Impact of California Consumer Privacy Act (CCPA) on Data Breaches Reporting

Ebenezer Acquah*
Department of Public Policy and Administration, Florida International University
eacqu002@fiu.edu

Sukumar Ganapati
Department of Public Policy and Administration, Florida International University
ganapati@fiu.edu

Yoon-Jung Choi
Department of Public Policy and Administration, Florida International University
yoonchoi@fiu.edu

ABSTRACT

This article is an exploratory analysis of the impact of the California Consumer Privacy Act (CCPA) on data breaches that result in exposing sensitive private data of consumers. The CCPA applies to large for-profit businesses that collect and disseminate personal information of Californian consumers. It provides for consumer rights and imposes notification and security requirements on businesses that collect private information. We analyzed how CCPA affects data breach notifications that are required by the state's Office of Auditor General, for the period 2012 to 2023. The analysis provides interesting insights into the impact of CCPA on the pattern of data breaches. Our principal finding is that privacy breaches reduced to some extent after CCPA. Importantly, CCPA has helped in the overall improvement in reporting privacy breaches. We surmise that the CCPA brought more data breaches into light.

CCS CONCEPTS

• :; • **Security and privacy**; • **Human and societal aspects of security and privacy**;

KEYWORDS

Privacy, Data Breaches, Cybersecurity, notification

ACM Reference Format:
Ebenezer Acquah, Sukumar Ganapati, and Yoon-Jung Choi. 2024. Impact of California Consumer Privacy Act (CCPA) on Data Breaches Reporting. In *25th Annual International Conference on Digital Government Research (DGO 2024), June 11–14, 2024, Taipei, Taiwan*. ACM, New York, NY, USA, 8 pages. https://doi.org/10.1145/3657054.3657082

1 INTRODUCTION

California Consumer Privacy Act (CCPA) is a pivotal milestone in the realm of data protection in the United States. It was enacted in 2018 and it became effective in 2020. The CCPA is arguably a comprehensive framework aimed at safeguarding sensitive personal information. Its main objective is to secure the privacy of California consumers by offering them a control over their digital footprint. It gives Californians the right to know what personal information (PI) is being collected about them, whether this information is sold and to whom, the right to access their information, the right to delete any personal information collected, and the right to opt-out from the sale of their information. The CCPA mainly applies to for-profit businesses that are large in their size or operations. California is the first state to have promulgated such a wide-ranging privacy policy in the United States. California's privacy policy followed closely on the heels of the European Union's General Data Protection Regulation (GDPR), also enacted in 2018. More states have adopted privacy laws since then (e.g. Colorado, Virginia). The CCPA was amended with the California Privacy Rights Act (2020), which facilitated the formation of California Privacy Protection Agency (CPPA) to implement and enforce the California Consumer Privacy Act. Until 2020, the implementation fell directly under the California's Office of Attorney General (OAG). The formation of the CPPA (which began functioning in 2022) is another indicator of the California state's seriousness with respect to privacy protection.

In this paper, we make an exploratory analysis of the impact of the CCPA on data breaches in California. A data breach is the unencrypted personal information that is acquired, or reasonably believed to have been acquired, by an unauthorized person. The California state has required since 2003 that public agencies and business entities must notify affected consumers about these data breaches (as per California Civil Code Section 1798.29(a) for state agencies and California Civil Code Section 1798.82(a) for businesses). Since 2012, the state has required a sample copy of a breach notice must also be provided to the California OAG. The state OAG has consequently maintained a record of the breach notices since 2012. Examination of the pattern of the data breach notices thus provide useful insights into the impact of CCPA on the reported data breaches.

We use the lens of institutional theory to frame the conceptual basis. Institutional theory holds that transparency mechanisms (like data breach notification) may not themselves reduce the incidences (of the data breaches) ([Chen and Ganapati 2023]. Rather, a legal institutional measure (like the CCPA) is required for providing adequate legal deterrence for firms to implement methods that reduce the breaches. Hence, the presumption for the paper is rather simple: the CCPA should result in a reduction of data breaches. The CCPA should also result in overall betterment of data breach notifications. From a research design perspective, it is worth noting that the CCPA does not directly provision the need for data breach reporting. The reporting process was already in place for public and private entities when CCPA was enacted. The data breach

*Corresponding author.

DGO 2024, June 11–14, 2024, Taipei, Taiwan

ACM ISBN 979-8-4007-0988-3/24/06
https://doi.org/10.1145/3657054.3657082

reporting documented by OAG are thus independent of the CCPA requirements. The data breach reporting process can be considered as a transparency requirement: it requires notification but does not hold any (dis)incentives for the firms reporting the breaches. CCPA requirements apply certain legal conditions on businesses, which then would induce the businesses to fulfill the compliance requirements. Businesses fulfilling the compliance requirements would then automatically carry out technological measures that would result in reduction of the data breaches.

2 BACKGROUND

The California Consumer Privacy Act (CCPA) aims to give Californian consumers control over their personal information. The law defines personal information as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household.". The scope of such personal information ranges from basic data (e.g., name, address, etc.) to that of sensitive data (e.g. social security, biometrics, etc.). The personal information does not encompass publicly available data that are legally in the public domain (e.g., government records such as property deeds, licenses). The 2018 CCPA provides consumers with certain rights to control their personal data. They have the right to know about the personal information that a business collects and how it is used and shared. They have the right to delete personal information collected from them. They have the right to opt-out of the sale or sharing of their personal information. Exercising these rights should not result in non-discrimination. The 2020 amendment of CCPA added new privacy protections: the right to rectify any inaccurate personal information that a business collects about individuals; and the right to limit the use and disclosure of sensitive personal information collected about individuals.

The CCPA mainly applies to large businesses that meet any of the following threshold criteria: gross annual revenue of over $25 million; buy, sell, or share the personal information of 100,000 or more California residents, households, or devices; or derive 50% or more of their annual revenue from selling California residents' personal information. The law applies to data brokers, who knowingly collect and sell the personal information of consumers to third parties. These data brokers collect information about consumers from different sources (e.g. websites, public records) and repackage the data. The CCPA does not apply to public or nonprofit organizations. The CCPA imposes certain security requirements on businesses to safeguard consumers' private information. The businesses need to inform consumers about the types of personal information that are collected and the purpose for which the information is used. The businesses should implement reasonable security measures for safeguarding an individual's personal information to protect such information from unauthorized or illegal access, destruction, use, modification, or disclosure. If the CCPA requirements are violated, individuals can sue the business for their data breach, when there is a loss of nonencrypted and nonredacted personal information due to the business's failure to take adequate security procedures. The claimants can seek statutory damages ranging from $100 to $750 per consumer per incident. The California state can also take legal actions on the businesses that violate CCPA requirements. The state can seek civil penalties of $2,500 for each violation or $7,500 for each intentional violation.

Clearly, the CCPA provides some legal teeth to protect private information. The CCPA goals go beyond simple compliance, aiming to change the power dynamics between businesses and consumers in the data ecosystem. Businesses, on one hand, have the responsibility to take adequate measures to protect the private data they collect. There are significant checks on corporations regarding data handling procedures/ practices: corporations are required to have a robust data protection measures in place, disclose data collection, and notify affected parties and regulatory agencies of data breaches as soon as possible [Alpert 2020]. Consumers, on the other hand, have legal rights to control their personal information collected by the businesses. They have control on how their data are used, disclosed, and sold. They can sue the businesses for data breaches. The CCPA thus provides a balancing mechanism between businesses' responsibilities and consumers' rights to protect the private information.

There are, however, divergent viewpoints on the imposition of CCPA [Alpert 2020]. Corporate representatives frequently view privacy like a commodity, focusing on operational challenges and economic considerations of the data use[Layton and Elaluf-Calderwood 2019]. Data, after all, are precious commodity in the digital world which can be harvested in various ways for marketing purposes. Laws such as the CCPA incur significant costs of compliance on businesses, along with an increase data maintenance costs. Consumers could shy away from sharing their information, which could otherwise be useful in these marketing campaigns. Consumer advocates on the other hand, stress individual autonomy and protection from data exploitation when they argue that privacy is a fundamental right. This ideological divide has influenced the different interpretations of the provisions of the CCPA, which includes definitions of personal information, opt-out mechanisms, and non-discrimination rules [Baik 2020].

Consumer advocates differ in the extent to which the CCPA could empower consumers to have rights over the data; they argue for more stringent requirements on businesses. The GDPR, which was passed in Europe at the same time as CCPA, holds stricter data portability and imposes more stringent requirements on businesses. The GDPR provisions did have the "Brussels effect" on CCPA [Gunst, Simon and De Ville, Ferdi 2021], but does not go as far in protecting individual data or imposing checks on businesses. Nevertheless, the CCPA is the first such comprehensive legislation in the United States at the state level [Chander and William 2021]. Other states like Colorado, Connecticut, Virginia and Utah have closely followed on California's lead to protect individual privacy. There are still no federal level policy guidelines on protecting individual privacy [Rothstein and Tovino 2019].

3 RESEARCH QUESTION, THEORETICAL FRAMEWORK, AND METHODOLOGY

This article aims to answer a significant question in the above context: Does the CCPA have an impact on the data breaches? This study is possibly among the first to make such an empirical analysis to examine the effect of CCPA on data breaches. CCPA imposes legal requirements on businesses, which should arguably result

in improvement of their data maintenance and security mechanisms, leading to a reduction in the frequency of data breaches in the state. When corporations comply with CCPA, they do not only increase consumer trust but also reduce the possibility of expensive fines and legal ramifications from data breaches [Layton and Elaluf-Calderwood 2019]. Additionally, with CCPA's emphasis on accountability and transparency, businesses are encouraged to take proactive measures with respect to data security and breach prevention. In addition to compliance requirements, the CCPA should bring about a change in the organizational culture concerning data handling. Organizations need to integrate data privacy into their operations and emphasize it as a core value. This shift demands investments in technology, personnel, and processes to ensure ongoing compliance and effective risk management. Hence, our overall presumption is simple: CCPA should result in a reduction in the data breaches in California. There should also be an overall improvement in the data breach notification practices.

We build on the institutional theory to examine the above research question. Institutions form the legal matrix (formal laws and policies) and conventions that act as constraints, as well as opportunities, that structure business processes [North 1990]. Institutions affect transaction costs of the businesses. Thus, in the case of California, the policy imposes costs of compliance with the CCPA law. Literature on transparency shows that the transparency may not, by itself, result in reduction in intended outcomes. Corruption, for example, cannot be reduced only with transparency laws, but require additional legal sanctions for such reduction. In the same vein, even if states impose legal requirements on notification of data breaches, the data breaches are not going to reduce without added legal compliance requirements. The CCPA imposes such legal requirements on businesses to change their business operations and data maintenance processes. To put the institutional environment of California in context, the state has had laws with respect to transparency of data breaches since 2003. Public agencies and businesses are required to notify California residents when they experience a breach of the residents' personal information. Since 2012, businesses and government agencies have also been required to notify the state's Office of the Attorney General (OAG) on breaches affecting more than 500 Californians. As a part of the transparency process, the OAG has been posting the breach notices on the OAG's website. The OAG could take legal action on the entities that experience a data breach. Hence, in our analysis, we examine the impact of the CCPA on the data breaches reported through the OAG. The OAG data are longitudinal, spanning from 2012 to the current year, and are independent of the CCPA requirements. Hence, we are able to compare the breach notifications before and after the implementation of CCPA. Our analysis thus provides institutional insights into the impact of the CCPA on data breaches over time. The OAG dataset of breaches is rich, comprising records of 3,705 organizations, including the names of organizations, the number of breaches they experienced, the dates of these breaches, and the dates the breaches were reported.

3.1 Operationalization of Variables and Analysis

As this study aims to explore the California Consumer Privacy Act (CCPA) by analyzing breach notifications filed with the California Attorney General's Office, it is essential to clarify the distinction between a data breach and a data breach notification. A "data breach" refers to an incident sensitive, protected, or confidential data is assessed, disclosed, or compromised without authorization. This breach may involve various types of data, such as personal information of individuals, financial records, or proprietary business data.

On the other hand, a "breach notification" is a formal communication or reports filed by an organization to relevant authority, such as the California Office of Attorney General (OAG), informing that a data breach has occurred. This notification is a legal requirement under a regulation like the CCPA and often includes details about the breach. Information such as the type of the data that was breached, the extent of breach, and steps taken to mitigate the breach's impacts are included in the notification filing. The OAG breach notification dataset from 2012 to 2023 is thus quite rich in providing details about the breaches. Our unit of analysis here is thus the breach notification, not the breach event itself. Yet, the analysis of breach notifications provides insights into CCPA's impact on breach events. We extracted the following variables from the dataset for analyzing CCPA's impact:

Breach Incident Year (Incident Year): The year in which the data breach occurred. We extracted the year from the date of the breach indicated in the dataset.

Report Year (Reported Year): The year a breach was reported to OAG. We extracted the year from the date a breach report was filed.

Breach Count (Count Breach): The total number of breaches experienced by an organization within a specific year. This is a raw count from the dataset.

Report Count (Count File): The total number of breach notifications filed by an organization in a particular year. Each notification may report a single breach or multiple breaches.

Days Gap Between Breach and Reporting (Days Gap Report): The number of days between the occurrence of a breach and the filing of report. This is calculated by subtracting the breach date from the report filing date for each incident.

Average Number of Breaches Per Report (Avg Breach Report): The average number of breaches included in each filed report. This variable is calculated by dividing the total number of breaches by the total number of reports for each year.

Days Gap Within Report for Multi-Breach Reports (Days Gap Within): The average number of days between breaches when multiple breaches are reported in a single report. This variable is calculated by averaging the days gap for all multi-breach reports filed in a given year.

Since this is an exploratory study of the impact of the CCPA, we mainly focused on descriptive statistics for analytical purposes. Therefore, we are not undertaking any hypothesis-testing yet. Specifically, we aim to advance understanding of the relationship between CCPA and data breach reporting patterns for three reasons. First, we examine which measures are significant in this relationship, comparing them before and after implementation of

CCPA. Second, we investigate potential relationships between such patterns by examining the types of filers or reports. Third, this analysis provides a basis for the model that can be used as a framework for evaluating the CCPA's impact. Thus, this paper sets up the foundation for testing different hypotheses of CCPA's impact on breaches.

4 FINDINGS AND DISCUSSIONS

The OAG dataset spans over 12 years from 2012 through 2023. CCPA was enacted in 2018 and implemented in 2020; hence to discern CCPA's impact, we chose its year of implementation as the intervention year for pre-post analysis. The OAG dataset includes 3,139 entities which gave 3,702 breach notifications covering 4,970 data breaches. In other words, each report contains one or more breaches, with an average of 1.34 breaches. The majority of the notifications (63%, 2,356 total) reported single breach, and the remaining (27% or 1,346) reported multiple breaches. Within these notifications reporting multiple breaches, the range of dates between the first and last breach are quite varied. The patterns in this "within-report" range are indication of the urgency that the filer gives to reporting breach incidents; CCPA could be instrumental in influencing this pattern. Lastly, we can also distinguish between "new entrants" and "repeaters" among the 3,139 reporting entities. 2,838 are the new entrants who reported only one notification during the 12-year period; the remaining 301 are repeaters who filed multiple notifications (totaling 864 notifications).

To examine CCPA's impact, we performed trend analysis to assess changes in breach reporting over time. The trend analysis provides insights into the occurrence of data breaches pre- and post-implementation of CCPA. We analyzed four trends: frequency of breach notifications; types of breach notification filers; pattern of breach notifications; and time gap between an actual breach incident and notification. The first analysis is simply the trend in frequency of breach notifications pre- and post CCPA. The second analysis drills down on two types of notification filers: "single-filers" (who report a single breach per notification) and "multi-filers" (who report more than one breach per notification). This allows us to more closely examine CCPA's impact on filers who have multiple breaches. The third analysis of breach notification patterns provides insights into average number of breaches per notification. It provides insights into the trends in central tendency of breaches across different organizations over time. The fourth time gap analysis examines CCPA's impact on the time gap between a breach and its notification. An important aspect to recall in this context is that CCPA applies to businesses only; the data breach notifications, however, apply for both public and private entities. Hence, our analyses provides insights into CCPA's ecological impact across organizations, rather than private businesses only. The following sections summarize the major findings of CCPA's impact from the trend analysis.

4.1 CCPA's impact on frequency of data breaches.

Figure 1 shows the trend in frequency of data breach notifications annually for the 12-year period. The figure shows that the number of notifications has risen constantly, with an especially sharp rise

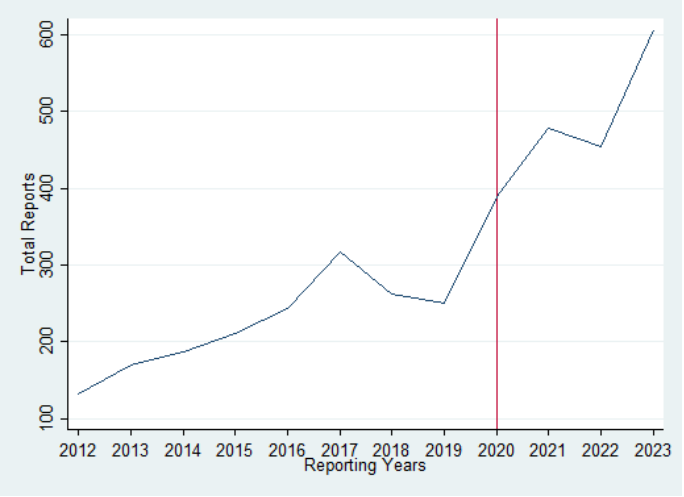

Figure 1: Frequency of data breach NOTIFICATIONS by reporting year

Figure 2: Frequency of data breach COUNTS by incident year

from 2019 to 2021. This sharp increase likely happened in the context of Covid-19, when there was a hike in pandemic-related ransomware incidents. Employees were allowed to work from home in many organizations, which increased the attack surface. However, the organizations themselves may not have had adequate time to be prepared with cybersecurity protections. There are slight dips in two periods (2017-2019 and 2021-2022). The frequency of annual notifications, however, should not be interpreted as if the actual incidents happened in that corresponding year. Rather, the annual notifications simply show that the notifications went out that year, regardless of when the data breach incident actually happened. Hence, we need to interpret this data carefully in relation to CCPA's impact on data breaches.

To take a deeper look, we parsed the data for actual counts of data breach incidents per year during the 12-year period. That is,

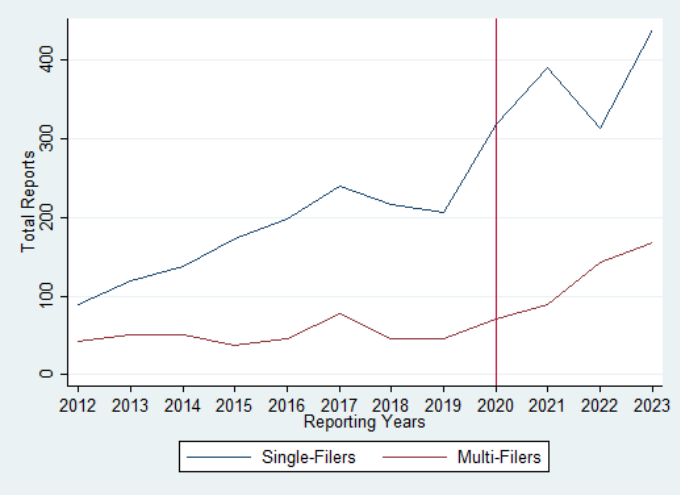

Figure 3: Frequency of data breach NOTIFICATIONS by reporting year, Single vs Multi-filers

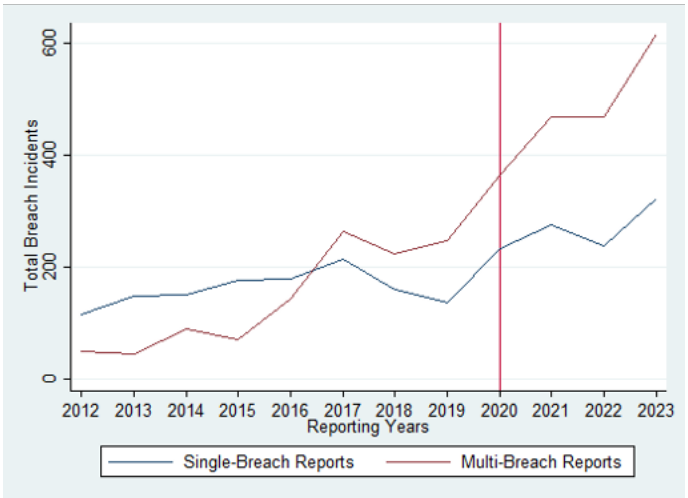

Figure 4: Frequency of data breach COUNTS by incident year, Single vs Multi-filers

we mapped incidents reported in a notification to the year of actual occurrence, rather than associating with the year of notification. Figure 2 shows the overall trend of such actual data breach incidents annually. The chart shows that there is a steep increase in the frequency of data breaches from 2012 to 2020, but reduced sharply thereafter. The overall trend thus does indicate that the frequency of data breaches reduced since the CCPA's implementation. In particular, unlike Figure 1, Figure 2 shows that there is a significant difference in steepness from 2019-20 to 2020-21. There is considerable flattening of data breach incidents between 2020-2021, Clearly, many of the data breach notifications in 2020-21 belonged to those data breach incidents that happened in 2019-20. The frequency of data breach incidents dropped sharply in 2021-22. In fact, there is a parallel trend between Figure 1 and 2 for 2020-21 in terms of the dip. Combined with the flattening in 2020-21, the dip in 2021-22 could be an early indication of the effect of CCPA: businesses had to take more security measures to protect private information.

We should, however, be careful in attributing the overall reduction in data breach incidents to CCPA alone. As mentioned earlier, cybersecurity incidents (particularly ransomware) had increased globally in 2020-21, when the cyberattack, surface had grown exponentially due to remote work in the context of Covid-19. Data breach incidents had also grown significantly in the context of the overall growth in the cybersecurity incidents in 2020-21. The fall in data breach incidents after 2020 could also be coincidental to the overall reduction in the cybersecurity attacks in the post Covid-19 context. In other words, the fall in frequency of data breach incidents may be a reflection of the global ecological rise and decline of cybersecurity incidents. Still, we cannot rule out the impact of CCPA in reducing the data breach incidents after 2020. The causal relationship between the CCPA and the reduction in data breach incidents would require a deeper analysis, examining the other environmental factors and ruling out other spurious relationships.

4.2 CCPA's impact on data breach filers

We examined the differences in trends between those business entities that filed a single notification report of data breach incident (single-filer) vs those that file in the file multiple notification reports of data breach incidents (multi-filers). This examination is useful in the context of CCPA to see if the law nudged both types of filers in the same way. Figure 3 provides a comparison of the single vs multi-filers' notification reports and actual data breach incidents respectively. It shows a steady increase in notification reports before and after CCPA implementation. Yet, there is a difference in the trends between the single-filers and multi-filers. The increase in trend of single-filer notification reports is sharper than that of multi-filers.

This suggests that the CCPA has potentially influenced an increase in reporting activities in general among single-filers. New reporting entities continued to grow. The multi-filers also shows a general upward trend but with a less steep slope, indicating a more gradual increase in report counts over the years. After the introduction of the CCPA, both single-filers and multi-filers demonstrate a notable increase in reporting, with single-filers showing a more pronounced growth. The comparison reveals that while both groups were affected by the CCPA, single-filers' reporting behavior might have been more significantly impacted. The similarities lie in the overall upward trends for both groups, reflecting a broader shift towards increased reporting over the years, likely driven by heightened regulatory requirements and awareness of data breach implications.

Figure 4 also compares the trends of the annual breach incidents reported in single-breach and multi-breach filers. This figure shows interesting divergence between the two types of filers. Annual data breach incidents has increased significantly for multi-breach filers compared to single-breach filers over the years. Multi-breach filers surpassed single-breach filers in 2016-17 and the gap between them widened since then. While the single-breach filers increased modestly since then, the multi-breach filers increased more steeply,

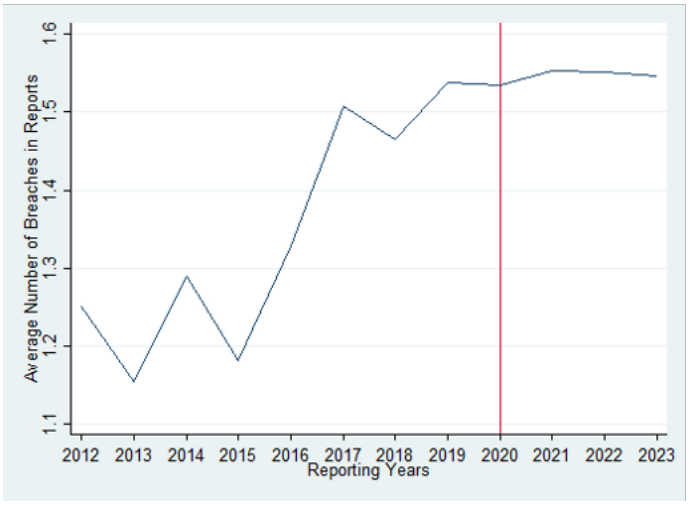

Figure 5: Average number of breach incidents per notification report

accounting for this increasing gap. The pattern shows an increase in tendency to file multi-breaches, which was reinforced after CCPA implementation as well. We do not see similar tendency for single-breach filers. This aspect requires deeper examination for why such divergence has occurred over the years. One hypothesis based on preliminary examination of the two types of reports is that filers have tended to consolidate their notifications of data breaches.

4.3 CCPA's impact on data breach notification pattern

We investigated the pattern of data breach notifications with respect to the number of breach incidents per notification. This examination should show if the CCPA had any impact on the pattern of how businesses report the breach incidents. Figure 5 shows the trend in average ratio of data breaches to notifications. There's a noticeable upward trend in the average number of breaches included in each report leading up to the CCPA implementation in 2020, after which the average has leveled off. This suggests that initially, more breaches were being included in each report, but with the advent of the CCPA, the rate of breaches per notification has stabilized.

The decrease in the average number of breaches per report post-CCPA could indeed be interpreted as an improvement in breach notification, potentially indicating more timely reporting. That is, breaches are being reported as they occur rather than in-groups or batches. However, there could also be other factors at play. For instance, the CCPA and similar regulations have likely influenced the standardization of breach reporting practices, providing clearer guidelines for organizations. Stricter reporting requirements mandated by such regulations could have also resulted in more frequent reporting with fewer breaches per report, reflecting a trend towards prompt disclosure.

At the same time, improvements in cybersecurity measures and proactive prevention strategies could be leading to a decrease in the number of breaches, resulting in fewer breaches per notification. Technological advancements and enhanced security protocols have possibly enabled faster breach detection and isolation, contributing

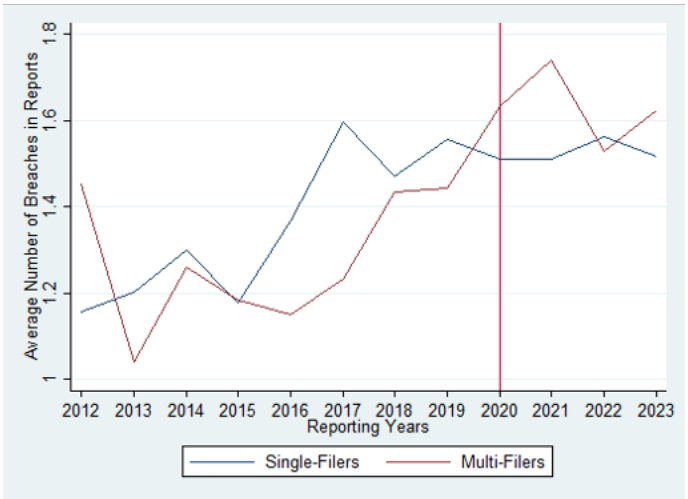

Figure 6: Average number of breach incidents per notification report, Single- vs Multi-filers

to the decline in reported breaches per incident. Additionally, organizations could have refined their risk management strategies, creating more segmented and precise reporting of breaches, which aligns with the observed stabilization in the average number of breaches per report post-CCPA. This multifaceted approach suggests a comprehensive shift towards improved breach notification process in the wake of evolving data protection regulations.

Figure 6 compares the trend of the average number of breaches per notification report filed by single-breach versus multi-breach filers. Both trends exhibit enormous variability over the years. Yet, while multi-filers shows a consistent increase, the single-filers held somewhat steady before CCPA implementation. Post-CCPA implementation, there is a divergence: the average for single-filers is held steady, whereas the average for multi-filers rose before falling. This rise for multi-filers may suggest a possible rush to

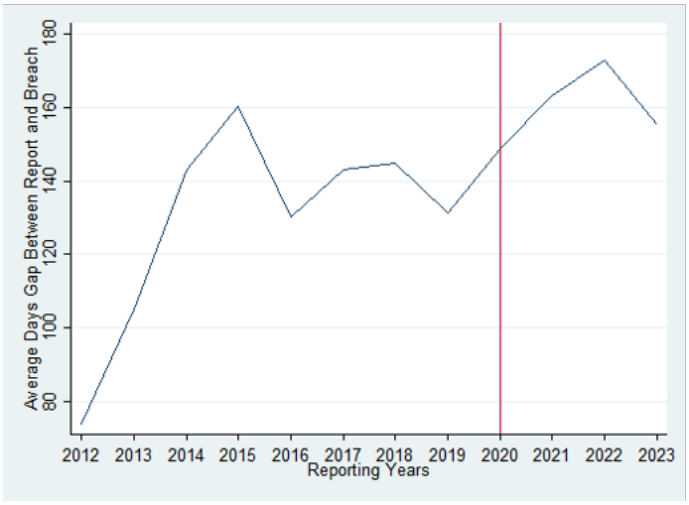

Figure 7: Average days gap between breach and notification

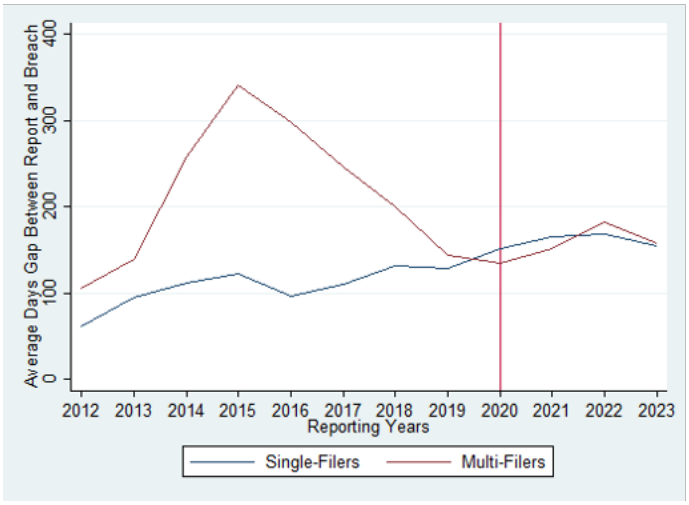

Figure 8: Average days gap between breach and notification, Single- vs Multi-filers

report breaches in the wake of CCPA enforcement, followed by a normalization in subsequent years. The trends suggest overall multi-filers had more volatile patterns in terms of the average number of breaches reported per notification report. They also demonstrate divergence in post-CCPA trends between single-filers and multi-filers in direction compared to those in pre-CCPA.

4.4 CCPA's impact on time gap between data breach incidence and notification

Since CCPA has stringent requirements on the notification of data breaches, we examined if it has had any impact on the time it takes to notify an incident (i.e. time gap between breach and its notification, measured in number of days). Figure 7 shows this graph, tracking the average gap in days between the occurrence and notification of data breach incidents. The graph shows an initial rapid increase followed by fluctuations over the years. The time gap trend kept increasing pre- and post CCPA implementation. The new regulatory environment of CCPA may have thus initially extended the reporting time. Post-CCPA, the graph indicates continued variability, with periods of both increase and decrease in the average reporting gap, reflecting ongoing changes in detection, reporting processes, and possibly the complexity of data breach incidents.

Figure 8 further illustrates the trends in days gap for single-breach filers and multi-breach filers. Although there is a difference between the two types of filers from 2012 to 2019, there is no significant difference in their trends pre- and post- CCPA implementation. The figure shows similarity between the single- and multi-filers. This is further indication that the CCPA may have stabilized the number of days it takes to provide a notification report of a breach incident.

Finally, we examined the time gap within multi-breach notifications. Figure 9 shows the average number of days between when

Figure 9: Average days gap between breach and notification within report

multiple breaches within a multi-breach notification. The trend shows a sharp increase in the time from 2012, peaking around 2016, which suggests that during this period, there may have been delays or complexities in reporting multiple breaches together. Following the peak, there's a consistent decrease in the average time gap, especially after the CCPA's implementation. The trendline reflects a potential improvement in the timeliness of reporting multiple breaches. This decrease could be influenced by the CCPA's requirements for prompt reporting or perhaps enhancements in detection and response processes that enabled organizations to report more efficiently.

5 CONCLUSION

This study on the impact of the CCPA provides an initial preliminary assessment of its impact on data breaches and their reporting. We discovered three general patterns. First, the number of data breaches and reports in California has increased significantly over the last decade; although stricter regulations have been implemented in recent years, we have found no evidence of fewer breaches or reports. Second, the more noticeable patterns before and after the CCPA were on standardized practices or consistency rather than changes in the number of incidents or reports. Third, we found some promising evidence of improved timely reporting in multi-breach reports and multi-filers. However, the causal connection between CCPA and the reduction requires deeper study to rule out spurious relationships. Investigation of the associated notification also shows improvements in the process. There is a steady increase in new entrants filing the breach notifications (especially single-filers). The trend in the average number of breaches included in each notification leveled off after CCPA implementation. Lastly, the time gap between data breach incident and notification also reduced with the CCPA. The notable reduction in the time interval between data breaches and their reporting suggests enhanced reporting practices, potentially influenced by the CCPA's stringent requirements for timely notification. It is evident that the CCPA has catalyzed a considerable shift in organizational data management and privacy compliance.

We must acknowledge certain key shortcomings in this study. This is an exploratory study. Hence, we have not made any causal claims with respect to the influence of CCPA on data breaches. Secondly, we have only 3 years of post CCPA implementation in the study. A more detailed causal examination would require a longer term study. A more holistic long-term study on impacts of the CCPA could also provide insights into the businesses' practices with respect to consumers, Comparative analysis or studies across different states or countries with varying privacy regulations would contribute to a broader understanding of the global impact of such policies. Comparative analyses could reveal common trends and unique contextual factors influencing cybersecurity outcomes.

REFERENCES

[1] David Alpert. 2020. BEYOND REQUEST-AND-RESPOND: WHY DATA ACCESS WILL BE INSUFFICIENT TO TAME BIG TECH. *COLUMBIA LAW REVIEW* 120, 5 (JUN 2020), 1215–1254.

[2] Jeeyun (Sophia) Baik. 2020. Data privacy against innovation or against discrimination?: The case of the California Consumer Privacy Act (CCPA). *TELEMATICS AND INFORMATICS* 52 (SEP 2020), 101431. https://doi.org/10.1016/j.tele.2020.101431

[3] Anupam Kaminski Chander and Margot E. McGeveran William. 2020-2021. Catalyzing Privacy Law. *Minnesota Law Review* 105, 4 (2020-2021), 1733–1802.

[4] Can Chen and Sukumar Ganapati. 2023. Do transparency mechanisms reduce government corruption? A meta-analysis. *International Review of Administrative Sciences* 89, 1 (2023), 257–272. https://doi.org/10.1177/00208523211033236 arXiv:https://doi.org/10.1177/00208523211033236

[5] Gunst, Simon and De Ville, Ferdi. 2021. The Brussels effect : how the GDPR conquered Silicon Valley. *EUROPEAN FOREIGN AFFAIRS REVIEW* 26, 3 (2021), 437–458.

[6] Roslyn Layton and Silvia Elaluf-Calderwood. 2019. A Social Economic Analysis of the Impact of GDPR on Security and Privacy Practices. In *2019 12TH CMI CONFERENCE ON CYBERSECURITY AND PRIVACY (CMI)*. CMI; IEEE Denmark Sect; Wireless World Res Forum; Smart City Cluster Denmark, IEEE, 345 E 47TH ST, NEW YORK, NY 10017 USA, 74–79. https://doi.org/10.1109/cmi48017.2019.8962288 12th CMI Conference on Cybersecurity and Privacy (CMI), Aalborg Univ Copenhagen, Copenhagen, DENMARK, NOV 28-29, 2019.

[7] Douglass C. North. 1990. *Institutions, Institutional Change and Economic Performance*. Cambridge University Press, Cambridge.

[8] Mark A. Rothstein and Stacey A. Tovino. 2019. California Takes the Lead on Data Privacy Law. *HASTINGS CENTER REPORT* 49, 5 (SEP 2019), 4–5. https://doi.org/10.1002/hast.1042