, Meta, which faced a $1.3 billion fine, or Amazon, which faced a $888 million fine have quickly found out how beneficial it is to comply with these regulations.

5. Policy Recommendations

In this paper we have examined the benefits and setbacks posed by the privacy laws, GDPR and CCPA, to small businesses within the U.S. With the age of technology marching ever onward, we must be prepared to alter regulations to protect both user privacy and innovation no matter the size of organization. Various policy recommendations to assist small businesses are as follows:

1. Proportional Compliance Requirements: Privacy laws could introduce tiered compliance requirements based on company size and data processing activities. For instance, small businesses handling minimal sensitive data could be subject to simplified audits or reporting procedures.
2. Subsidized Compliance Assistance: Governments or privacy regulatory agencies could provide grants or subsidies to assist small businesses in covering the costs of compliance tools and resources.
3. Flexible Timelines for Implementation: Extending timelines for compliance deadlines could allow small businesses to adapt gradually without jeopardizing their operations.
4. Centralized Resources: Establish a centralized platform offering free templates, guides, and access to consultants for small businesses navigating compliance.

To further elaborate on possible changes to both the CCPA and GDPR, here are some positive aspects they could incorporate that take inspiration from the other:

1. From GDPR to CCPA: GDPR's global applicability could serve as a model for expanding CCPA protections beyond California residents. Additionally, GDPR's

detailed consent and data transfer guidelines could enhance CCPA's framework to provide more clarity for businesses and consumers.

2. From CCPA to GDPR: The CCPA's exemptions for smaller entities could inspire GDPR to adopt scalable regulations, reducing undue burdens on micro and small enterprises. Additionally, the CCPA's focus on household and device data could enrich GDPR's scope, aligning protections with emerging digital technologies.

These recommendations aim to strike a balance between safeguarding consumer rights and supporting the growth and innovation of small businesses. By fostering collaboration between regulators, industry leaders, and small enterprises, a fairer and more sustainable regulatory landscape can emerge.

References:

1. Advisera. (n.d.). *EU GDPR vs. European Data Protection Directive*. Retrieved October 1, 2024, from https://advisera.com/articles/eu-gdpr-vs-european-data-protection-directive/#:~:text=Although%20respectable%20at%20the%20time,data%20processing%20outside%20of%20EU.
2. AmtrustFinancial. (n.d.). *What Is the General Data Protection Regulation (GDPR)?* Retrieved September 30, 2024, from https://amtrustfinancial.com/resource-center/trends-and-research/gdpr.

3. Bloomberg Law. (n.d.). *California consumer privacy laws*. Retrieved October 4, 2024, from https://pro.bloomberglaw.com/insights/privacy/california-consumer-privacy-laws/#:~:text=As%20the%20first%20comprehensive%20consumer,the%20way%20companies%20do%20business.

4. GDPR-Info. (n.d.). *Recital 9 – General Data Protection Regulation (GDPR)*. Retrieved October 1, 2024, from https://gdpr-info.eu/recitals/no-9/#:~:text=The%20objectives%20and%20principles%20of,in%20particular%20with%20regard%20to.
5. Goldfarb, A., Tucker, C., & Greenstein, S. (2022). *Privacy and innovation* (No. 30028). National Bureau of Economic Research. Retrieved October 10, 2024, from https://www.nber.org/papers/w30028.
6. Investopedia. (n.d.). *General Data Protection Regulation (GDPR)*. Retrieved October 1, 2024, from https://www.investopedia.com/terms/g/general-data-protection-regulation-gdpr.asp#toc-criticism-of-the-gdpr.
7. Nightfall AI. (n.d.). *California data breach notification law*. Retrieved October 4, 2024, from https://www.nightfall.ai/blog/california-data-breach-notification-law-nightfall.
8. ShardSecure. (n.d.). *The most common GDPR violations*. Retrieved October 1, 2024, from https://shardsecure.com/blog/most-common-gdpr-violations.
9. Truendo.com. (2024). *GDPR vs. CCPA: Comparative Analysis and Business Implications*. Retrieved September 30, 2024, from

https://www.truendo.com/blog/dpr-vs-ccpa-a-comparative-analysis-of-privacy-laws-and-their-implications-for-businesses.

10. Varonis. (n.d.). *The GDPR effect: A 5-year review*. Retrieved October 10, 2024, from https://www.varonis.com/blog/gdpr-effect-review#:~:text=US%20companies%20had%20to%20spend,%247.8%20billion%20on%20GDPR%20prep.
11. Wikipedia. (n.d.). *California Privacy Rights Act*. Retrieved October 4, 2024, from https://en.wikipedia.org/wiki/California_Privacy_Rights_Act#cite_note-6.
12. Wong, Richmond Y., et al. (2023). *Privacy Legislation as Business Risks: How GDPR and CCPA Are Represented in Technology Companies' Investment Risk Disclosures*. *Proceedings of the ACM on Human-Computer Interaction*, vol. 7, no. CSCW1, 14 Apr. 2023, pp. 1–26. Retrieved September 30, 2024, from https://doi.org/10.1145/3579515.
13. Statista. (n.d.). Percentage of firms worldwide collecting personal data as of 2020, by type. Retrieved January 6, 2025, from https://www.statista.com/statistics/1172965/firms-collecting-personal-data/
14. European Data Protection Supervisor (EDPS). (n.d.). *History of the General Data Protection Regulation (GDPR)*. Retrieved January 6, 2025, from https://www.edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en#:~:text=In%202016%2C%20the%20EU%20adopted,internet%20was%20in%20its%20infancy.

15. Secure Privacy. (n.d.). *CCPA fines: Understanding penalties and enforcement actions.* Retrieved January 6, 2025, from https://secureprivacy.ai/blog/ccpa-fines.
16. Davis, Ariel, et al. (2021). *Small business compliance under GDPR and CCPA: Comparative challenges and opportunities.* Social Science Research Network. Retrieved January 6, 2025, from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3827228.
17. California Department of Finance. (2020). CCPA regulations: Standardized regulatory impact assessment (SRIA). Retrieved January 10, 2025, from https://dof.ca.gov/wp-content/uploads/sites/352/Forecasting/Economics/Documents/CCPA_Regulations-SRIA-DOF.pdf.
18. California Office of the Attorney General. (n.d.). California Consumer Privacy Act (CCPA). Retrieved January 10, 2025, from https://oag.ca.gov/privacy/ccpa#:~:text=What%20businesses%20does%20the%20CCPA,California%20residents%20or%20households;%20or.
19. CookieYes. (n.d.). CCPA vs. GDPR: Key Differences and Similarities. Retrieved January 11, 2025, from https://www.cookieyes.com/blog/ccpa-vs-gdpr/#:~:text=CCPA%20is%20specific%20to%20California,effect%20on%20May%2025%2C%202018.
20. GDPR.eu. (n.d.). 2019 Small Business Survey: GDPR Compliance Challenges. Retrieved January 11, 2025, from https://gdpr.eu/2019-small-business-survey/#:~:text=One%20year%20after%20the%20EU%27s,they%20were%20struggling%20to%20comply.

21. MIT Sloan School of Management. (n.d.). How GDPR Reduced Firms' Data and Computation Use. Retrieved January 11, 2025, from https://mitsloan.mit.edu/ideas-made-to-matter/gdpr-reduced-firms-data-and-computation-use#:~:text=The%20GDPR%20affects%20more%20than,in%20countries%20around%20the%20world.
22. California Privacy Protection Agency. (2024, December 17). Announcement: Civil Code § 1978.199.90(a) and Penalty Amounts. Retrieved January 11, 2025, from https://cppa.ca.gov/announcements/2024/20241217.html?mkt_tok=MTM4LUVaTS0wNDIAAAGXfxVNtfJct8rhP2rgKOzxn7s5Hc6uBA5g-qEdnToKFRa0uuNciz41lsHOdkIK1SF6DXyPPhY_k8PuhLtw-Liqez8HSTK6F93DDeKT9Rd9st4k#:~:text=Civil%20Code%20§%201978.199.90(a):&text=Civil%20penalty%20amounts-,Not%20more%20than%20$2%2C663%20for%20each%20violation%20or%20$7%2C988%20for,under%2016%20years%20of%20age.