How Understanding Legislation In California Can Clarify Data Privacy Responsibilities

A Research Paper submitted to the Department of Engineering and Society

Presented to the Faculty of the School of Engineering and Applied Science

University of Virginia • Charlottesville, Virginia

In Partial Fulfillment of the Requirements for the Degree

Bachelor of Science, School of Engineering

Jordan Crawley

Spring 2023

On my honor as a University Student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments

Advisor

Pedro A. P. Francisco, Department of Engineering and Society

Introduction

The Internet has doubtlessly been one of the most important technological innovations developments of the last century. Needless to say, it's also come a very long way since its original inception in the late 1960s. Many would likely agree that overall, the Internet has been a boon to society in many ways. To name just a few, the Internet allows us to experience generally increased ease of living, increased and speedier access to information, and even increased social connection over distances and with people we might not otherwise interact. This makes the Internet one of the most important technological innovations in the last century. As predicted by Stansberry, Anderson, and Raine in their 2020 article *The Internet will continue to make life better*, the Internet's relevance will only increase as time goes on (Stansberry et al., 2020, para. 3), and more and more of our society will become intertwined with the use of the Internet as well as the storage of information therein. However, the increasing intertwining of the Internet with our daily lives also means that protecting personal data has become more important than ever. Even so, the United States has really lagged behind in this area compared to other countries, such as the European Union.

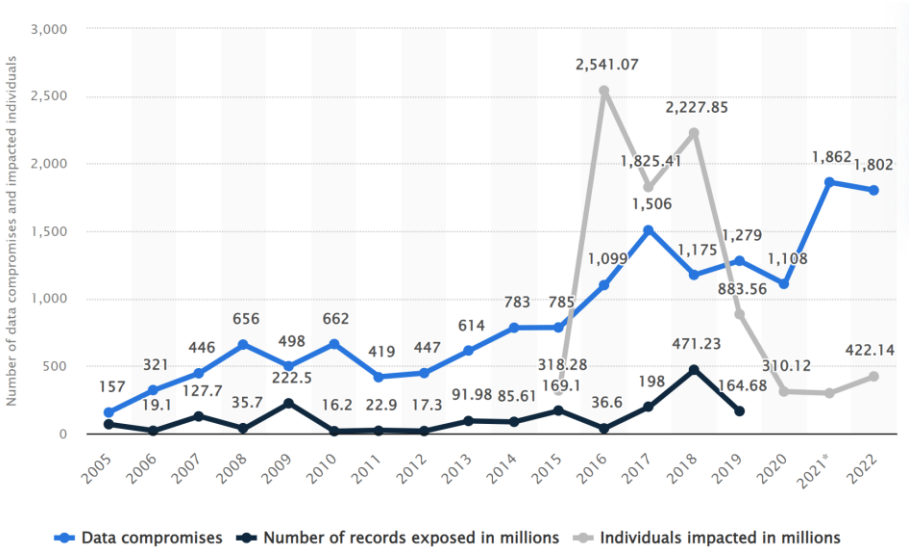
One state in particular though, California, is the exception to this statement, as their legislation has been made much clearer over time. Therefore, by analyzing California's data privacy legislation and how it came into being, it might be easier to form a more concrete legal understanding for the rest of the U.S. to follow regarding the topic. This is especially true if one looks at the legislation through the lens of Actor Network Theory, examining the relationships between the government, cybercriminals, companies, individual users, etc., as proposed by California's legislation.

Background and Significance

Just as the Internet continues to expand, so too do the concerns that arise around it. One such concern is the rise of cybercriminals and cyberattacks, which have recently become a big concern for both individual users of the Internet and large companies. These attacks often threaten to steal user information, which cybercriminals can use to identify users, resell elsewhere, etc. As a society, we've seen an increase in large-scale data breaches in recent years, demonstrated in figure 1 below. This trend is predicted to continue over time as more and more aspects of our society become interwoven with the Internet.

Figure 1

Large Scale Data Breaches 2005-2022



This risk of data breaches, in addition to general concern of personal data misuse by companies, the government, etc., also give rise to another important issue: it highlights the importance of everyone in our society being on the same page in regards to understanding what responsibilities exist between users, companies, the government, cybercriminals, etc., when an incident regarding user personal data does occur. Without such clarity, it is difficult to decide who is at fault or what sort of consequences, if any, are viable when these events do occur.

However, as it is now, there is a distinct lack of understanding of these responsibilities and how they may impact consequences of a data breach or similar incident. This is especially true in the United States, as legislation regarding these areas is largely unclear.

Methods

In order to form a full picture of how the United States might learn from California's legislation, it is important to examine a few key documents. Firstly, and arguably most importantly, it is important to examine the legislation of the state of California itself. Namely, the two big documents that make up the bulk of California's recent data privacy legislation, the CCPA and CPRA, are both important to understand in order to get a working understanding of the actual changes made themselves. In addition, it is also important to examine accounts made through articles and other small literature that details the actual history of these changes and the circumstances surrounding the documents as they were developed. These accounts will give an idea of why certain changes were made, as well as what justified the changes in the eyes of the involved parties.

Lastly, it is also important to examine modern discussion from area experts and other commentators regarding the recent legislation in California. Doing this will give a glimpse into the success of the legislation thus far, as well as current public reactions to the changes by the most interested parties. The reactions of these parties are important to understand, of course, because they may indicate the likelihood of further revisions to the legislation as well as inform speculation on how the larger public across the United States might react if similar changes were made.

Results and Discussion

California's data privacy legislation is comprised of two main documents. These are the California Consumer Privacy Act (CCPA) and the California Privacy Rights Act (CPRA). The CCPA was signed into law in June of 2018 and took effect in January of 2020, while the CPRA was signed into law in December of 2020 and took effect in January of 2023. The CPRA is considered by many as an expansion of the CCPA, as it primarily amends and expands on the CCPA's existing provisions.

The CCPA imposes explicitly-stated obligations on businesses, service providers, and third parties to guarantee certain rights to consumers (individual users) under penalty of law. These rights are, in order; the right to know personal information collected by the business about the consumer, the right to delete personal information collected from the consumer, the right to opt-out of the sale of personal information, the right to opt-in to the sale of personal information of consumers under the age of 16, the right to non-discriminatory treatment for exercising any rights, and the right to initiate a private cause of action for data breaches. The CCPA also clearly states that violations of the act or failure to uphold these protections is the fault of the aforementioned responsible parties and makes said parties liable to civil penalties, as well as enables consumers to receive damages and/or non-monetary relief on a case-by-case basis (California Consumer Privacy Act. 2018).

In addition to further defining key terms used in the CCPA and addressing some more specific case-by-case violations, the more recent CPRA also adds a fourth category, contractors, to the list of responsible parties, and also adds two additional protections for users. These new protections are, in order, the right to correct inaccurate personal information and the right to limit use and disclosure of sensitive personal information (California Privacy Rights Act, 2020).

Notably, the legislation that would eventually become the CCPA was redrafted and amended many times from its inception in 2016 all the way until 2019. Analyzing the history of these changes is key to understanding the impact various sociotechnical factors had on the legislation's development, so it's worth investigating. The origins of the CCPA can be traced back to a slightly older document, the General Data Protection Regulation (GDPR), which was adopted by the European Union in April of 2016. The European Union, in addition to modern California, is widely regarded as having much clearer legislation and enforcement of data privacy compared to the broader United States, and much of that clarity is due to this particular piece of legislation.

At the time of its inception, the GDPR became a huge and important actor in the tech world at large and in the network of California data privacy as a whole. California has the undisputed largest tech industry of any state in the US, with almost double the tech-related workforce size of the next ranked state (High Tech, 2023). The tech industry being so important to the state naturally meant that handling changes introduced by the GDPR would be important for the many companies that worked there. As such, tech companies collectively spent several millions of dollars hiring lawyers and legal counsel just after the GDPR was adopted to ensure they wouldn't violate the specified protections in their operations overseas. Overall, this incident indicates that the simple act of seeing data privacy legislation successfully implemented was enough to influence those who may foresee themselves being affected to consider taking steps adapting said legislation on a larger scale.

The existence and adoption of this document, which brought forth clear data privacy policies that placed an emphasis on user protection and consumer empowerment, also became popular with those working or interested in the area of data privacy throughout the United States,

and especially in California. Only one year later after this document was adopted, in October of 2017, Alastair Mactaggart, Rick Arney, and Mary Stone Ross filed a ballot initiative in the state of California, the specifications included in which would ultimately become the base of the CCPA. According to an article posted on the information and enterprise technology news website, CIO Dive, it is believed that Mactaggart was inspired to file the initiative after a reportedly disturbing conversation at a dinner party with an ex-Google engineer, wherein the engineer told Mactaggart "if people just understood how much we knew about them, they'd be really worried" (Schwartz, 2019).

As a real-estate developer, Mactaggart had little experience in actualizing the necessary steps to achieve the legal protections he envisioned, so he enlisted the help of Arney, a finance executive who had worked in the California Senate 20 years ago. Neither Mactaggart nor Arney were particularly experienced in privacy policy, but still understood the implications of their current state of privacy affairs and the necessity of change. So, they enlisted the aid of Ross, another neighborhood friend who previously worked at the CIA and had a better understanding of privacy expertise (Wakabayashi, 2018). This incident is an excellent example of how even everyday individuals in the state, when made aware of their lack of privacy rights and potential ramifications, are capable of taking steps toward change. It also paints a picture as to the perceived importance of data privacy legislation to the general public of California.

Only 2 months later, in December of 2017 the California Secretary of State announced that the ballot initiative proponents, who adopted the name "Californians for Consumer Privacy", would need to collect petition signatures. Specifically, they'd need at least 365,880 registered Californian voters to approve of the initiative for it to appear on the next ballot. In only a year, the initiative had instead garnered over 600,000 votes, indicating the immense public support of

the proposed protections. Eventually though, Assemblymember Ed Chau of the California Senate Committee on Rules proposed S.B. 1121 in early 2018, a bill which contained almost identical language in many areas as the language introduced in the ballot initiative. It is speculated by many that this bill was conceived as a direct response to the ballot initiative amid growing public interest in data privacy and increasing ballot signatures (Greenberg, 2020).

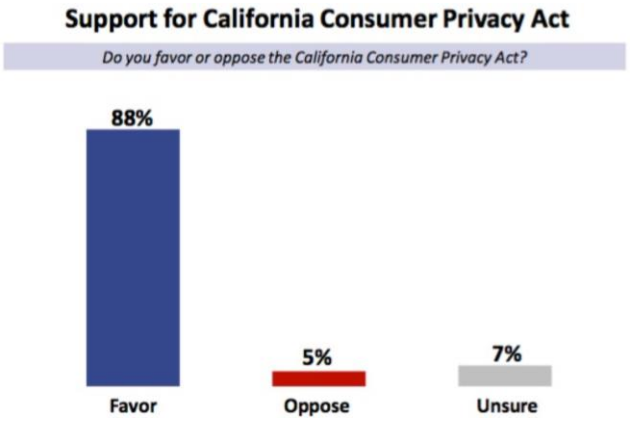
This claim is also substantiated by the fact that the Californians for Consumer Privacy reportedly reached a deal with state legislators to withdraw the proposed ballot initiative if S.B. 1121 was passed and signed by the Governor. After withdrawing the ballot in June of 2018, it was approved in the same month. The enthusiastic coverage of the ballot by media at the time, as well as its constant discussion over the months leading up to its adoption by both legislators and the Californians for Consumer Privacy indicate overwhelming public support of the policies that the legislation would bring into action. Chau, who lead the California Assembly's Privacy and Consumer Protection Committee in addition to proposing the bill, even called the event a "historic step" for California consumers (Greenberg, 2020).

The CPRA's history is substantially less involved than that of the CCPA. All in all, legislators decided after receiving feedback from both companies and the public, as well as reviewing the CCPA's documentation, that it was best to expand specific protections granted by the CCPA and to clarify the designated outcomes of specific incidents, including increased penalties for misuse of personal information belonging to minors and fines related to newly defined "sensitive data" (Pfeifle, 2022). Thus, the CPRA was effectively tacked onto the CCPA's existing clauses as a list of amendments. This shorter and simpler history has also earned the CPRA the nickname of "CCPA Version 2" or "CCPA Part 2" by some parties.

Overall, public reception of the CCPA and CPRA have been overwhelmingly positive, at least within the state of California itself. This is further illustrated by the figure below, which shows statistics taken from a survey conducted by the Californians for Consumer Privacy in 2019 regarding the public's reception of California's new data privacy legislation.

Figure 2

Public Reception of CCPA (Velazquez, 2020)



Conclusion

Observing both the history and current state of California's data privacy legislation can lead yield several key takeaways that may help to better inform upcoming data privacy legislation as it continues to develop throughout the rest of the United States. Firstly, it's important to analyze some of the key actors that influenced the development of said California legislation. The most prominent of these to observe include California legislators, the general public of California, existing documentation/policies, tech companies, and the international technology industry/economy.

The role of California legislators should not be overlooked in this network. The state's legislators have consistently shown a willingness to reach a consensus on difficult to grasp topics

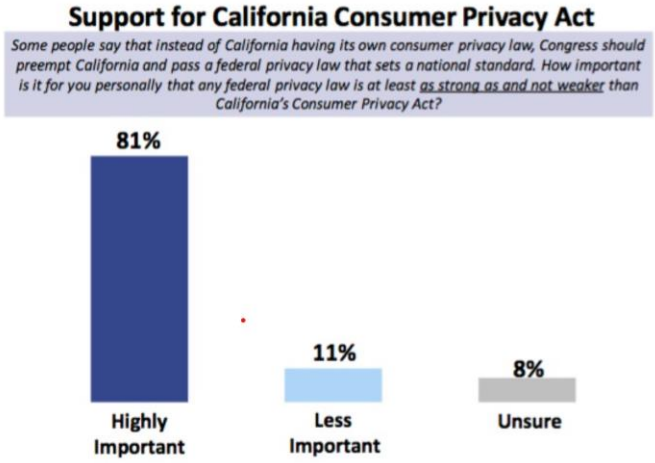
in the tech industry, even working alongside subject matter experts where necessary. Through the amendments made through the CPRA and other smaller legislation, the legislators have strived to place importance on creating understandable legislation using clear and precise language to avoid ambiguous responsibilities ensure fairness for both consumers and companies throughout the development of the state's laws.

If data privacy legislation was to be implemented on a larger or federal scale, adapting these existing clarifications and definitions would be essential to speeding up the process of creating smooth and easily-understandable legislation. Just as the GDPR served in a way as a sort of basic template for California to develop the CCPA and CPRA, the CCPA and CPRA could now be used analogously by the rest of the United States to decide what clauses should be included in larger scale lawmaking. Doing so should help to eliminate the extra months and years of discussion and legal slowdowns that occurred as California developed their legislation, now that working definitions and clear policies are already in place within the US.

Furthermore, the results of upcoming data privacy efforts throughout the United States will be largely dependent on the attitudes of the public, as well as their level of awareness regarding the use and misuse of their personal data. Figure 3 below visualizes the opinions of 777 registered California voters when surveyed by the Californians for Consumer Privacy on whether they think subsequent federal law should be at least as strong as the CCPA and not weaker. As pictured, the results found that respondents overwhelmingly placed high importance on this idea.

Figure 3

Public Support of CCPA Strength (Velazquez, 2020)



If the opinions shown in this survey are anywhere near consistent for a national sampling, one might imagine that federal data privacy legislation could be on its way sooner rather than later. However, it is also important to remember that the opinions of California voters are likely also influenced by the fact that so much of the state's economy revolves around the tech industry. Thus, it is possible that Californian citizens possess a heightened awareness and investment in data privacy policy as compared to citizens in other states.

With these factors identified, one possible path to seeking out high-quality data privacy legislation in the rest of the country could be to increase education with regards to the current state of data privacy for the average US citizen, as suggested in an article by Daphne Leprince-Ringuet (Leprince-Ringuet, 2019). Were all citizens as data-conscious as Californians, the United States might see action taken on the issue faster than it is being taken at present.

References

Bea, & VandenBerk. (2020). *California and Europe lead the way on data privacy – more states to follow*. Bea VandenBerk Attorneys at Law. Retrieved April 2023, from https://www.beavandenberk.com/ip/computer-internet/california-and-europe-lead-the-way-on-data-privacy-more-states-to-follow/

Bloomberg. (2023). *California Consumer Privacy Laws – CCPA & CPRA*. Bloomberg Law. Retrieved April 2023, from https://pro.bloomberglaw.com/brief/california-consumer-privacy-laws-ccpa-cpra/

California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq. (2018).

California Consumer Privacy Act (CCPA). State of California - Department of Justice. (2023, May 1). Retrieved May 2023, from https://oag.ca.gov/privacy/ccpa

California Privacy Rights Act, Cal. Civ. Code § 1798.100 et seq. (2020).

Greenberg, J. (2020, July 1). *California privacy legislation: A timeline of key events*. Future of Privacy Forum. Retrieved April 2023, from https://fpf.org/blog/california-privacy-legislation-a-timeline-of-key-events/

High Tech. California Governors Office of Business and Economic Development. (2023). Retrieved April 2023, from https://business.ca.gov/industries/high-tech/

Ingram, C. F. and D. (2019, May 14). *California's new Data Privacy Law could change the internet in the US*. CNBC. Retrieved April 2023, from https://www.cnbc.com/2019/05/14/california-consumer-privacy-act-could-change-the-internet-in-the-us.html

Leprince-Ringuet, D. (2019, December 20). *What is the CCPA? Everything you need to know about the California Consumer Privacy Act right now*. ZDNET. Retrieved April 2023, from https://www.zdnet.com/article/california-consumer-privacy-act-everything-you-need-to-know-about-the-ccpa/

Paul, K. (2019, December 30). *California's groundbreaking privacy law takes effect in January. what does it do?* The Guardian. Retrieved April 2023, from https://www.theguardian.com/us-news/2019/dec/30/california-consumer-privacy-act-what-does-it-do

Petrosyan, A. (2023, April 1). *Annual number of data compromises and individuals impacted in the United States from 2005 to 2022*. Statista. Retrieved April 2023, from https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/

Pfeifle, S. (2022, August 24). *The Experts Guide to California Privacy Law | CCPA & CPRA.* Osano. Retrieved April 2023, from https://www.osano.com/articles/california-privacy-laws-ccpa-cpra

Ranger, S. (2019, November 4). *GDPR is missing the point, says Edward Snowden*. ZDNET. Retrieved April 2023, from https://www.zdnet.com/article/gdpr-is-missing-the-point-says-edward-snowden/

Stansberry, K., Anderson, J., & Rainie, L. (2020, July 9). *The internet will continue to make life better.* Pew Research Center: Internet, Science and Tech. Retrieved August 1, 2022, from https://www.pewresearch.org/internet/2019/10/28/4-the-internet-will-continue-to-make-life-better/

Schwartz, S. (2019, May 22). *How a real estate developer gave California a head start in data privacy legislation*. CIO Dive. Retrieved April 2023, from https://www.ciodive.com/news/how-a-real-estate-developer-gave-california-a-head-start-in-data-privacy-le/555012/

Sirota, D. (2019, November 14). *California's new Data Privacy Law brings U.S. closer to GDPR*. TechCrunch. Retrieved April 2023, from https://techcrunch.com/2019/11/14/californias-new-data-privacy-law-brings-u-s-closer-to-gdpr/

de la Torre, L. (2020, May 6). GDPR matchup: The California Consumer Privacy Act 2018. Retrieved April 2023, from https://iapp.org/news/a/gdpr-matchup-california-consumer-privacy-act/

Velazquez, N. (2020, September 18). *Key findings from California Privacy Survey*. Californians For Consumer Privacy. Retrieved April 2023, from https://www.caprivacy.org/icymi-summary-of-key-findings-from-california-privacy-survey/

Wakabayashi, D. (2018, May 14). *Silicon Valley faces regulatory fight with California Ballot Measure*. SFGATE. Retrieved April 2023, from https://www.sfgate.com/business/article/Silicon-Valley-faces-regulatory-fight-with-12913625.php