Assessing the Impact of the Implementation of the California Consumer Privacy Act on the United States through Policy Evaluation

by

C.G.J. Putman

S1596179

c.g.j.putman@student.utwente.nl

Submitted in partial fulfillment of the requirements for the degree of Master of Science, program Public Administration, University of Twente

2019/2020

Supervisors:

Dr. S. Donnelly - Mr. Dr. L.C.P. Broos

Faculty of Behavioural, Management and Social Sciences (BMS),

Public Administration (PA)

Summary

As of January 1st, 2020, the state of California has implemented a new law aimed at protecting the (digital) privacy of their citizens. This law, the "California Consumer Privacy Act" - CCPA, is often dubbed the American counterpart of the in European "General Data Protection Regulation" - GDPR. In this research, the process of how the CCPA came into place is explored, the contents of this new law are being examined, and possibly far reaching consequences are being discussed through a combination of qualitative and quantitative research methods. Possible consequences of the law are examined through available data, published by government institutions on state level. Possible reach of the law is examined through examining the territorial and material scope of the law and comparison with the GDPR. An important aspect of this research is to discover if the California effect is occurring, and to which extent. The extent to which the California effect occurs is important to determine the possible negative consequences to the state of California, primarily on economic terms.

First of all, through analysis of the legislative process and the legal documents corresponding to the CCPA as published by the state of California, the thought and development processes in the process of designing the CCPA are examined. Since the regulation has only just been actively implemented, it is difficult to perform an observation of the effects this regulation has. Nevertheless, employment data is examined to see if any trends can be spotted, and if the official state growth predictions have changed between pre- and post CCPA times. Continuing on this respect, parallels with GDPR are drawn to predict the consequences of this new statewide privacy regulation. Furthermore, through a process called the California effect, it has been discovered that restrictive regulation as implemented in California is likely to spread to other states or even the United States as a whole. By combining information from both of these areas with leading theories in the field of Public Administration, Business Administration and others, a substantiated prediction is made about the future of this law and its consequences.

Results show that more than half of US states have, at time of writing, at least discussed researching consumer data privacy regulations. This at least partially supports the hypothesis regarding the presence of the California effect. Nevertheless, only three have succeeded in actually implementing such regulations. Furthermore, no real negative economic consequences due to the implementation of announcement of the CCPA in 2018, or the implementation of the act in 2020 could be observed. Both the rise of consumer data privacy regulations as well as the economic consequences should be monitored and observed in the near and further away future, and should be analyzed again in future academic research.

1. Introduction

Technological developments and innovations have always posed a challenge for policymakers. This has been the case in the past, with inventions like the car or the firearm, as well as in current days with developments in the area of information technology like artificial intelligence, big data and the internet of things. With such developments, questions arise with respect to how and if standing rules and regulations should be adapted to these changes, or if new regulations should be drawn up to prevent powerful parties from exploiting the average citizen. Such a discussion has been going on in the past several years as well, this time due to the growing influence of large tech companies (commonly referred to as Big Tech) and their data collection methods.

In 2016, the European Union initiated the General Data Protection Regulation (GDPR) to protect personal data and the privacy of all individual citizens of countries in the EU. Furthermore, it also assesses the transfer of data from countries within the EU zone and outside the zone, like the United States. Following in the footsteps of the EU, the state of California, home to Silicon Valley providing corporate space to the major tech giants in the world such as Google, Facebook and Amazon, adopted similar regulations to the GDPR. The so-called California Consumer Privacy Act (CCPA) was passed in 2018 and is viewed as its American counterpart. While these regulations apply only to the 40 million residents of the state of California, these regulations have significant effect on the corporations conducting any activities within this state which have to comply with them. These include the earlier mentioned Big Tech companies. It is interesting to see which possibly far reaching consequences the implementation of these regulations have on the United States' cyber landscape through a process called the "California Effect".

1.2 Scientific and Social Relevance of this Research

Previous research on this topic is scarce, which makes sense as the researched phenomenon is quite a recent one. The CCPA was signed into law in 2018, but has only become effective as of January 2020. Previous research directly related to this field (not related to privacy regulations in general) has mainly focused on comparisons with other privacy regulations such as the EU GDPR, the effect of these regulations on corporate life, and lastly how to comply with these newly implemented regulations. Prime examples of previous research conducted in this field are as follows:

1. Bukaty (2019) focuses on how to comply with these rules and regulations, from a market point of view.

2. Chander et al. (2019) researches what caused the sudden uptake in states designing and passing data privacy laws.
3. Marini et al. (2018) introduces an extensive analysis to present a comparison of the CCPA with the GDPR.

It is clearly visible that there is not yet a comprehensive review available which makes clear the process which has led up to designing and implementing this new privacy act. By combining research as mentioned above, especially those as presented in Chander et al. (2019) and Marini et al. (2018) with newly collected data and theories in and outside the field of public administration, insight can be gained in the possibly far reaching consequences of this regulation. This might serve as a predictor for new statewide legislation to come in the future, as well as serve as an indication of steps to take as governing bodies in response to the initiation of this new act.

In respect to the possible social relevance of this research: it is important to have knowledge of how this new type of regulation has come to life. Over the coming years, Big Tech will continue to have an increasingly important role in the life of the average consumer. More and more data will be collected, and citizens have a right to know what happens to their data and have a right to deny the usage of their data for any type of (commercial) gain. By having knowledge of this process, citizens might be able to instigate change in their state, or it might be possible to predict which area is next in regards to this privacy conscious process. This could provide citizens with the privacy that they deserve, or at least give them control to gain back the privacy they once lost.

1.3 Research Question and Sub Questions

For this thesis, a desk research will be conducted which will focus on evaluating the policy itself, the (possible) effects of the policy implementation and the process which lead up to the design and implementation of this policy. To do so, a research question and a set of sub questions have been formulated. The main research question is as follows:

1.3.1 Main Research Question

What possible economical and regulatory consequences could the implementation of the California Consumer Privacy Act have on the different U.S. states, and more specifically, the situation of the state of California?

1.3.2 Sub Questions

1. What are the intended consequences of the CCPA, as drawn up in legal documents by the California legislative bodies?
2. What may be the unintended consequences of the CCPA on the market environment and economy of the state of California in relation to its competitor states? That is, will California see businesses move out of the state to seek refuge elsewhere?
3. Given the territorial scope of the CCPA, and when compared to the similar case of the European GDPR, what could be the possible reach of consequences for areas outside of the state of California?
4. Given the CCPA, which regulatory responses might one expect of other states of the United States as a reaction to the implementation of the CCPA in the state of California?
    - For this sub question four different hypothetical scenarios have been identified. These are as follows:
        i. No active response
        ii. Replicate
        iii. Slim down
        iv. Super-equivalence (gold-plating)

2. Theoretical Framework

What follows is some theoretical context which will form the foundation of many aspects of this research paper. First of all, a short literature review is conducted to determine previous work which has been conducted in this field. This primarily concerns papers which relate directly to the CCPA, GDPR or other privacy regulations. Secondly, the theories of the California effect by David Vogel (1995) and the Delaware effect by Daines (2001) are elaborated on. This is followed up by an analysis of more recent work on these two topics, including a novel theory which is dubbed the Brussels effect, and relates closely to the work of Vogel.

2.1 Brief Literature Review

As indicated in the previous section, there are three prime examples of previous research conducted on the field of the California Consumer Privacy Act, or the increase in privacy related regulations in general. Furthermore, there are some other sources of literature which might prove to be useful in this research. What follows is a short overview of these scientific sources, with a summary and explanation of why these can prove to be useful for this research.

Bukaty (2019) provides an extensive analysis of the CCPA, decomposing the regulation into the most important aspects and explaining ambiguous elements where necessary. Furthermore, it provides recommendations and guidelines on how to comply with this new regulation from a corporate point of view. Because of this, it could provide important insights into understanding the technical legal components of this regulation, as well as to understand the consequences of this regulation to the market.

Chander et al. (2019) researches the more general developments in regards to the sudden increase in privacy and data related regulations in the United States. Again, as is common in research in this field, parallels are drawn to the European GDPR, as it is believed this could have catalyzed these developments. Throughout this research, it is argued that instead of Brussels, it is California and its GDPR that has catalyzed the spread of privacy related laws across the country. To go even further, the authors raise the question why Europe's data privacy approach has failed to instigate similar processes in the US for over 20 years. The conclusions of this research might especially prove to be useful to be able to answer sub question 3 and sub question 4.

Fenwick et al. (2016) describes multiple approaches on how to regulate technology in a situation where policymakers find it difficult to keep up, and compares this to how policymaking has been done up to this date. By making use of more proactive, dynamic and responsive lawmaking methods, innovation can still be promoted while safeguarding citizens from taking advantage of large tech companies. It provides three principles on how to regulate the world of tomorrow, which one could say is today. This could help provide insight into why certain considerations were taken or discarded during the design process of the CCPA, as well as explain why the state of California has always taken an approach of proactive implementation of laws and regulations before issues related to technological developments become apparent.

Marini et al. (2018) compares the CCPA with the earlier implemented European equivalent, namely the General Data Protection Regulation, which is aimed at every organization which wishes to do business within the European Union and processes personal data of its clients. Drawing this parallel could provide insight into if the CCPA is inspired by the GDPR, which consequently could be used to predict the consequences of this regulation. After all, the GDPR has been active for several years now which makes it possible to perform an analysis based on observation of consequences related actions.

Vogel (1995) describes the so-called "California Effect". This encompasses the shift of regulations (primarily in regards to consumer and environmental protection) to more stricter standards. Many regulations which were initially adopted by the state of California were consequently adopted by more

states of the United States, or even the entire country. Based on this described effect, an analysis may be conducted to see if it is likely that an adaptation of the CCPA will be adopted in other states as well. This might help answer research question 4, especially when combined with literature as described in Chander et al. (2019).

2.1.1 California Effect

Over the past couple of decades, the state of California has shown to implement many progressive legislations primarily focused at defending consumer rights and protecting the environment from exploitation of (mostly) large multinationals. As widely known, the state of California houses many large (tech) companies which contribute significantly to the state's economy and the economy of the United States as a whole (Evans, 2019). These regulations often go beyond national legislation. The first prime examples of such stricter, or more progressive regulation can be seen after the implementation of the federal "Clean Air Act", introduced in the year 1970 (Sivas, 2018). After this act was initiated on a national level, the state of California has gone far beyond the requirements of this regulation to (mainly) protect their own environment and limit pollution, as well as protect their citizens from other types of exploitation by larger parties (as often in such cases, when not taken care of properly, there is a risk of creating a David vs Goliath situation). This process of shifting towards stricter regulatory standards than nationally is required was first described in literature by Vogel (1995), and was dubbed as the "California Effect".

A consequence of implementing more stricter state legislation is that it is likely these regulations are also imposed on anyone wishing to do business with companies or consumers within the state of California. According to Vogel (1997), this process takes place in a number of steps. First of all, a legislative body of a state, country or any other geographical region may deny market access of a product of a certain company or country of origin to their region if it does not comply with the rules and regulations set by this legislative body. Depending on the economic importance of such a region, this may result in the entire production line of such a company being adapted to adhere to these stricter regulations. According to Princen (1999), this is often less expensive than altering the production line to produce an alternative product with slight deviations. Such companies might consequently advocate for stricter regulations in their home region as well, as this would eradicate the competitive disadvantage of having to produce higher quality goods when compared to cheaper products aimed solely at the domestic market. In the case that legislation imposes stricter regulations on countries as a whole, it is likely the government of such a country is involved much more directly, as economic impact reaches beyond individual cases.

2.1.2 Delaware Effect

While the state of California has a history of implementing stricter rules than national legislation, the state of Delaware is known for doing the exact opposite. Taking advantage of such differences in regulations, speaking from a corporate point of view, is called "regulatory arbitrage". The state of Delaware has in the past created a legal climate which is (was) very attractive to corporations in the United States, by, for example, not requiring any state sales and corporate income taxes. To be able to profit from these (lack of) regulations, in such situations (and in the case of the state of Delaware), it is not always necessary to have one's headquarters situated in the state. Establishing a subsidiary branch in the state might be enough to adhere to local regulations and therefore profit from these tax benefits. Economically speaking, this can pay off significantly for both the state and the corporations. And, according to figures of the Delaware Division of Corporations (n.d), this indeed does pay off for the state of Delaware. It is indicated that over 1 million corporations have chosen the state of Delaware as their home, while approximately 66% of all Fortune 500 companies (which ranks US companies based on their yearly total revenue) have a legal seat in this state. As a consequence, Delaware is heavily reliant on these corporations to retain their legal status in their state, as a significant percentage of state revenues is collected through fees originating from these companies. Recent numbers are unknown, but according to Romano (1985), these once totaled around 20% of total state revenue.

According to Daines (2001), the reason for this attractive climate for corporations is manyfold. Firstly, the rules and regulations, including court precedents, are advantageous towards businesses. Furthermore, it is the only state which has its own specialized Chancery Court, to resolve corporate law disputes. Continuing, the laws and regulations in Delaware are well known, and relatively certain. Lastly, the state of Delaware is known to quite quickly adapt its rules and regulations to respond to the changing needs of the changing corporate climate. Some experts argue that, due to the earlier mentioned dependency on revenue generated from business fees, it adjusts its laws, regulations and processes to aid influential businesses just so that they keep their legal seat in their state. This could cause a so-called (inter)national race to the bottom: if other states wish to attract businesses to their state as well, there are little options except for loosening their regulations as well. Similar situations can even be seen within the European Union, where standardization and unionization is normally seen as an important goal. Member states Luxembourg, Ireland and the Netherlands are all present in the tax-haven top ten of Hines (2010), ITEP (2017) and Zucman (2018). National, or in this case, even international standards on corporate and tax law might prove to be one of few options to counter this slippery slope.

2.1.3 Recent Developments

2.1.3.1 European Union/Brussels Effect

Besides the California and Delaware effect, increased attention is paid on the power of unionizing effects like the European Union in countering the Delaware effect and improving its own market position through a process similar to the California effect. This process, in the case of the European Union described by Bradford (2012) as the Brussels effect, entails the use of the global power (in both terms of political influence and market size) the EU has to influence local regulations through its legal institutions and standards. Over the past decades, the EU has successfully exported its rules and regulations internationally which is slowly leading to Europeanization of important aspects of global commerce. Examples of areas of laws and regulations which are influenced are plentiful, including measures concerning antitrust, privacy, health and environmental law. A recent example of such regulation is the General Data Protection Regulation of 2016, which is said by many to have influenced the adoption of the California Consumer Privacy Act of 2018.

2.1.3.2 Delaware Effect

In (somewhat) recent years, research has focused on re-evaluating the actual impact of the presumed Delaware effect. An example of such research is presented in Subramanian (2002), which approaches the change in impact of the Delaware effect based on average firm value. According to Subramanian, the average value of a Delaware based firm when compared to firms outside of Delaware was around 2-3% higher over the period between 1991-1996. As this higher value was highly stable over a period of five years, the author argues that this was very likely due to Delaware's specific corporate law, as was suggested in Daines (2001). When looking at the period after 1996 (up to 2001), this difference seems to have disappeared as no significant difference in value could be observed. The author poses two possible explanations for this, however, under either theory, it is argued Delaware corporations became undifferentiated from corporations in other states in this mid-nineties period.

However, the author indicates that the Delaware effect possibly might re-occur in the future. As this paper is nearly 20 years old, it is interesting to see what more recent published research has to say in regards to this topic. This is especially the case with the (once) emerging tech-state of California, in an age where technology is taking a more and more prominent role in corporate life and life in general (10% of all Fortune 500 companies operates within the technology sector, with even more firms operating in the highly related sector of telecommunications) (Fortune 500, 2019). Unfortunately, no significant research

has been conducted on the specific topic of the Delaware effect, or even more desirable, the regulatory race to the bottom in the state of Delaware over the past couple of years.

2.1.3.4 California Effect

After the initial publication by David Vogel in 1995, little to no research has focused on re-evaluating the theory to see if it is still applicable in current day and age (Vogel, 1995). The theory of Vogel has since been applied in many different cases and research setups, however, in such cases only as the concept of forcing stricter regulatory standards upon other parties by making use of the sheer market power of a certain entity. The actual reference to the state of California gets less and less attention, which might seem odd, as the theory is based primarily on the progressive policy of this state.

When looking beyond scientific research conducted in the field, focusing on regulations which were partly or completely adopted by other states or even nationwide after California had implemented them, one can still see that the state takes on a leading role in progressive regulatory standards. This is especially the case when looking at environmental standards, with one major example being California's vehicle emission standards. Since the seventies, as of the introduction of the earlier mentioned Clean Air Act, the state of California has the possibility to set their own emission standards, as Los Angeles suffered from extreme smog at the time. Subsequently, the state set their own emission standards, which predate nationwide standards. Other states in the United States may adopt the California standards, but not set their own standards (EPA, n.d.). Since then, thirteen other states and the District of Columbia have adopted these emission standards, together accounting for around a third of the national car market (Edelstein, 2017). Because of this market power, carmakers often opt to design their vehicles to adhere to these standards, possibly increasing production costs. As a response, in recent developments, president Trump's administration has made an attempt to strip the state of California of their rights to set their own emission standards to cut car prices. There are general worries about the environmental impact of this decision. However, according to the Trump administration, these worries are unjustified: it is argued that the impact on the environment will be minimal (BBC, 2019). The actual effects are, however, still to be seen.

The most recent regulation which is likely to spark some changes in the entire United States, which is also the topic of this research, is bound to be the CCPA. According to multiple reports, many other states are already in the process of designing and implementing privacy regulations themselves. Nevada and Maine have already implemented their own privacy regulations, and at least 11 other states are said to consider

implementing privacy related regulations themselves as well (Hautala, 2020). If economically influential states such as Texas, New York and Florida would consider such regulations as well, this might have significant consequences on corporate actions or adoption of nationwide regulation. If such is to be the case, it is not unthinkable a scenario as has taken place in the automotive industry will take place in the tech industry as well.

2.1.4 Method of Analysis

So, all in all, what might one expect to see in regards to developments in California and the regions outside of this state when relating this to each of these hypotheses as explained above? And where should one search for empirical evidence supporting these hypotheses?

2.1.4.1 California Effect

When regarding the California effect, assuming the state of California actually has the power to significantly affect the actions of other regulatory regions, one should search for indications or actual implementations of digital privacy related regulations in other states, or even countries. In contrast, one should also look for discussions between members of various regulatory bodies which may have resulted in the decision to, for example, not do anything at all in regards to privacy regulations. There may be a vast number of underlying reasons on why a decision has been made to act with a certain response to the introduction of the CCPA.

2.1.4.2 Delaware Effect

In case of the Delaware effect, one has to observe if the state of California is suffering from employers or employees leaving the state in favor of other competitor states. Quarterly data on this is available through the Employment Development Department. It might, however, be necessary to monitor this data over a longer period of time as slight decreases over the short term could be a coincidence or just be caused by a certain natural flow. Furthermore, this data should be put in comparison to data from other states, taking into account the various regulations which are implemented in other competitor states. Only then a proper conclusion can be drawn. Due to the fact that this regulation has only just been implemented, and historical data is not yet available, this might pose to be the biggest challenge to this research. Furthermore, the recent Coronavirus pandemic has made data even more distorted. State's projections are already anticipating on this by adjusting their predictions by making use of historical growth figures, extrapolating these to compensate for the impact of this pandemic. The actual effect of the pandemic, however, will only likely be visible until well after publication of this research.

2.1.4.3 Comparison to the GDPR: Comparative Law Research

In this research, a short comparison is made with the GDPR, the most commonly known privacy regulation in the world. Even though both regulations focus on privacy, direct comparison is inherently impossible due to various implications. This is where comparative law research methodologies come in place. There are multiple ways to approach comparative law research, but in this instance one of the methods that is used is the "law-in-context" method. The perspective of this method notes that differences in institutional contexts play a very important role in explaining differences between laws. Therefore, this method aims at understanding a certain law, as a foreign observer to the legal system it is situated in, and then explaining why the law is the way it has been implemented. A downside of this method is that, on its own, it generally only provides more general explanatory propositions (Merryman, 1974). Therefore, the explanatory propositions which are derived from using this method should be tested against empirical data. For this research, this might pose to be somewhat of an issue, as the more relevant and useful data is likely to appear over a longer period of time (years) (Van Hoecke, 2015).

Besides the law-in-context method, this research also makes use of the so-called "common core" method. This focuses on finding commonalities and differences between regulations, and more particular, if harmonization of laws is possible based on the commonalities which were found. Of course, that is not the case in this research, but through comparison on the basis of this methodology one might discover if aspects of the CCPA were inspired by the GDPR (Van Hoecke, 2015).

Comparative law research is, however, by no means flawless. Overall speaking, scholars argue that comparative law is too complex, and that the current form is too superficial. It is said that comparing legal systems is "like comparing different world versions", as the entire context may never be understood. In contrast to this, a movement focused on the simplicity of comparative law has been created as well, which argue that comparative law is not about every detail, but about providing an accurate description of the foreign legal system (Siems, 2007).

In regards to this research, as indicated before, propositions have to be tested against empirical data. This is not always available. In the case of this research only little data is available, due to how recently this law has only been implemented. Secondly, one is likely to make use of earlier conducted comparative research as a scientific source. As indicated by Pieters (2009), it is often difficult to identify the considerations which were taken by the author of the earlier comparative work. This makes it difficult to

assess if the earlier conducted research is of high quality. These aspects are impacting in which respect conclusions can be drawn from the gathered results.

2.2 The Legislative System of California

The process of an idea, which leads up to a bill, which consequently leads to the actual implementation of this bill as a law follows a certain lifecycle. This process is often simply referred to as the "legislative process" and consists of a couple number of individual steps. Understanding this process is key to understanding the evolution of the CCPA as an idea up to one of the most innovative privacy regulations of the United States. The main actors operating within this process are situated in the California State Legislature, which consists of two separate houses: the Senate and the Assembly. These two houses consist of 120 members in total, 40 Senators and 80 Assembly members. The legislative process can roughly be described as follows (California Legislative Information, n.d.; California State Senate, 2013; FCLCA, n.d.; UCLA, 2020):

- Everything starts with an idea. This idea for a bill can come from anyone, this does not have to be an actor within the legislative system.
- This idea has to be picked up by a member of the California State Legislature. This legislator consequently has to send the idea to the Legislative Counsel, which drafts the idea into a bill. This draft bill is returned to the legislator, which introduces the bill in the legislator's corresponding house.
- Each bill gets its own number and descriptive title. A bill originating from the Senate is depicted by the indication SB (Senate bill), while a bill from the Assembly is indicated by AB (Assembly bill). Following the introduction, bills may not be acted upon for a period of thirty days.
- After the introduction, the bill is presented to the Rules Committee of the corresponding house, where it is assigned to a topic appropriate policy committee. If the bill requires any expenditures, it is also presented to one of the house's fiscal committees. What follows are committee hearings, in which the proposed bill can be supported or opposed by members of the committee, possibly accompanied by letters of support or opposition. Bills may be passed, passed with amendments or rejected through a voting process.
- Passed bills are read for a second time in the house of the corresponding legislature. Afterwards, they are assigned a third reading, which has given members of the house time to prepare bill analysis. The author explains the bill to the house, after the bill is discussed by the members. Finally, the bill

is voted on. If the bill is rejected, the bill may be reconsidered and a new voting round may be necessary.

- The process as explained above is repeated once more in the other house.
- If in the other house, some amendments are requested, it must be returned to the house of origin to come to an agreement in regards to these amendments. In the case that the amendments can not be agreed upon, the bill is sent to a committee consisting of members of both houses to resolve the differences. If the committee has come to an agreement, the bill is returned to both houses for a vote.

As a final step, the governor has the last say. The governor can choose to sign the bill into law, allow it to become a law without actually signing it off, or veto the bill. In this last case, the veto can be overruled by a two-thirds vote of both the Senate and the Assembly. Bills becoming a law are sent to the Secretary of State for a final review.

2.2.1 The Initiative Process

Besides the process mentioned above, there is also an alternative option when it comes to putting new laws into action. This is done through the so-called "Initiative Process", which gives civilians the opportunity to draft their own bills and put these up for vote for the Californian citizens. California has a long standing history in regards to making use of civilian initiative processes to shape their public policies. They are one of the first states to implement referenda in their state, and is the number 2 state in how many times referenda were held since its introduction, only after the state of Oregon with over 350 initiatives having appeared on the state's ballot. Statistics show a sharp increase in the number of initiatives over the past two decades as well, indicating clear involvement of citizens in the decision making process. This is also reflected through a recent survey conducted by the Public Policy Institute of California, which indicates that around 72% of the participants in the survey (which were a representation of likely voters in the state) think it is a good thing that citizens can influence the political agenda by putting in initiatives which might later return in new laws and regulations (PPIC, 2019).

Simplified, and put in chronological steps, the Initiative Process roughly works as follows (State of California Department of Justice, n.d.; California Secretary of State, 2019):

1. A California citizen writes the draft text of a bill, known as the initiative draft. This draft is consequently sent to the Attorney General, to be given an official title and summary.

2. Initiatives require a certain number of signatures of California citizens to become qualified for voting. This requires a petition to be spread among citizens, more often than not this could require significant campaigning.
3. The signatures are handed over to county election officials, to be verified for authenticity.
4. Depending on if the verification succeeds or fails and if deadline dates are met, the initiative may either be approved or failed by the Secretary of State.
5. If the initiative is approved, it is now up to the citizens of the state of California to cast a vote on the initiative. In the case the majority of the California citizens vote in front of the initiative, a corresponding law can be put in action.

As mentioned in bullet point 2, sometimes heavy campaigning is necessary for initiatives to be into vote. It is estimated that over the last 20 years, around 2 billion dollars was spent on initiatives, which includes campaigning. Continuing, in three separate instances, expenditures reached well over the 100 million dollar mark for a single initiative (PPIC, 2019).

2.2.2 Following the Process

Of course, the processes mentioned above are all very interesting in theory, but do not give a proper image of what happens to an individual bill. Therefore, what is even more interesting is being able to follow the entire process of an idea becoming a law in practice. For the average citizen, it might not always be that clear on how to monitor this process, which could make one doubt if progress is actually being made. Fortunately, the state of California provides a lot of insight in the processes which lead up to implementation of new laws and regulations. They offer several tools for citizens, academia or policymakers to follow the individual steps of this process through the California Legislative Information (n.d.) platform. For this research in particular, this could provide clear insight into the thought processes which lie behind how the law was drawn up and initiated in the way it currently is actively maintained. This openness to the process also creates possibilities for the average citizen, interest groups and lobbying organizations to mingle themselves into the social debate surrounding new regulations, especially if they regard consumer protection such as the CCPA. As a consequence, throughout the process of the bill being drawn up, up to it being enacted, various demands are being made in respect to changing the bill. Parties supporting and opposing the regulations are seen making statements to influence the opinion of policymakers, and steer the regulation into their desired direction.

On the earlier mentioned California Legislative Information platform, the most complete overview of a bill can of course be found in the actual bill text, which provides the contents of the bill including comments which indicate that certain amendments (additions or removal of certain components to the initial bill) have been made to the bill text. This could, besides that it provides knowledge of the bill itself, when combined with external third party data (for example news outlets) give insight in what influenced legislatures to amend certain aspects of statements within the law. For example, the influence of lobbying organizations might be identified, or a swing in public opinion could be detected. Continuing on this topic of thought processes, a chronological historical overview of legislative activity is also provided. This includes information such as the initial submission date, when it was (possibly) amended and when it was approved as a bill to be turned into an official law. Besides this, closely relating to the historical overview, the current status of a bill in the process can also be found. This is, however, not applicable for the CCPA as it is currently active.

Possibly most important, the website also provides reports of legislative staff which describe the possible opposing or supporting arguments in regards to the legislation. Furthermore, the possible impact of the new legislation is discussed by the staff as well, which is also reported on. Combining this with historical information such as the comments provided with the amendments could provide an interesting insight in the considerations which were taken to shape the bill as it was in the end implemented.

3. The Intended Consequences of the CCPA

Knowing where to find the details and developments of bills, what can one say about the CCPA? In this section, the purpose of the CCPA is laid out by following the process from the first mentioning of the bill up to the implementation of the CCPA as an act in 2020. This should make clear which considerations were taken during the process, and how it evolved from being a simple addition to standing regulations up to a standalone act with far reaching consequences.

When solely looking at the history of the CCPA, or AB-375, one can see that the bill was only once amended in the Assembly but was amended in five different occasions by the Senate. What follows is a short summary of all these changes, indicating roughly what was added to the initial bill as presented by Assembly member Chau on February 9, 2017 (Bill AB-375, February 2017). This only includes the changes which were done to the initial bill, AB-375. Several other amendments were proposed after the bill was already accepted. An example of this is SB-1211, which amends several sections and adds a new one.

3.1 From a Bill to an Act

Let us start with the initial introduction in February 2017, by Assembly Member Ed Chau (Bill AB-375, February 2017). It wished to prohibit various institutions, including public agencies, telephone corporations or cable corporations from disclosing privacy sensitive information to law enforcement agencies. This should make sure that the rights of the public (and law enforcement agencies in particular) to access personal information relevant for their operations and the respect for individual privacy will be more balanced. Simply put, this would (public) institutions or law enforcement agencies obtain a search warrant if one wishes to acquire such privacy sensitive information without the consent of the individual in particular. Some exceptions to this are raised, which can be found in section 6254.16 and 2891 of its respective codes. Initially, intentions were to only amend several already existing sections in the Government and Public Utilities code.

When looking at the second version, the first and only amendment by the Assembly, something strange occurs (Bill AB-375, April 2017). The entire bill is replaced by a repeal regarding a rating system for video arcade systems. Digging deeper into this bill, the bill analysis indicates that the reason for this is to "simplify consumer protection laws", which is in line with the goals of the CCPA. Furthermore, this amendment is proposed due to it being an obsolete requirement, caused by technological advancements, which is a similar argument as why new privacy regulations might be necessary. Besides this, there is not much information available on why this amendment to an only remotely related law is relevant for the original bill.

The third version marks some significant changes, as it includes several amendments from the Senate (Bill AB-375, June 2017). Furthermore, it can clearly be seen that there is recognition of the importance of this bill, as it has moved on from the aspect of only amending existing sections of the Government and Public Utilities code. In this third version, it is indicated to add an additional chapter to the Business and Professions code, dedicated to consumer privacy. This is also the first instance in which the act was actually given a name, namely the California Broadband Internet Privacy Act. Regarding the content, because the contents of this bill would translate to a whole new chapter in the Business and Professions code, the bill is much more formalized and structured. It starts off with a list of definitions, something which was largely absent in previous versions. Furthermore, it lies the focus of the bill on the aspect of Internet Service Providers as the owners, or requesters of privacy sensitive data. In this context it defines situations in which the ISP may provide this data to third parties, and what kind of data one might provide

in a certain situation. An important aspect of this, is the act of providing consent. If no consent is provided by the consumer, the right to share data with third-parties is significantly restricted. Furthermore, it is indicated that consent may at all times be revoked by the consumer, putting the consumer even more in control of its data. The last major point of change regards the inclusion of the requirement for ISPs to maintain reasonable security provisions to prevent unlawful disclosure. This includes proper lawful security measures as well as the procedure to delete data from its systems when it is no longer necessary for the operations it was collected. Lastly, it prohibits ISPs to not offer their services to consumers in case that they do not agree to disclose certain privacy sensitive information.

In the fourth version, the list of definitions is extended to include several topic-specific terms, most certainly to create a solid legal foundation (Bill AB-375, August 2017). Furthermore, this new version of the then called California Broadband Internet Privacy act includes quite some significant extra statements and requirements towards ISPs. It now includes the requirement of ISPs to notify their consumers of their privacy policies, the earlier described aspects of requiring proper security measures, to notify users in case of a data breach and maintain a record of any data breach unless there is enough reason to believe that no harm is likely to occur due to this breach. Aspects included in the previous version are still present in this one, albeit it re-written in instances where it was deemed necessary. This version is not analyzed by any Senate or Assembly Committee, or no reports of these committee reviews are published by the state of California.

In this fifth version, the third time the Senate has amended the bill, some initially confusing amendments have been made (Bill AB-375, September 2017). First of all, the segment which required ISPs (now referred to as BIAS through the entire document; Broadband Internet Access Service) to disclose their privacy policy to consumers is completely omitted from the document. This is the case for the aspect of ISPs having to apply proper lawful security measures for the protection of their data and notify their users in case of a data breach as well. This can be explained due to it being redundant in this specific act, as it is argued that this is already present in existing law (Bus. & Prof. Code Secs. 22575, 22576 and 22577). Another important aspect added to this version is the inclusion of a date for when the act should be enacted, being January 1st, 2019. As we all know now, this date was not met, and the act was made active exactly one year later. Lastly, once again, some definitions were redefined, added or omitted from the document.

Some interesting information which can be found in the Senate floor analysis of this version of the bill is the recognition of changes due to the Trump administration (Bill Analysis AB-375, 15th September 2017). It is indicated that the California Legislature has been "shepherding a number of measures designed to codify policy ahead of inevitable rollbacks by the Trump administration". This also explains why the California Legislature wishes to implement this bill as soon as possible, as they wish to reinstate privacy rules which were previously finalized by the Federal Communications Commission only a year ago, but were recently repealed by the Trump administration and US congress.

The fifth and fore last amended version of this act presents the name of the act as we know it all: The California Consumer Privacy act of 2018 (Bill AB-375, June 2018). It is to note that over 8 months have passed since the previous version, and it therefore comes with no surprise that the act has undergone some significant changes. When comparing this version to the last amendment and enrolled version, one can see that the act has only undergone marginal changes through these last iterations: it is the near final version. In this version, readability has been improved significantly. It starts off by clearly listing the arguments why this act has to be implemented, which mostly relate to developments in quite recent history, and what rights this act aims to ensure for all California citizens. This includes the right of Californians to know what data is collected, what it is used for, being able to access it, being able to deny the sale of this data, and ensuring that services are still provided even when denying the sale of this data.

Furthermore, this version also clarifies the rights and duties of citizens and businesses by introducing clear statements written from this point of view (e.g. a business shall, a consumer shall). The contents of the act are not that much different when compared to the previous version; the base statements which were present in nearly all previous versions are still included in this near final act. Some aspects are, however, specified by including several possible scenarios which may occur when wishing to exercise a right. An example of this is the right of consumers to request businesses to delete any personal information they have of this consumer. This was present in the previous version as well, as can be read in 22552e, albeit earlier described as providing an opt-out mechanism.

Continuing, it is laid out in which situations this act will need to be enforced, and which sanctions may be expected when one is in violation of these new rules and regulations. This includes, for example, fines per each individual violation (of up to 2500 dollars per violation, 7500 dollars if deemed intentional). The proceedings of any settlement due to violations of this act will for 20% be allocated to the Consumer Privacy Fund, with the remaining 80% being allocated to the jurisdiction responsible for the action leading

to the civil penalty. To compensate businesses for the costs which inevitably have to be made to comply with this act, it is indicated that any business or third party may seek assistance of the Attorney General for guidance on how to comply with the contents of this act. The earlier mentioned 20% of fine proceedings is partially used to finance this guidance, and compliance to the new regulations in general.

3.2 The Goals and Consequences of the CCPA Summarized

Based on the information described above, what are the primary goals and consequential implications of the CCPA as can be found in the final version of the act? Summarizing, from a consumer point of view, these are as follows:

- The consumer is put back in the driver's seat when regarding the use of their personal, digital data, as recent technological advancements has increased the generation and processing of this data significantly.
- Consumers are given an option to opt-out to data collection by organizations when interacting with one of their services.
- These regulations count for minors as well, however, any child younger than the age of 13 has to ask their parents to allow for their consent to share data. Children between 13 and 16 year old are able to provide consent themselves.

From an organization's point of view, the implications are much more far reaching, with many of them having to invest to implement some serious changes. These can roughly be summarized as follows:

- The organization has to inform the consumer about which type of personal data is collected about the consumer and for what purpose it is collected.
- The organization has to provide the consumer with an option to opt-out to data collection.
- Organizations already dealing with the processing or sales of this consumer data (especially when regarding sharing with third parties) have to notify the consumer of these actions as well, and provide them with an opportunity to put a halt to this.
- The organization has to, upon request of the consumer, delete all personal information relating to this individual. If data is shared to a third party, this party must delete this information as well.
- The organization may not discriminate against consumers which choose to opt-out of data processing, sharing or sales.
- The organization has to implement reasonable security measures to protect data from being breached.

4. Territorial and Material Scope

More often than not, laws and regulations each have their own material and territorial (or geographical) scope which is clearly defined within the actual language of the law or bill. These two types of scopes roughly define the jurisdictional reach of regulations. In the case of the CCPA, this is especially important information, as it can provide important insights into the possible area of effect of this new type of privacy regulation. Since the CCPA has only just been instituted, it is not yet easy to say how far the consequences of this regulation will reach in the coming time, especially outside of the state. It is, however, not unthinkable that the CCPA will have significant consequences on the rest of the United States, due to their sheer market power which causes the so-called California effect as described earlier. Therefore, besides looking at the scope as defined in the legislative text of the CCPA itself, it is also necessary to look beyond this and take a look at similar regulations to be able to estimate its possible reach. Of course, the first regulation which comes to mind is the GDPR, dubbed its European equivalent (and vice-versa). Comparing the territorial scope of the CCPA with the territorial scope of the GDPR can, due to the presumed similarities between the two regulations, provide even more interesting insights in regards to the possible spread of (similar) measures imposed by the CCPA. What follows are the (summarized) scopes of both the CCPA and the GDPR, and a comparison between them.

4.1 Definitions

First of all, to be able to correctly understand this section, it is useful to start off with the two definitions of personal data for both the GDPR and the CCPA which are mentioned in the actual language of the bills. These are as follows:

GDPR: "'personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;" (Article 4.1)

CCPA: ""Personal information" means information that identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." (1798.140, o, 1)

4.3 Analysis of the Scopes

Now that it is clear how both regulations interpret and define the term "personal data", it is necessary to define both the territorial scope of the GDPR and the CCPA to see if there are similarities or striking dissimilarities between these two.

4.3.1 GDPR

Fortunately, the territorial scope of the GDPR is clearly defined in the language of the regulation, and is elaborated on in Article 3. The definition of this territorial scope is very broadly defined, and is as follows (GDPR - Article 3, 2016):

1. *This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not.*

2. *This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:*
   a. *the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or*
   b. *the monitoring of their behaviour as far as their behaviour takes place within the Union.*

3. *This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law.*

What becomes clear throughout the entirety of Article 3, is that it multiple times indicates that it does not matter if the entity wishing to act out its operations within the European Union is situated in a country which is part of the Union. It is even more specifically stated that it does not matter where the data is processed; if the data is collected from data subjects within the European Union, the GDPR is applicable to the specific entity. This has become even more clear through a ruling of the Court of Justice of the European Union. They ruled that, within the context of the GDPR, an organization established within the EU can be defined as an entity conducting "any real and effective activity – even a minimal one - exercised by a controller or processor through stable arrangements." in the case of Weltimmo vs NAIH (Curia, 2015). It was argued that a single presence within the EU is sufficient to be determined "established" within the territorial boundaries of the Union. In the case of Weltimmo, this requirement was more than met. The organization offered their website in the Hungarian language, effectively meaning that they offer their services in Hungarian targeted at potential consumers speaking Hungarian. Furthermore, if this was not

yet enough for the court to base their decision on, they made use of a Hungarian postal address, bank account and had a local agent responsible for operations in Hungary. Consequently, it comes with no surprise that the court argued their activities were “mainly or entirely directed at that Member State”, and therefore had to adhere to the GDPR (Twobirds, 2018).

Concluding, the main important takeaway in the case of the GDPR is that there are virtually no set boundaries or minimums in regards to the size or intention of the entity when talking about data collection and processing. Furthermore, what becomes clear throughout the entirety of Article 3, the geographical boundaries are set quite broadly. Not for profit organizations, freelancers or other small business entities are not excluded from this regulation. This is in great contrast to the CCPA (which is elaborated on later), as in the case of the CCPA, the regulations only apply to organizations with a certain number of consumers, amount of revenue or amount of revenue created through the sales of personal (privacy sensitive) data.

In regards to the material scope, the GDPR does not apply in three specific cases. First of all, it does not apply to data collection and processing methods as covered by the EU Law Enforcement Directive (which was introduced together with the GDPR) regarding data processing for law enforcement purposes. Secondly, when data collection and processing is necessary for national security purposes it is excluded as well. Lastly, when it regards data collection and processing by individuals only used for personal purposes, which of course does not include personal purposes for commercial use, it does not lie within the scope of the GDPR as well.

4.3.2 CCPA

The CCPA has its own territorial and material scope as well, however, it is not as clearly defined as in the case of the GDPR. In contrast to the GDPR, which has an entire article dedicated to defining the territorial scope, the CCPA does not include this in its legal text. There are some statements, however, which can be found throughout the regulatory statements which define a territorial scope.

The CCPA defines three separate conditions which determine if one has to deal with the consequences of the regulation, or not. All three of these conditions have to be met to fall within the territorial scope of the CCPA. These conditions can be found in sections 1798.140 (two conditions) and 1798.145 (one condition), and the contents of these conditions can roughly be described as follows:

1. The controller of the data has to be established in the state of California. This also accounts for any parent or subsidiary companies which are established in the state of California. Furthermore, this

controller must also directly qualify as a business. Factors which determine this may include physical presence, having employees active within the state, or having licenses to operate as a business within the state of California. Parent or subsidiary companies which share common branding with a controller which has been qualified as doing business may fall under the CCPA as well, even if they are not physically established in the state of California.

2. The owner of the data, also known as the data subject, has to be a resident of the state of California. This on itself is consequently split up in two conditions of which one has to be met to fulfil this parent condition. First, the individual may not be in California for a temporary purpose. If this condition is not met, the individual has to be domiciled in California to be influenced by the CCPA regulation.
3. The commercial activities which require the collection and processing of data of the individual must take place (to some degree) in the state of California. This means that, if data of a California is collected, but the commercial activity takes place completely outside of the state of California, it is excluded from the CCPA. This, however, is a very narrow definition, and will therefore only likely occur seldomly:
    a. The controller collects the data whilst the consumer is not in the state of California
    b. No part of the sale of the consumer's data is taking place in the state of California
    c. No personal data collected from the consumer is being sold while the consumer is in the state of California at a particular moment

Besides these aspects mentioned above, some more requirements exist in regards to the controller of the data. As mentioned earlier, in contrast to the requirements of the GDPR, the CCPA applies to for-profit organizations only. Besides this general remark, these for-profit organizations must meet at least one of the following criteria:

- The controller of the data must have a minimum gross yearly revenue of 25 million dollars;
- The controller of the data must annually buy, sell, receive or share the data of at least 50.000 consumers. This amount may be reached by only one of these four mentioned activities, but a combined total of 50.000 consumers is possible as well (e.g. data of 20.000 consumers is bought and data of 30.000 consumers is sold, totaling at 50.000 transactions);
- The controller of the data derives at least 50% of its annual revenue through one of the above activities (buy, sell, receive or share consumer data).

Just like with the GDPR, where there are some exceptions in regards to national security and personal individual purposes, there are some specific exceptions in terms of the scope of the CCPA as well. The list of information exempted from the material scope of the CCPA is as follows:

- Aggregated or de-identified data. Which, according to 1798.140(h) has to fulfil the following criteria to be classified as such:
- The de-identified data must not be able to identify or describe the consumer in any way. Even more so, one must not be able to relate the data to or even remotely associate the data to a particular consumer;
- The business entity should implement sufficient measures to make sure the de-identified data can not be re-identified;
- The business entity should implement sufficient measures to make sure the de-identified data will not be breached;
- The business entity itself may not in any case attempt to re-identify the de-identified data.
- Collection of employee information; e.g. in cases of data collected from applicants to a job vacancy.
- Collection of information between businesses, a so-called Business-to-Business relationship, in the case that both businesses are exempted from the CCPA.
- A specific exemption, specifically tailored to car dealers and car buyers, which states that vehicle ownership information may be stored and shared between car dealers and manufacturers for warranty or recall purposes.
- Data which is already subject to other US laws or regulation is exempt from the CCPA; it overrules the state specific regulations. Examples of this are:
- Personal health information, collected by entities which are subject to Health Insurance Portability and Accountability Act or the Confidentiality of Medical Information Act;
- Information gathered through clinical trials, which is subject to the Federal Policy for the Protection of Human Subjects;
- Certain financial information, as is already covered through the California Financial Information Privacy Act and the Gramm Leach-Bliley Act
- State motor vehicle records, which are already subject to the Driver's Privacy Protection Act.

In many of the above exceptions counts that, in the case that the data is breached due to, for example, malfunctioning of systems or a security breach by a malicious party, the entity which has collected or is controlling the data (the controller) is not exempt of being held responsible for this data breach or loss.

4.4 Main Differences

Having analyzed both territorial and material scopes, the main differences can now be identified. These are, summarized, as follows:

In terms of the territorial scope, the GDPR applies to any entity which is established in the EU. It does not matter if the data processing actually occurs in the EU. Established is interpreted in a very broad sense. In the case if the entity is not established in the EU, but is still dealing with data from subjects within the EU, regulations still apply. In the case of the CCPA, if the activity is conducted wholly outside of the state of California but still concerns a California citizen, it does not apply. This does not mean that entities outside of the state can not fall under these regulations, as the definition of "doing business in California" is quite vague, and if certain criteria are met an organization may still be considered doing business in the state.

In terms of the material scope, the differences mainly lie in the exclusions which are plentiful in the case of the CCPA. The GDPR only excludes processing through non-automated processes and processing conducted by individuals for personal use. One could therefore state that the scope of the GDPR is much broader in this respect.

4.5 Enforcement

Of course, if one implements regulations, they have to be enforced. If this is not the case, why introduce regulations at all? The territorial and material scope of both privacy regulations provide strict guidelines on who, when and how to enforce. In regards to the CCPA, the state of California has given organizations the time to ready themselves for the new regulations, but as of July 2020, organizations risk sanctions as enforcement has begun. But, because the digital landscape knows no physical borders, it might be difficult to detect and enforce these regulations. It is therefore interesting to once again look at the GDPR, and see how the EU has implemented such enforcing mechanisms. What follows is a brief analysis of the enforcement of the GDPR and CCPA, their implications, recent developments, and what lessons can be learned from the EU's experiences.

4.5.1 Enforcing the GDPR

The process of enforcement of the GDOR, as described by the European Commission (2018) through a fact sheet, is roughly as follows:

It all starts with the suspicion that an organization does not respect the new data protection rules, either through monitoring and check-ups or a report from a concerned user. The local Data Protection Authority of a country is consequently tasked to analyze the case of the organization violating the rules. From this

analysis, two conclusions may follow: the rules are respected, or the rules are breached. In the first case, no action has to be taken, in the second case the local Data Protection Authority can opt to impose a fine or impose other sanctions. A combination of this is also a possibility.

Through this process, it becomes clear that the enforcement is largely in the hands of the EU member state's Data Protection Authorities, overseen by the European Data Protection Board. This is also where issues arise. Not all member states (are able to) allocate sufficient resources to these authorities, meaning that enforcement of the GDPR is not done as well as the EU initially hoped. Monitoring organizations, performing routine checks to see if the rules are implemented sufficiently and responding to notices of rule breaches requires an amount of manpower some states just can not cope with. Reports indicate that out of 30 countries having adopted the GDPR, only 9 were happy with the amount of resources allocated to their authorities. This likely is also reflected in the number of fines given respective to the number of filed violation reports: as of November 2020, only 395 fines were given since the GDPR became in effect (CMS, 2020). In contrast, by May 2019, the European Commission had already filed over 144.000 complaints (European Commission, 2019).

Besides the lack of reports leading to fines, in recent times concerns are arising regarding misuse of the GDPR for a government's own agenda. According to the digital right advocates of AccessNow (2020), some countries use the GDPR to "curtail investigative journalism" or target NGOs to reveal their sources. Furthermore, in May 2020, Hungary suspended some of the GDPR rights during the COVID-19 pandemic. This was made possible through the state of emergency the country was in, and has been in as of time of writing, and Article 23 of the GDPR which allows restriction of rights if that is "necessary and proportionate to safeguard national security, defense, or public security". As a response, the European Data Protection Board has launched an investigation, and is reviewing Article 23 to include more strict guidelines as to which it is applicable (EDPB, 2020).

Lastly, from the entirely opposite point of view, that of the organizations affected by the GDPR, most of them which deal with citizens of EU member states have applied the well-known checkboxes on websites which one is required to tick if one wishes to make use of all the services provided. In some cases though, especially when the service provided is focused on US citizens only (like local news outlets), access from outside of the US is entirely blocked. In that case, likely the consideration has been taken that it is not worthwhile to profit from the foreign market compared to the investments in the IT infrastructure that

have to be made. When there is no access, or when no data is collected at all, enforcement is of course not applicable.

4.5.2 Enforcing the CCPA

As becomes clear from the analysis above, enforcing privacy regulations in a digital landscape is by no means an easy task. Figures, however, show that this indeed is very necessary. In a survey conducted by IAPP in collaboration with FairWarning, it was concluded that about 50% of IT and privacy professionals had at least once reported a data breach. Continuing, around two-thirds of these professionals had documented at least one privacy related incident in the past three years (IAPP, 2020). These incidents, to once again repeat punishable by fines of up to 2500 dollars per violation and 7500 dollars per intentional violation, can therefore add up significantly monetarily when the breach considers thousands of records.

According to sources, enforcement is well underway. In early July 2020, California deputy attorney general Stacey Schesser indicated that the initial swath of warning letters were already sent. The letters were sent to organizations which consumers had complained directly about to the attorney general's office, but also through social media platforms such as Twitter. After this warning, businesses have 30 days to comply with the regulations, or they risk facing other penalties. The office of the attorney general therefore advised organizations to confirm that they comply with the new measures. The presence of the key privacy disclosures such as a "do not sell" button on one's website is specifically stressed in this request (Davis, 2020; Schiff, 2020).

Enforcement now still mainly relies on action of the deputy general's office to consumer complaints and manual social media crawling. When comparing this to the GDPR, it occurs that no central agency or authority exists which exclusively focuses on the task of enforcement. This will change in the future through a proposal called the California Privacy Rights Act, which has been accepted through ballot on November 3, 2020. The CPRA will extend on many aspects of the CCPA, including the introduction of the California Privacy Protection agency dedicated to enforcing the then extended privacy law. This new law will take in effect on January 1, 2023 (O'Reilly, 2020). It therefore still remains to be seen how this agency will deal with the issues the European Data Protection Authorities are facing. The state of California is larger than most EU countries in terms of population, and ranks as the fifth largest economy in the world if it were to be a nation on itself (CBS News, 2018). It is therefore unlikely that the enforcing workload will be much lower when compared to the average EU country. From the perspective of the legislature, one

can only hope that technology to automatically detect obvious offenders will be further developed, which could potentially lower the workload and aid enforcement significantly.

5. Consequences of Consumer Privacy Regulations

Since the GDPR has been active for several years now, the consequences of these new types of privacy measurements are slowly becoming visible. This makes it possible to analyze these and possibly make a prediction of the consequences of the CCPA. To do so, it is necessary to understand which impact fields one should carry out such an analysis. In this analysis, it is chosen to conduct such an analysis on three different fields. These three different fields of analysis are similar to the so-called "regulatory impact analysis" (RIA) which is conducted before a regulation is initiated in many countries and regulatory regions around the world. In the European Union, this RIA focuses on an assessment on the fields of economic, social and environmental impact (Ballantine and Devonald, 2006). Of these three, environmental impact of this regulation is likely to be negligible, but for the sake of completeness it will nevertheless be shortly discussed in this section as well.

5.1 Economic Impact

Let us start with the most extensive part of analysis: the economic impact of the GDPR privacy measurements. Several studies were dedicated to estimating the economic impact of this regulation to the European Union. One of the earliest publications of research in this field can be found in Allen et al. (2018). The initial version of this research was presented as early as May 2018; the same month the GDPR was implemented in the EU after its announcement in 2016. The fact that this paper was published so early makes it even more interesting. It provides insight into how accurate predictive models of the impact of privacy regulation might be since the statements made can be somewhat fact checked with knowledge of statistics and studies conducted in the two additional years which have passed.

Allen et al. (2018) argues that, besides the intended consequences of the GDPR, the regulatory changes might create a new market. This market consists of financial products which have the goal of mitigating risks associated with handling and processing privacy sensitive data. This however, are not financial products which seek to cover losses in events where, for example, data loss occurs. The authors argue that the main risks for these data handlers lies in the sudden decrease or entire evaporation of monetary value of data. This is the case as consent to the use of this data, exchange of this data or the sale of this data to third parties might be withdrawn at any given time by the user, instantly rendering it worthless. The authors compare this system to American stock options.

Furthermore, the authors fear that the introduction of the GDPR might result in organizations affected by these regulations, these same data handlers and processors, are going to reduce their product offerings to citizens living or working in the union. It is not elaborated on extensively, but it is argued that this is a direct consequence of the introduced additional risk.

Continuing, research conducted as presented in Jia et al. (2018) indicates significant impact of the GDPR on investments into startup organizations within the EU. It is found that the effect of the GDPR on investments are "broadly negative", especially when considering foreign investments on younger organizations such as startups, and even more so when regarding firms which rely on data intensive activities for their main source of income. Putting this into numbers, an average decrease of around 26 percent in the overall number of monthly EU deals is recorded. Continuing, the total amount of capital raised has decreased as well, with an average recorded decrease of approximately 34 percent less capital raised per deal. According to the authors, these numbers should be taken in consideration when discussing the implementation of similar privacy protection regulations.

Aridor et al. (2020) presents a broad but elaborative study on the economic consequences of the GDPR. The study is conducted in the sector of online advertising, to be more precise, a dataset which spans a representative part of the online travel industry is used for analysis. It does so by first of all looking at the actual use of the possibilities provided by the GDPR by the consumers. That is: what percentage of the consumers is making use of the option of denying consent of data use. Secondly, it tries to discover if the composition of consumers of organizations has changed due to the new regulatory changes. Lastly, and probably most importantly, it tries to estimate what impact the new regulations have on organizations which heavily rely on data handling for conducting their activities, in this case the advertising industry. When looking at the results, some significant negative effects to the number of interactions with advertisements can be observed from an advertiser point of view: a drop of around 12.5 percent in "intermediary-observed consumers" is found. In contrast, however, the value generated from these remaining consumers is increased, as contact between consumer and organizations is maintained for a longer period of time as . This compensates at least partially for the earlier mentioned losses. All of this is caused by a decrease in targeted advertising, by opting-out of using personal data to personalize advertisements. The consumers which have willingly chosen to accept advertisements possibly prefer these personalized ads, increasing the likelihood of interaction, therefore increasing the value for them and for the advertiser.

Lastly, in a study conducted in 2018 and presented in Seo et al. (2018), results are presented on research conducted on the consequences of the GDPR in respect to the IoT industry. Results are presented based on a hypothetical case of data breach, and the costs which relate to such a data breach. These relate mainly to legal costs and costs to prevent such a data breach from occurring. Both a qualitative and quantitative analysis is conducted, which both present some interesting results. On the basis of this analysis lies the Gordon and Loeb model (2002), which is a tool to determine what kind of investment a company should make in regards to information security. Due to regulations such as the GDPR, which has increased fines significantly in some instances as it scales through company revenue and requires some hefty security measures related to prevention, costs relating to data infringement (protection) may increase significantly. Based on quantitative analysis, it was estimated that this could increase costs of IoT firms in this respect by 300 to 400 percent on average, with peaks up to 1800 percent.

5.2 Social impact

The social impact of the GDPR, or even every other privacy related regulation which is or is yet to be introduced, mainly revolves around the intended purposes of the regulation. As explained earlier, these regulations are all designed to protect citizens from exploitation of their personal, privacy sensitive data by larger entities. This means that such regulations, if designed, implemented and maintained properly, should be able to counter many of the concerns relating to the loss of privacy. To continue this analysis, it is important to first lay out the primary concerns which relate to privacy in the digital sector. These mainly arise from platforms relating to social media, search engines or web shops which make use of so-called social profiling. An online principle which is primarily related to Web 2.0 websites, which emerged in the early 2000s (Murugesan, 2007). Research as presented in Caviglione and Coccoli (2011) highlights the main concerns when regarding Web 2.0, which (summarized) are as follows:

- Interaction with Web 2.0 platforms are driven by user information input. That is, the platforms provide a better, more personalized user experience when more information is shared with the platform. It comes with no surprise that these platforms encourage users to share information as detailed as possible.
- This detailed information, which is often visible for the public to see, or at least for friends to see, opens up new possibilities for fraudulent behavior. For example, with most General Practitioners in the Netherlands, name and date of birth is enough to conduct a phone consult and consequently possibly retrieve sensitive medical details.

- Furthermore, hackers may use the public information to crack passwords and misuse someone's personal account on various websites. This can be done by using a generated library of personal words, as well as by using public information to answer "secret questions" to request a new password in case of loss.

The issues mentioned above are amplified through the automated linkage of applications to each one and other, of which many users are not even aware. Sharing sensitive data can be as simple as entering a website. Furthermore, many web applications nowadays allow for signing in with accounts of social platforms, such as a Facebook or Google account. When doing so, data is automatically shared. The user is often noticed (but not always) about what data is shared with the application, but many users do not take the time to go through these messages and simply agree with the terms and conditions. This is something the GDPR tackles by requiring "freely given, specific, informed and unambiguous" consent (Intersoft Consulting, 2018). Social consequences of leaking personal data may be, obviously, significant. Issues like identity theft (especially digitally), stalking, catfishing are not uncommon. Consequences for people on the work floor may occur as well. It is indicated that an increasing number of employers is scanning the internet and specifically social media to screen potential employees. Furthermore, behavior of employees in their spare time might be shared online by the employee himself, or one of his friends. This is slowly breaking down the wall between work and private life, which might pose to be an issue in certain situations. By being forced to treat personal data more carefully through a mandatory opt-in/opt-out system, this at least provides users with options to limit the spread of data across the web as far as this is possible.

5.3 Environmental impact

At first glance, one might not even begin to think that privacy regulations will have an effect on the environment. However, since this regulation has an impact on one of the largest energy consumers of the planet, the internet, any slight change which effects it might still turn out to have quite a measurable impact. To put this in perspective, according to a report of the Swedish KTH Royal Institute of Technology in 2019, the internet is responsible for around 10% of global energy consumption (KTH, 2014 via Cornucopia.cornubot.se). Energy consumption is generated by server activity, which is consequently caused by web traffic. That is, the amount of data that is transferred between servers, within servers and between servers and computers. Reducing this amount of traffic should, in theory, result in lower energy consumption.

As a result of the GDPR, users can decline to accept trackers on websites which collect data from them. This consequently results in a website which generates much less traffic, as was also noticed by USA Today in 2018, which ran a separate GDPR proof website for EU visitors. They noticed the website felt much more responsive, and loaded much quicker in comparison to its US counterpart. German web developer Marcel Freinbichler consequently ran a few tests, to see what could have caused this. It turned out the amount of traffic generated by visiting the website of US Today was reduced significantly, from around 5.2MB to 500KB, one-tenth of the original size of the web page. Consequently, loading times were reduced significantly as well (Frick, 2018). Furthermore, all these trackers of, for example, Amazon, Facebook or Google, make a connection to their own servers. This means that connecting to a website does not mean one is only connecting to the website it wishes to visit, it causes a whole chain of activity behind the scenes. One user tried to cut Google out of his life completely; it turned out this was nearly impossible as many websites rely on Google's web services to function, rendering large parts of the internet not usable. Something which is near impossible to deal with these days.

All in all, if websites would be optimized for compliance with the GDPR, or likely any other online privacy regulation, some measurable energy savings could be obtained. This, most likely, unforeseen positive side effect should however, of course, not be a leading argument in the discussion on implementing privacy regulations.

5.4 Possible Implications

But what does this tell us about the possible consequences of the CCPA? Well, these could prove to be quite similar. This is especially the case for the aspects of social and environmental impact, as these should not vary significantly between similar types of regulations. Of course, the finer details of the regulation will determine to which extent certain aspects are impacted. A less strict regulation, which one could argue the CCPA is in comparison to the GDPR, might result in an impact of smaller magnitude. This, however, is all quite difficult to measure, as this mainly relies on qualitative data. Environmental impact could be measurable through converting web traffic to energy consumption, however, this depends on so many variables that this is a very difficult operation.

6. The Unintended Consequences of the CCPA

Now that the basic theories as explained above are known, it is possible to elaborate on the two main hypotheses which lie on the basis of this research (or in other words: which lie on the basis of the possible consequences of the implementation of the CCPA).

The first, based on the theory of the California effect as proposed by David Vogel (1995), regards the widespread of similar regulations throughout the country due to the sheer market power the state of California possesses. An indicator of this can be seen in the relative and even absolute GDP of this state when compared to other states of countries in the world. As of 2019, there was no US state which had a higher GDP than the state of California. Even more so, as a standalone country the state alone would rank as the 5th largest economy in the world (Evans, 2019).

The other hypothesis which is to be assessed, is in regards if the CCPA could possibly have a significant negative effect on the state, through companies leaving the state due to these stricter regulations. This hypothesis has close relation to the earlier described Delaware effect. This process, however, might prove difficult to assess, as the effects are possibly only visible on the long term and the act was only initiated as of the first of January 2020, and only was announced around 2 years ago, in early 2018. What follows is an analysis of this phenomenon, as far as possible with the data which is currently available to the public.

6.1 The Response of Organizations to the CCPA

Throughout the process of designing a bill, it is likely to gather large groups supporting or opposing it. These groups of people, often gathered in larger interest groups or unified through lobbying organizations, often seek to influence the lawmaking process by using the power they possess (which is often economic market power or the public opinion). This can significantly alter the contents of laws and regulation, steering away from the initial goal of the initial proposed bill. Of course, this can go in both directions, slimming down the original contents or going far beyond what was initially proposed. What follows is an overview of the opposition and support towards the bill, including their statements supporting their point of view. This provides additional context on the roadmap of why the bill was changed in the ways it was throughout the process.

6.1.1 Opposition towards the Act

It comes with no surprise that many large organizations, especially those companies situated in the tech sector (which is one of the larger employing sectors in the state of California due to presence of companies such as Apple, Intel and Alphabet), were not particularly full of joy when it was announced the state would start investigating the necessity of new privacy regulations (Kolmar, 2020). Many of these companies rely on (as in, for example, trade in) personal data for their primary source of income. This is especially the case for large tech companies which have direct interaction with consumers through the internet, such as

Facebook, Amazon and Google. Facebook, for example, generated around 98.5% of their total revenue from (personalized targeted) advertisements in the year 2019 (Clement, 2020). Increased privacy regulations pose a significant threat to their day to day business activities. Many of these companies therefore have made attempts to alter the draft regulations in the early stages of designing the CCPA, or even try to stop it altogether, by conducting extensive lobbying activities. Lobbying is by no means a new phenomenon in the political arena, especially not in the state of California. It was estimated that over a period of nine months in the year 2019 (January to November) around 300 million dollars in total was spent on Sacramento lobbying, which is around 2 million dollars each day (Myers, 2019). Some of these lobbying activities were conducted by individual companies, however, most larger more impactful lobbying attempts are made by larger business advocacy groups, of which the largest and most commonly known non-industry bound group most definitely is the California Chamber of Commerce.

The California Chamber of Commerce has more than 40.000 members, and combinedly accounts for around 25% of the private job market in the state of California (CalChamber, n.d.). Another prominent lobbying group active in conducting counter lobbying activities against the CCPA is the so-called "Internet Association", founded in 2012 by internet giants such as the earlier in this section mentioned Facebook, Amazon and Google, as well as eBay and Microsoft (Internet Association, n.d.). This interest group reportedly spent around 176.000 dollars in the third quarter of 2018 alone on lobbying against the CCPA (Tsukayama, 2019). Interest groups from many other industries such as the automotive, film, financial services and medical sector were seen conducting lobbying activities as well. On the 6th of August, 2018, over forty businesses and interest groups even joined hands and formed a coalition to try and make an attempt to change the way the legislation was formulated. They did so by sending a twenty page long letter to democratic California Senator Bill Dodd, suggesting changes and raising concerns in respect to several aspects of the proposed bill (Coalition of California Businesses, 2018). Many of the proposed changes were an attempt to at least delay the period in which compliance was required, essentially introducing some kind of grace period (of 12 months after the final bill would be drawn up, similar to the GDPR) to make sure businesses would be able to comply without having to operate at significantly increased pace.

Furthermore, multiple attempts were made to make the bill more specific, or in other words, narrow down the scope of the regulations. Many of the statements of the bill are defined quite broadly, which creates the possibility of wide interpretation resulting in possibly a stronger legal position for the citizens of California. An example of such a statement which was attempted to be changed was the basic definition

of personal information, as was previously laid out in this paper. Aspects of this definition such as information that "relates to", "is capable of being associated with", "directly or indirectly" were proposed to be omitted from the definition. In contrast, when regarding statements to what personal information does not include were consequently suggested to be extended to include aggregate consumer information as well as de-identified and pseudonymized consumer information (Coalition of California Businesses, 2018).

The current position of the California Chamber of Commerce on the CCPA is indifferent, which makes sense, as the regulation has been passed so the only reasonable thing they can do is to accept it and make sure it does not get expanded further into a direction which may limit the abilities of their members to do business. Sarah Boot, one of their lobbyists, stated in 2018 that they feel the CCPA is "deeply flawed", and that the stakes are "astronomical" as once the initiative is passed, the ability to amend the regulation in the future is made virtually impossible due to legislation. These statements were consequently backed by various interest groups (Fang, 2018).

6.1.2 Support for the Act

Besides heavy opposition, as mentioned earlier in the section in regards to lobbying attempts by large corporations and interest groups, there are also many organizations which have expressed support for the CCPA. Traces of this support can be found throughout the entire process, from the phase of it still being a mere idea up to the final version as enacted as an act. In the bill analysis, these arguments in support are clearly laid out.

In the analysis of the first release of the bill, conducted by the Assembly Committee on Privacy and Consumer Protection, the Consumer Federation of California indicates that personal data collected from specific households (at this stage, this still merely regarded utility usage data) "raises legitimate questions about Fourth Amendment privacy protections" . It is argued that through this metadata, much more personal, privacy sensitive information may be revealed. Therefore, it should be treated in the same way as cell phone or email records, both requiring warrants to acquire the data without consumer consent (Assembly Bill Analysis AB-375, 24th March 2017).

Analysis conducted by the Senate Committee on Energy, Utilities and Communications does not include actual individual statements of support, besides the one provided by the author, Assembly member Chau. It does, however, include a list of over 40 individuals supporting the bill, including one from a US congressman, and one from the Mayor of San Francisco, consumer organizations and even some

internet/mobile service providers. The latter seems unique, as the list of opposing parties primarily consists of tech giants and internet/mobile service providers, or organizations representing these companies. One would therefore not expect ISPs to be present in the support list, even if they are smaller ones. (Bill Analysis AB-375, 17th July 2017).

In the Senate Judiciary Committee analysis that followed, many supporters which were already mentioned in previous analysis formed an unnamed coalition in which they indicated their support for the bill, which was now turned into an act. This coalition of privacy rights, consumer rights, and civil liberty organizations stresses the power of internet service providers in today's society, being able to view individual consumer behavior without consumers being able to easily protect them from this phenomenon. It is argued that this is even more amplified by the fact that around 41% of Americans only have a single option available in their area to choose from for getting high speed internet access. This insight in people's personal lives brings with it all types of threats to adoption of e-commerce, the freedom of speech and association, may aid discrimination and governmental overreach, and increase risk of theft of highly sensitive personal data. Increased protection, on the other hand, could encourage adoption of internet usage, making way to conduct more and more day-to-day activities from home through online channels (Bill Analysis AB-375, 18th July 2017).

In the analysis that follows, the support statement has remained unchanged, and is repeated once more. Furthermore, additional support is given by the California Low-Income Consumer Coalition, which bases their support on an argument related to so-called "pay-for-privacy" business models. They argue that low-income Californians and people of color are particularly vulnerable to these constructions which ask for an additional fee for increased data protection. Sometimes these products in itself are offered without initial costs, but (digital) advertising techniques make it seem highly necessary to buy this additional protection. This is a similar business model to the model which is often used for mobile applications targeted at children, the so-called "freemium" model. This, however, is completely unnecessary as privacy is a guaranteed right in the state's constitution, rights which no one should be charged for (Bill Analysis AB-375, 15th September 2017).

Support is also provided by Common Sense Kids Action, part of the larger organization Common Sense. This is an independent not for profit organization which dedicates itself to make sure children, and families as a whole, can use media and technology in the best and safest way as possible (Common Sense, n.d.). Besides providing tools, media reviews and advice for parents and families, they also partner up with

policymakers and large tech companies to make sure regulation and digital platforms are built with the young user in mind. In regards to the CCPA, they feel that it takes “the critical first step to protect the privacy of kids, families and all consumers with this first-in-the-nation legislation” (Bill Analysis AB-375, 25th June 2018).

In the Assembly Floor Analysis of the near final version of the act, another consumer protection organization speaks out their support for the act. Consumer Watchdog writes that the CCPA is “a substantial forward step for privacy protection in California”. They specifically praise the transparency which will be created due to this act, as well as inclusion of the statements regarding the right to still receive service if one refuses to have their data sold, something which was not yet present in standing regulation. Consumer Attorneys of California released a small statement of support as well, indicating it is a small and very specific, but positive step towards protecting consumers’ data (Bill Analysis AB-375, 27th June 2018).

The last support statements come from the Center of Humane Technology (CHT), and CALPIRG (an advocate for the public interest) (CALPIRG, n.d.). CHT adds in on the support in respect to the protections for children, with similar arguments as were provided by Common Sense. It is indicated that this will be the first generation to grow up online, and whose digital wellbeing might significantly affect their personal developments. The CCPA is told to increase the protection of children, especially for children under 16 and under 13, as it is now required for them to opt-in for sale of their personal data as well. In the case of children under 13 years old, this means that their parents or legal guardian is required to provide this permission for them. CALPIRG states it support for the act, if it is amended in such a way that companies will not be able to exercise price discrimination practices (Bill Analysis AB-375, 27th June 2018).

It is important to note that in the final version, only four supporting parties are still mentioned. These being Common Sense Kids Action, Consumer Attorneys of California, Consumer Watchdog and the Center for Humane Technology. In contrast, the list of opposing parties still consists of around 40 organizations, many of them being lobbying organizations such as the California Chamber of Commerce and the Internet Association (Bill Analysis AB-375, 28th June 2018).

6.2 The Response of the Market in Facts and Figures

6.2.1 California Job Market Data

Finding hard evidence on the effect of the CCPA on the labor market, and consequently the economy of the state of California and other involved states is a difficult task. Some of the prime indicators one could take a look at are the statistics relating to employment. That is, can one see a shift in the number of employers or employees in the most directly affected industry. Fortunately, several employment, economics and labor departments of various states and the United States as a whole offer great insights in the yearly or often even monthly changes within sectors. Unfortunately, due to the 2020 Coronavirus pandemic, these results are often significantly distorted and can not offer an insight in employment rates starting from around March 2020. This makes it so that the period to evaluate the consequences of the CCPA on is made even shorter than it already was. Nevertheless, the statistics are worth taking a look at, as they might provide some indication of a response of the market towards new privacy regulations popping up all around the United States.

Therefore, let us first look at the overall number of jobs created and lost in the state of California, disregarding industry specific data. Data from the US Bureau of Labor Statistics (2020) show an interesting, but inconclusive development. Over the past couple of years, on average, the number of gross jobs gained was significantly higher when compared to the number of gross jobs lost. However, this gap has slowly been closed over the first six months of 2019. If this trend would have continued, this could have resulted in a situation where the number of jobs lost could, in the near future, become higher than the number of jobs created (see Figure 6.1). This could mean that companies are leaving the state of California for other states, which results in less job openings. However, data of the second and third quarters of 2019 show a sharp contrasting increase in the number of jobs created and lost. This shows recovery of the labor market in California. Data from quarters one and two of 2020 are not yet available. It is, however, likely that these numbers would show a continuation of this trend up to Q2, where the Coronavirus pandemic threw a spanner in the works.

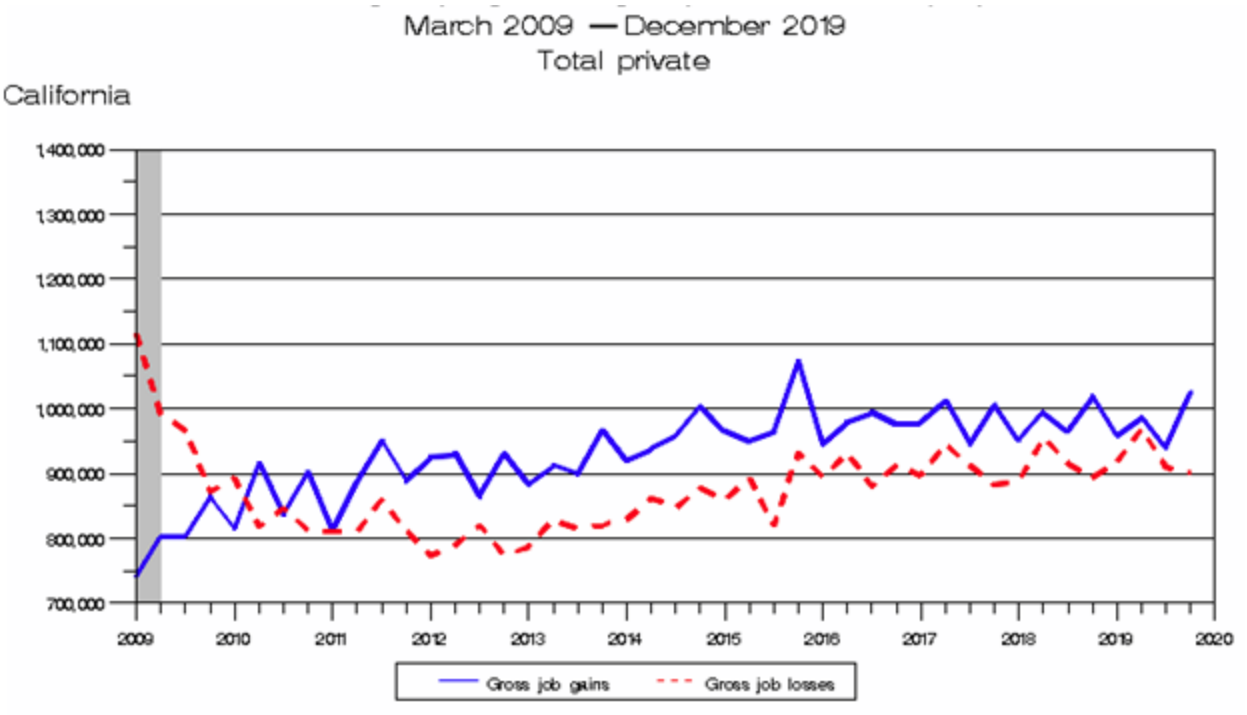

Figure 6.1: Private sector gross job gains and gross job losses, seasonally adjusted (US Bureau of Labor Statistics, 2020)

6.2.2 California Survey Data

The findings as presented above move in contrast to multiple surveys conducted under a large number of California citizens. According to a survey conducted by the Edelman Intelligence agency in 2019, around 53% of Californians which participated in this survey considered leaving the state, compared to a result of 49% of the study conducted the year before (Daniels, 2019). This desire to leave the state was mostly indicated by millennials. It is argued that costs have risen above the average income of a California citizen, which is why many citizens are considering moving to other states even though California offers many opportunities. A situation similar to that of New York is created; rents are too high and only affordable if one is descendent of a wealthy family.

This is supported by a recent study by Berkeley University (DiCamillo, 2019). The majority of participants in this study (71%) indicated that the high cost of housing is the main reason for considering leaving the state, followed by high taxes (58%) and political culture (46%, primarily conservative voters). Participants of the Edelman survey provided similar answers, ranking housing factors as the primary reason for possibly wanting to leave the state to pursue hopes elsewhere.

The actual numbers regarding depopulation speak for itself; for the seventh year in a row, more people are leaving the state of California then people are moving in. Furthermore, according to census data, the most popular states people are moving to are Texas with 86.000 departures, Arizona with 70.000 departures and lastly Washington with 55.000 departures (Sanchez, 2019).

Not only citizens of the state prefer Texas as their primary option in leaving the state, companies are choosing for Texas as well. According to reports from 2018, over the year 2016 (the most recent year available at that time) 1800 relocation events occurred. This was the highest number of departures since 2008. Furthermore, it was found that a total of approximately 13.000 companies have left the state within this nine year period (worth around $77 billion dollars in capital). Most popular destination for these companies was claimed to be Texas, and has been for at least a decade. This is backed up by most recent numbers, which claim that of these 1800 relocations in 2016, a sixth was destined for the state of Texas (Hethcock, 2019). One of the latest companies which has chosen Texas over California has been Fortune 500 giant Charles Schwab, announcing they would move to Northern Texas after their merger with TD Ameritrade (DiFurio, 2019). Furthermore, Amazon announced in November 2018 that they would move their secondary corporate headquarters to Virginia, not opting for Los Angeles which offered many benefits to Amazon to bait them to choose for them instead. This consequently resulted in a loss of 50.000 potential jobs and billions of investments in the region (Chiland, 2018).

Summarizing, at least based on this information, one could say the state of California has seen better days in regards to economic prosperity. Of course, the state still remains the number one economic powerhouse of the United States. However, the past couple of years, or even decade, have shown a decline in respect to its attractiveness towards companies. The ever expanding web of regulations result in a rather unfavorable business climate when compared to some competitor states. Therefore due this vast number of regulations, the individual of the CCPA might not yet be measurable, or even slightly show up in the statistics. However, it is not unlikely to assume that this will only add more weight on the scale for some entrepreneurs which, prior to the introduction of the CCPA, were already leaning towards establishing a new company in a state other than California, or considering leaving the state with an already established company. This might be even more so the case if, according to a survey conducted by PossibleNow in August 2019, indeed more than half of the participating companies are not ready for the CCPA by the 1st of January, 2020 (Olson, 2019). The real impact of the CCPA therefore is possible still to be felt by the economy, when CIO/CEO's realize that complying with these new regulations is too much of a burden, or simply too costly. In such a case, moving might be an option, assuming that it is possible

for your organization. That is, for example, the case if an organization might be able to move its operations entirely to a different state, or one's primary operation is not data collection but the annual revenue criteria is met (e.g. over 25 million dollars in revenue, but only a small customer base of which data is collected). If this is not the case, moving will probably be too costly, as the entire California market will have to be disregarded.

6.2.3 Industry Specific Data

The findings as presented above on the general state of the California labor market provides some slight indications on what to look for, but due to the broad character of this data, it is also susceptible to much more influential factors than industry specific data. For example, environmental regulation might have significant impact in terms of employment in the agricultural sector, while this might have only little influence on the technology sector. What follows is an analysis on industry level, or to be more precise, the industry of "Data Processing, Hosting & Related Services", the sector of which you should expect to suffer the most from the CCPA. Data from this industry is available on state level and should encompass the same companies in each and every state. Data of this industry is published on a quarterly or even monthly basis (depending on the state), providing fairly accurate information on the flow of employees towards or away from a certain state and specific industry. Furthermore, states provide bi-annual growth projections for each industry, which might prove to be a useful comparison between pre-CCPA and post-CCPA times. Albeit only based on predictions on how the market may respond in the future, based on historical data. What follows is an analysis on the states of California, Texas, and for historical sake, Delaware, on the movement of the labor force within the likely most affected sector.

6.2.3.1 California

According to statistics from the Employment Development Department of the State of California and the US Bureau of Labor Statistics, the Data Processing industry has only grown over the last few years in terms of employment (Employment Development Department of California, 2020; US Bureau of Labor Statistics, 2020). The absolute numbers on how many California citizens were employed in this specific sector move in sharp contrast to the generally expected hypothesis of the sector shrinking because of sharper regulations. According to the data provided by the government institutions, over the years 2018 until now, where the CCPA was already well announced and on its way and (future) business owners should know the consequences of the bill, the total number of employees within this sector has only grown. And quite significant as well. Starting off in January 2018, an estimated number of 46.362 citizens were employed in

the data processing sector. As of June 2020, despite the recession caused by the Coronavirus crisis the United States is currently in, this has still grown by approximately 9.000 extra employees, an increase of nearly 20%. In this period of recession, between the months April and May 2020 and still going on, the number of people employed in this sector has shrunk by around 3%, equal to approximately 1700 employees. The sector, however, already has recovered from this minor setback, showing mirrored growth numbers over the period between May and June 2020. Looking at the overall trend as shown in the graph, comparing it to pre-2018 numbers, no real hick-ups in this growth can be spotted either. There are absolutely no signs of a decline, or a decline happening anytime soon. Therefore, there seems to be no negative effect as a result of the new privacy regulations either.

It is important to note that the Data Processing sector is one of the few sectors which has still managed to grow in size over the past couple of months, despite the current state of recession, and only one of four sectors to show a grow of over 5% when compared to last year. Seemingly, this sector is still thriving quite well. Future projections support this positive trend, predicting a very positive future as well, as indicated by bi-yearly publications. Estimates of 2016 were that in 2026, the total number of employees in the sector was projected to grow from approximately 40.000 employees up to 56.400 employees, a growth of 41%. These, of course, are still predictions which were made before the announcement of the CCPA and made far before the current recession due to the Coronavirus pandemic, and might therefore still have to be adjusted. Predictions from the year 2018, however, predict a similar growth over a period of 10 years. They estimate that the sector will have grown by nearly 42%, from around 46.000 employees to 66.700 employees in 2028. If in the projections of 2018 the CCPA were indeed to be considered, one might conclude that experts do not feel that the CCPA will have a significant impact, if any, on the employment rates in this sector. At least not in the near future (Employment Development Department of California, 2020; US Bureau of Labor Statistics, 2020).

6.2.3.2 Texas

When looking at the statistics of a major competitor state, Texas, one can see an uptake in employment as well. Again, in the sector of “Data Processing, Hosting & Related Services”, as of March 2020, according to the US Bureau of Labor Statistics (2020) this provided employment for 37.999 Texas citizens. When compared to May 2020, this has dropped quite significantly, down to around 36.400 Texas citizens being employed in that industry at that time (Texas Workforce Commission, 2020). Again, quite likely the consequences of the Coronavirus pandemic are visible. The reports from March 2020, just before the

widespread virus breakout, showed the highest numbers they had ever been over the past two years. Nevertheless, when regarding an overall view of this industry taken over a period of two years, it can clearly be seen that the tendency of this sector is to grow, and is likely to keep growing in the future. As of January 2018, around 33.000 people worked in this sector, showing a growth of around 15% between then and the last pre-Coronavirus measurements, a period of only 27 months. It is, however, difficult to attribute this growth to the introduction of stricter privacy laws in other states only, as many other factors have to be taken into account as well. However, once again, there seem to be no signs of the sector being excessively boosted by the introduction of new laws and regulations.

Just as with the state of California, the Texas Workforce Commission (2020) has released growth projections of each of their sectors. As of writing, the 2018-2028 projections were not yet released, making a direct comparison not possible. Nevertheless, in 2016, the state of Texas projected an industry growth of 13.2% within 10 years, up to the year 2026. They estimated around 35.000 people would be employed in this sector by then, something which has already been far and wide reached as of today. It could be the case, however, that if the CCPA was not introduced, growth would have been larger in the state of California and growth would have been less significant in the state of Texas. This could at least partially explain the excessive growth of this sector in this state. The earlier mentioned California projections, however, do not seem to indicate this, as these growth predictions remained roughly unchanged. Natural flow and regulation, or the worldwide general growth of the digital sector and consequently the increasing amount of data the world is producing are far more likely to be the explanation of the observed growth phenomena. As in many other instances, one might say that correlation does not directly mean a causation.

6.2.3.3 Delaware

For theoretical purposes, the last state which will be looked at in terms of sector growth will be Delaware, of course due to the earlier described Delaware effect. Even though in current days, the state of Delaware might not be the prime example of lenient regulations anymore, and many other states pull ahead in terms of big name companies and number of employees within this sector, it is still interesting to see if the theory holds this day. Even if it is only to a slight extent. According to the US Bureau of Labor Statistics (2020), only 540 citizens were employed in this sector. This has gone down significantly as of January 2020, with only 390 employees remaining.

Based on trends and previously gathered results, the state of Delaware has also made some projections to where the sector will be within 10 years from 2018. This already shows some very significant and clear trends in respect to the significant negative growth rate of the data processing sector in the state of Delaware. The state of Delaware projects a significant decline of this sector, to the point where the sector has become nearly nonexistent. Over a period of 10 years, the sector is predicted to decrease in size in terms of employment by approximately 87.5%, or 18.8% annually.. The data used by the Delaware Department of Labor uses different data then provided by the US Bureau of Labor Statistics, indicating 480 employees as of 2018, predicted to have shrunken to only 60 employees in 2028. This decrease in size is significantly larger than the earlier predicted shrinkage of 16.3% as published in the 2016-2026 long-term labor market projections. What causes this sudden change in projections is unknown.

6.2.3.4 National Growth

According to IBIS World (2020), an organization specialized in analyzing industry and market research, the pre-Coronavirus growth in this sector was estimated at around 2.8%. This explains the phenomena as explained in previous sections. Current estimates are however that, due to the pandemic, the sector instead will show a significant decline in growth. The numbers up to now indeed show a decline in growth, but when compared to last year, one can still see significantly higher rates in terms of employment.

Of course, this is only some anecdotal evidence of the possible effects of the CCPA, or the lack thereof, in the United States. To complement these statistics, what follows are the growth or loss statistics in this sector of the top 10 states in regards to employment in the general tech sector, as ranked by the CompTIA Cyberstates 2020 report. These states arguably are the most interesting alternative for big tech companies to move to, as these states offer employees which have the skills for the job and likely offer a suitable climate for tech companies to thrive in. After all, if this was not the case, the number of employees in the tech sector would have been significantly lower. Unsurprisingly, the state with the highest employment rate in the tech sector is California, followed on a distance by prime competitor state Texas. It is worth noting that nearly all states show growth in terms of tech employment; only four states show a small decrease in the number of jobs, and one showed no growth or loss at all.

State	Employment Tech Sector	Employment Data Processing Sector '20[1]	Employment Data Processing Sector '18[1]	Growth '18-'20[1]	Projections '16-'26[2]	Projections '18-'28[2]
California	1,866,951	55,009	46,362	18.65%	41%	42%
Texas	1,025,106	37,999	32,968	15.26%	13.2%	n/a
New York	679,083	21,612	18,311	18.03%	-1.9%	21%
Florida	585,296	20,016	18,716	6.95%	3.82%[3]	4.94%[4]
Virginia	446,507	13,554	11,193	21.1%	15.57%	15.57%
Pennsylvania	445,168	10,907	9,211	18.41%	6.1%	n/a
Illinois	441,205	11,177	10,302	8.49%	-0.18%	0.01%
Massachusetts	440,793	9,099	8,893	2.32%	N/A	5.38%
Michigan	412,324	7,564	6,664	13.51%	1.9%	1.8%
Ohio	401,066	8,873	7,822	13.44%	13.2%	n/a
Delaware	33,923	390	540	-27.8%	-16.3%	-87.75%

Table 6.1: Employment Statistics in the Top 10 Tech States of the United States

As becomes clearly visible from the statistics above, the state of California projects by far the largest growths of the largest tech states of the country. Furthermore, other states do not seem to profit as well from the California regulations as one could expect; earlier predicted growths or shrinkages in terms of employment in the data processing sector have remained roughly the same between the 2016 and 2018 projections. The only major exception in this is New York, which predicted a small shrink, but instead now projects the second highest growth of all states in this overview. The state of New York does not provide any additional reports on this as of yet, and reports on major data processing companies suddenly moving or experiencing large growth to/in the state of New York are difficult to find. One possible explanation could be the anticipation of the state to the departure of a large employer, which in the end did not come through.

[1] Statistics from January 2018 to March 2020, to provide the most complete overview excluding influence of the 2020 Coronavirus Pandemic (U.S. Bureau of Labor Statistics, 2018; US Bureau of Labor Statistics, 2020)

[2] Texas Workforce Commission (n.d), Employment Development Department of California (n.d.), Delaware Department of Labor (n.d.), New York State Department of Labor (n.d.), Florida Department of Economic Opportunity (n.d), Virginia Employment Commission (n.d.), Pennsylvania Department of Labor and Industry (n.d), Illinois Department of Employment Security (n.d), Massachusetts Department of Labor & Workforce Development (n.d.), Michigan Department of Labor and Economic Opportunity (n.d), Ohio Department of Job and Family Services (n.d.)

[3] The state of Florida uses time intervals different from other states, therefore this projection spans 2017-2025

[4] The state of Florida uses time intervals different from other states, therefore this projection spans 2018-2026

The reason why the impact of the CCPA is not (yet) visible, or will not even become visible in the future at all, is that multiple states around the country are in the process of researching or implementing their own privacy regulations as well. Therefore, there might not really exist a competitive advantage when moving to a different state. Pair this with the significant costs to move one's company to a different state, even if it only regards moving its legal seat from one state to the other, it might just not be worthwhile. As will be elaborated upon in the next section, as of August 2020, over 20 states have made steps in implementing consumer data privacy regulations, varying significantly in terms of scope and strictness (Noordyke, 2020). This includes the two prime competitor states of Texas and New York. Seeing that these states are trying to make steps through bills similar to the CCPA might help companies convince that taking action to avoid these privacy regulations is useless, as change is coming, whether you like it or not.

6.3 Possible Responses of States to the CCPA

Not much is written in literature in regards to how countries, states or member states of a certain union may respond to the implementation of possible influential new regulations in another jurisdictional area. However, basic theory and knowledge teaches us that a response to most dilemmas falls in one of four categories. Therefore, as a basic theory, the different responses one might expect from surrounding or economically competitive states can roughly be divided between these four different categories. These categories, as already briefly highlighted in the introduction section, are as follows:

No active response - do nothing

This does not need elaborate explaining. In this scenario, the legislative body in question decides to not respond to the regulatory action as taken by the state of California. Simply put, the current regulation will remain as it was before, and the response and possible consequences towards/of the CCPA is dependent on the market and society of this state. This could be risky business, as this might result in competitive disadvantages if the new regulation imposes new more favorable conditions. On the other hand, if one may observe that the regulations in a certain state are already more favorable than the other state, or might become even more favorable in comparison, this could prove to be very beneficial to the state's business climate. Of course, a major example of such a type of response is the earlier described approach taken by the state of Delaware in the late 1900s. Another more recent example of this could be the earlier mentioned state of Texas, which has become a more and more interesting option for U.S. citizens and businesses over the past years due to their favorable regulatory climate.

Replicate - do the same

In this scenario, the legislative body of a certain state decides to nearly one-on-one copy the regulations. This scenario is the scenario as is described in the earlier section in regards to the California effect; the regulations are replicated in other states due to, among other aspects, the sheer market power of (in this case) the state of California. More recent work as presented in Bradford (2019) mirrors this scenario to the ever increasing global (regulatory) power of the European Union.

An example of this is the earlier mentioned California Clean Air Act, which was copied by many other states and soon became the industry standard in the automotive sector (Sivas, 2018). As this scenario might once again unfold with the introduction of the CCPA, replication of this regulation by other states, and therefore its spread across the entire country, could prove to be beneficial for the state of California. There would be no regulatory advantages or disadvantages to be gained in other (competitor) states. On the other hand, states might be hesitant to adopt these regulations entirely, in fear of possible economic or social consequences.

Slim down - do less

Of course, besides implementing a one-on-one copy of the regulation, one might also choose to only adopt certain parts of the regulation in one's state or design similar regulations which have a slightly different, or less broad reach. Through being able to evaluate the consequences of an already implemented baseline regulation, such as the CCPA, one might see that certain aspects did not really achieve their intended outcomes, and might have gone too far. This might result in legislators opting for less strict regulation, or redefining the scope by (for example) making it less broad. This process was already seen in the last months of 2019, with many states researching the options of consumer data privacy regulations, looking at similar options, although often being softened on multiple aspects (Greenberg, 2020).

Super-equivalence - do more

In this last scenario, a state will respond to regulatory changes by implementing a similar type of regulation, but even go beyond this initial regulatory change. This is called super-equivalence, or gold-plating. This term is in the past few years primarily associated with the United Kingdom, having implemented many consumer protection regulations followed by the introduction of similar EU regulations, but having gone far beyond this to protect national interests. The topic has regained attention following the country's exit from the European Union after the 2016 Brexit referendum. Most often this

process of gold-plating took place when these regulatory changes regarded the financial services industry, as the UK has had a history of consumer issues in this field and wishes to prevent these issues in the future (Andenas and Chiu, 2014).

6.4 Responses of States in Practice

As indicated in the previous section, multiple states are already working on implementing, or have already implemented so-called CCPA copycat bills. As of August 2020, a total of 16 states were in the process of implementing one or multiple consumer privacy regulations. A total of 3 states, being California, Maine and Nevada have successfully implemented consumer privacy regulations. In another 8 states, the bill died in the process or was postponed indefinitely. The remaining 23 states have not yet announced to be working on passing new privacy regulations (Noordyke. 2020). As can be found in the analysis which follows in this section, a surprisingly high percentage of states are working on regulations which go beyond the goal of the CCPA.

Let us first look at the privacy regulations of the states of Maine and Nevada, as they have actually been able to successfully implement these regulations. Starting off with the state of Maine, already some major differences can be spotted. First of all, Maine's privacy law only focuses on Internet Service Providers, and not on other data processing institutions. It is indicated that it covers approximately 80 ISPs in the state of Maine, and only applies to ISPs serving customers which are physically located in the state of Maine and are billed for services in this state. This means that social media giants such as Google, Amazon and Facebook are not included in the reach of this law. On the other hand, it goes further than the CCPA in a way that it requires customers to opt-in to data processing, instead of the much more common opt-out option as provided by the CCPA and many other privacy regulations. Besides this, many other aspects of the CCPA such as right of access or right of deletion of personal data are not present in this law (Kalnenaite, 2019).

In the case of Nevada, the law can roughly be described as a significantly trimmed down version of the CCPA. For example, where the CCPA regards the "sale" of data as any act of "Selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means", the Nevada law defines this much more narrowly as "The exchange of covered information for monetary consideration by the operator to a person for the person to license or sell the covered information to additional persons". This makes that the CCPA covers much more situations in which data is transferred from one party to another when compared to its Nevada

counterpart. Again, just like with Maine's privacy law, many aspects in regards to the control of the data by the individual are lacking. Opting-out of data processing is as far as it goes in terms of control (Scott & Tonsager, 2019).

Most of the other initiative bills are still in Committee, with those of Hawaii and Maryland already having crossed the chamber and being put for review by committees a second time respectively. Washington even came very close to actually passing a privacy bill, but it was stranded in the Washington House of Representatives after two near-unanimous votes in favor of the bill by the Senate. The House demanded some amendments to which the Senate could not agree upon, mainly relating to the enforcement of the bill once it was active. As was drawn up, Washington's privacy act would have gone beyond what the CCPA is currently enforcing, opening the possibility for individuals to enforce the law in court through private right of action. They are now working on being able to pass a new and improved bill in 2021, on which the House can agree as well (Johnson, 2020).

6.4.1 New York and Texas: California- and Delaware Effect Candidates

The prime competitor states of California in terms of technical employment rates, Texas and New York, are not even near actually implementing their own privacy acts. Texas passed an act dubbed the "Texas Privacy Protection Act", however, it was significantly amended during the process up to it being enrolled. It does not actually provide any increased privacy towards consumers. Instead, the act has established a committee which is going to focus on studying existing data privacy laws in the state of Texas and other US states. A report of their findings was presented in September 2020. Furthermore, the accepted bill includes the requirement of having to notify individuals of their data being breached within 60 days of the occurrence of the data breach. In existing laws and regulations there was no limit set on how much time one could take to notify an individual of their data being breached (Texas State Legislature, 2019). In the case of New York, their New York Privacy Act would go beyond the regulations of the CCPA in many ways. First of all, the definition of what encompasses "data" is even broader than is the case in the CCPA. Next, just as in the case of Washington's proposed act, this privacy act would allow individuals to enforce the law in court through private right of action. Furthermore, the NYPA does not contain any upper or lower boundaries in terms of size of companies affected by the regulations, in neither employment size nor revenue. If you as an institution are dealing with data from New York residents, you are affected by the act. Lastly, the NYPA includes some additional controlling aspects not present in the CCPA, such as right of rectification, right to restriction of processing and the right against the use of data in decision making processes which are entirely automated (ADCG, 2020).

Based on these developments, Texas and New York may prove to be real candidates to reflect the Delaware and California Effect. But how did these states end up in the position they are currently in? New York, with great intent, but in the end not a desired outcome, and Texas which clearly has little to no intention at all and is currently only postponing their progress. In this section, these aspects are shortly being analyzed from the perspective of the policy making process. How is it influenced, what are the current developments and what are the expected developments in the near future?

6.4.1.1 New York

The New York Privacy Act was introduced by Democratic Senator Kevin Thomas. When one looks at the composition of the New York state legislature, one may not directly find any clues in respect to why a privacy bill has not come off the ground. After all, a large Democratic majority can be found in both the state Senate and Assembly (105-43 and 40-23 respectively). This, however, has only been the case since the 2018 elections as between 2010 and 2018 the Republicans had control over the New York state Senate. The Assembly, on the other hand, has been in control of the Democrats for decades (Ballotpedia, 2020). Any plans initiated by the Democratic party coalition should therefore have a decent chance of success, which leads to the consequence that the present discussions and lack of progress must be caused by the actual contents of the bill and not the general bill intentions itself. After all it is unlikely that a bill such as the NYPA has no chance of succeeding at all, as it would likely not even have been presented if internal discussions within the Democratic party had indicated that a majority of members were opposing data privacy regulations altogether.

Reasons for failure of the bill became apparent during a Senate hearing of the bill in June 2019. Allie Bohm, legal counsel for the American Civil Liberties Union of New York, argued that the bill had the good intentions at heart, but missed the specific language necessary to be the landmark bill it wishes to become. Creating a bill that does check all the necessary boxes, however, might prove to be a difficult job. The bill was criticized by many lobbying organizations and interest groups, such as the Retail Council for New York State, industry trade association TechNet, Tech NYC, the Business Council of New York State, and the Internet Association. These interest groups, especially the Internet Association, possess significant capital. Something interest groups on the other side of the coin, the more socially involved interest groups such as the New York City Liberties Union, can not compete against. Because of this criticism, fueled by these interest groups, the bill failed to find a majority coalition in the Senate. Therefore, there is belief that passing smaller individual bills might prove to be more effective, and achieve some of the goals

significantly earlier than a larger bill would have (Ropek, 2019). This way the discussion regarding a larger, all containing bill may then continue while certain rights are already protected through the implementation of these smaller, more narrowly focused bills.

This is exactly what has been done in the time between the bill initially failing and present day, while it still has not been implemented. Multiple consumer privacy related bills were passed, showing the increased traction and attention data privacy related regulation is getting. As an example, the so-called "Stop Hacks and Improve Electronic Data Security" (S5575) act was signed into law in July 2019, and has been in effect since March 2020. Through this act, a smaller aspect of the NYPA (and also other privacy bills such as the CCPA) is covered. This aspect concerns the requirement towards organizations to implement reasonable safeguards against data breaches. Furthermore, the legal definition of personal information has been broadened, as it previously only included the basics such as name and Social Security number (New York State Senate, 2019). Continuing, in this same session of July 2019, another bill was filed: S224, introduced by Senator Brad Hoylman. This again fulfils some of the goals set by the NYPA, which requires organizations to provide customers with the personal data they have collected upon request (and they must respond to such a request at least once a year). Additionally, it requires organizations to regularly inform customers in respect to which data is collected about them. This bill was originally filed way back in 2013, but never found enough ground to make it out of committee until just then (New York State Senate, 2019). For now, due to the 2020 Coronavirus pandemic, the all-encompassing bill to enact the NYPA is postponed indefinitely. For the privacy concerned citizens, activists and interest groups, the enactment of these smaller bills could in retrospect therefore very well be seen as ultimately being the right move at that moment. However, due to the pandemic, an additional bill has been introduced and has successfully passed the Senate. This bill S8448D, relating to "requirements for the collection and use of emergency health data and personal information and the use of technology to aid during COVID-19" (New York State Senate, 2020). The bill was introduced and co-supported by Democrats only. Developments such as this one again show the state's legislature intent to ensure protection of one's personal privacy in this digital age.

6.4.1.2 Texas

The Texas state legislature has had a Republican majority for decades in both the Senate and House of Representatives. It therefore comes with no surprise that the larger, all-encompassing Texas Consumer Privacy Act (HB4518) which was introduced by Democratic House of Representatives member Martinez

Fischer, had a hard time finding enough ground to gain a majority in the House. Besides this larger bill which did not find a majority, the much less impactful bill HB4390, the Texas Privacy Protection Act, did find enough ground to pass. This bill was co-sponsored by both Democrats as well as Republicans (Texas State Legislature, 2019). As indicated before, a task force has been founded to research the possibilities of a broader privacy related act. Regarding the findings of this task force, these have been published as of September 2020. Summarized, the recommendations of this task force mainly relate to considerations which have to be taken when proposing privacy related regulations. The recommendations do not, or only barely, relate to what provisions should be included in such related regulations. No recommendations are made which rights Texans should have relating to their personal data, or the (lack of) control of it. Obvious aspects relating to right of access, deletion, correction, portability, opt-in or opt-out options, third-party data processing or enforcement are not discussed in the report (Texas Privacy Protection Advisory Council, 2020). It therefore seems that the debate has not moved much since the advisory council was founded, and it does not seem likely that this report will move the debate further in the near future.

The state of Texas has not introduced any bill aimed at protecting one's privacy relating directly to the COVID-19 pandemic. On a national level, however, an attempt is made to regulate this nationwide. The US Congress introduced the so-called "COVID-19 Consumer Data Protection Act", which strives to "protect the privacy of consumers' personal health information, proximity data, device data, and geolocation data during the coronavirus public health crisis". Real progress, however, has not been made yet. It has been read twice in the Senate, and was referred to the Committee of Commerce, Science, and Transportation. No further action has been taken since (Wicker, 2020).

6.4.2 Responses Nationwide

Through evaluating the (potential) privacy bills which are (going to be) implemented around the United States, it is possible to determine which of the earlier defined four types of response approaches each of the states is taking. In previous sections, the responses of the most interesting states were already elaborated on. What follows is an aggregate table including all states which have at least introduced a bill to implement new consumer privacy regulations, based on the (proposed) bills, publications from news outlets, law experts, privacy advocates and research presented by Noordyke (2020). This includes the current status of the bill (active, work in progress or died), its corresponding response category and a short summary of why this is the case:

STATE	RESPONSE	STATUS	EXPLANATION
California	Do the same	ACTIVE	Acts as a baseline measurement for the rest of the United States.
Arizona	Do more	WIP	Except for no right of private action, Arizona offers more control over data by individuals than the CCPA does (Heaphy, 2020).
Connecticut	N/A	WIP	SB1108 established a Task Force to research Consumer Privacy Rights (Connecticut General Assembly, 2019).
Florida	Do less	DIED	Required a notice in regards to data collection, and provided an opt-out option (Florida Senate, 2020).
Hawaii	Do less	WIP	Was significantly trimmed down in the process (would have been: do more), now only requires clear consent of users to sell geolocation- of browser data (Hawaii House of Representatives, 2020).
Illinois	Do more	WIP	Consists of 2 Senate and 1 House bill, all being at least as strict as the California counterpart, with SB2330 going beyond this (Strauss & Rogers, 2020).
Iowa	Do the same	WIP	Was amended in March to broaden its scope, now covering most of Iowa's businesses. Requires a higher age of consent (18 vs 16), offers possibilities to restrict the use of data for certain purposes and ways of processing, but offers no control in terms of right of deletion and portability (Lande, 2020).
Louisiana	N/A	WIP	HR249 established a Task Force to research Consumer Privacy Rights (Louisiana State Legislature, 2019).
Maine	Do less	ACTIVE	Although Maine's law makes use of opt-in instead of opt-out, many basic user data control methods are lacking (Kalnenaite, 2019).
Maryland	Do more	WIP	Similar to the CCPA, with the exception that consumers need to be notified of ALL data shared with third parties, including data shared without monetary compensation (Clarip, n.d.).
Massachusetts	N/A	WIP	S120 issued a study order to study possible contents of a Consumer Privacy bill (Massachusetts General Court, 2020).
Minnesota	Do more	WIP	Extends on the CCPA by not having an upper or lower limit for companies being influenced by the regulations just as in New York's proposed act (Rosenkoetter, 2020).
Mississippi	Do the same	DIED	Largely copies the CCPA, literally copying some statements from the CCPA. Died in Committee (Rosenkoetter, 2020).
Nebraska	Do the same	WIP	Largely copies the CCPA, although some important aspects such as the terms "sale" and "disclosure" are undefined. The scope is slightly different as well (Hintz et al., 2020).
Nevada	Do less	ACTIVE	Trimmed down version of the CCPA in terms of scope and user data control (Scott & Tonsager, 2019).
New Hampshire	Do more	WIP	One of two bills largely copies the CCPA, with an additional bill allowing private right of action in case of a violation of one's privacy in regards to information shared with third party service providers (Canter et al., 2020).

New Jersey	Do more	WIP	Through a combination of two bills, besides requiring opt-in for data processing permission, it also opens up the way for private right of action through AB3255 (Dort & Noordyke, 2020).
New Mexico	Do the same	DIED	Largely copies the CCPA (some even dubbed it a word-for-word copy), opted for a higher age of consent of 18 instead of 16 years old. Died in the Senate (Kulp, 2020).
New York	Do more	WIP	Could become one of the far reaching privacy acts of the United States, raising the bar on nearly every aspect when compared to the CCPA (ADCG, 2020).
North Dakota	N/A	WIP	HB1485 arranges a "legislative management study" of consumer personal data disclosures (North Dakota Legislative Assembly, 2019).
Pennsylvania	Do the same	DIED	Largely copies the CCPA, as it is modelled after it. Died in Committee (Iacono and Weiss, 2019).
Rhode Island	Do the same	DIED	Largely copies the CCPA, with some exceptions in terms of scope and the possibility for private right of action. Died in Committee (Clarip, n.d.).
South Carolina	N/A	WIP	Unlike other acts, South Carolina's act focuses on biometric data, such as iris scans, fingerprints or hand and face geometry scans (South Carolina General Assembly, 2020).
Texas	N/A	WIP	Initial proposition bill was very similar to the CCPA, but died in Committee. HB4390 established a Task Force to research Consumer Privacy Rights (Texas State Legislature, 2019).
Virginia	Do more	DIED	Would be similar to the CCPA in many ways, but would offer even more personal data control to the user. Additionally, it would require data processors to conduct a "privacy risk assessment" for each of their processing activities (Katz, 2020).
Washington	Do more	DIED	Would have become one of the far reaching privacy acts of the United States, but died after not reaching an agreement between the Senate and the House (Johnson, 2020).
Wisconsin	Do less	DIED	The Assembly proposed three different privacy Acts, covering some aspects of the CCPA. All of them died in Committee (Giftos. 2020).

Table 6.2: Overview of the status of Consumer Privacy Regulations around the United States

As can be deduced from the table above, a total of six states were working on an act which is very comparable to the CCPA. Furthermore, a surprisingly large number of nine states were or are planning to go even further than the CCPA, imposing even stricter regulations upon data processors than what were already dubbed very strict regulations in the state of California. A number of five states had the intention of doing less than the CCPA. Among these five states are the only two states which have successfully passed a bill and enacted it besides California. Four other states have indicated that they will study possible Consumer Privacy regulations, although it is very much the question if this will actually lead to something. This is especially the case due to the Coronavirus pandemic, which postponed many bills

indefinitely. Lastly, South Carolina is a clear outlier which can not directly be compared to the CCPA, as it only regards biometric data.

It is clear that there is still a broad discussion going on between the legislative bodies in the majority of the above mentioned states. Many of the proposed bills died in the very early stages of the legislative process, or are still in the process of being heavily discussed and amended. Furthermore, in a number of states earlier proposed bills died in the process (sometimes even more than one), and new bills, often amended significantly, were put up for discussion. The question, however, remains if the 23 remaining states will try to implement some type of consumer data privacy act in the future. This is especially the case for a high-tech state such as Michigan, with its over 400.000 employees in the technical sector (Comptia, 2020).

7. Conclusions

It is safe to say that it is too early to draw conclusions on some aspects of the consequences of the California Consumer Privacy Act. There are, however, some clear aspects which can be observed when looking at the findings presented in this research. One of the main conclusions which can be drawn, is that the vast majority of the United States is working on implementing data privacy protection laws. One could therefore state that the California effect can definitely be observed, although it is still the question if this is due to the introduction of the CCPA, or if the time was just right for a change in privacy regulations. Many experts, however, dub other state privacy laws as being “copycat bills”, and multiple privacy regulations have used the CCPA (at least partly) as an inspiration for their own laws.

This is not unsurprisingly the case, as California is the largest state in the US in terms of population, and due to the territorial and material scope of the CCPA it is nearly impossible for organizations to not be affected by the CCPA if one wishes to operate or interact with California and its citizens. Denying service to California citizens would probably be too costly, something which now indeed does occur in some cases in regards to EU citizens wanting to access US web services. Some of these states are still in the very early stages of development though, with the only action taken being the creation of task forces or research groups. Other states have already implemented regulations, which often have used the CCPA as a blueprint for their measurements, sometimes even copying regulatory statements word-for-word. One can also observe that the development of such privacy laws is not always such a fluent process. In many states, it can lead to significant discussions, often fueled by the power of influential lobby groups, more often than financed by the big five of technology, bundled in power through the so-called “Internet

Association". This, as a consequence, leads to a situation in which only 3 of 27 states have an active data privacy law at time of writing. There is not much change in this to be expected any time soon, as (among other reasons) most legislative bodies are currently struggling in coping with the Coronavirus pandemic leading to bills being postponed indefinitely.

But what does this mean in regards to the Delaware effect? This is difficult to say. As indicated before, over half of the states in the US have started drawing up or at least started thinking about implementing new data privacy laws. It is likely that more states will follow. However, this does mean that about half of the states have not yet decided what they are going to do. It could very well be possible that some states decide to do nothing, and undercut California's law (and many other states) altogether. An example of such a state could be Texas, which are close to doing nothing as they are merely exploring possibilities as of now. In contrast, a significant number of states are also planning on gold plating the CCPA, taking drastic measures forward, even compared to the already quite invasive CCPA. These bills especially, can count on a lot of discussion between the different legislative bodies, as can be seen in Washington and New York. The future will tell how these bills will develop.

Regarding the economic consequences of this law, more research is needed. Data currently available suggests that there are no negative economic consequences at all, even in the sector one would think would be hit the hardest by the new measurements. On the contrary, the sector is predicted to grow by one of the largest percentages of the entire country. But, as previously indicated, significant negative economic effects are only likely to occur if California loses a large number of businesses. Avoiding the CCPA is realistically only possible for organizations which fall within a specific set of thresholds of the material and territorial scope of the CCPA, but wish to remain doing business with California citizens. Or, of course, for organizations which are able to move their entire operations from state to state. It will be interesting to see how this actually unfolds, as the law was only announced a little over 2 years ago, and is only active for several months now. Real results will likely show up over a period of years, not even talking about the significant amount of distortion in the data caused due to the global recession due to the Coronavirus pandemic. Employment data and growth predictions should be monitored and analyzed to see if a trend can be observed, and avoidance of this privacy law is actually occurring and having an impact.

All in all, it is safe to say that a wave of data privacy related laws is currently flooding the United States. It is likely that this is due to the introduction of the CCPA, as many signals point towards it as being the

baseline for privacy regulations. Once again California proves its historical reputation, pushing revolutionary laws which slowly spread to states across the country. Its market power is largely to credit for this. As of now, it is not yet clearly visible if there are any negative consequences involved financially. This is something the future will tell, and therefore should be closely monitored.

8. Future Research

As already highlighted many times before in this research, and in the conclusion, there is especially more research needed in the possible economic consequences of the CCPA on the state of California. It is currently not yet possible to draw definitive conclusions yet, based solely on the data that is available at this moment. Therefore, future research should focus on analyzing data such as presented in this research over a longer period of time. This should make it possible to predict a certain trend, and flatten out certain irregularities that might have occurred due to influences of external factors. Especially due to the current Coronavirus pandemic, data is distorted in such a way that it is difficult to draw any clear cut conclusions, even though data is already corrected by the governmental institutions to compensate for situations such as this pandemic. This is, however, something that should probably be researched by, or in collaboration with, an economics scholar. There are a significant number of other factors which might influence employment numbers, besides one single regulation which was newly implemented. These factors should be taken in account, something which likely requires in-depth financial calculations.

Besides analyzing data, qualitative research should be conducted in terms of the experiences of big tech companies affected by new privacy regulations. Through digging through records of Chambers of Commerce, one must be able to discover if an organization has moved (part of its assets) to a different state. These organizations in turn could be contacted and be interviewed on why they did, or did not act in the way that they did. Unfortunately, in the case of this research, the California Chamber of Commerce did not respond to any correspondence sent to them by the author. Digging through news outlets did not provide any significant results either, which makes sense, as these processes likely occur in the background. This additionally gathered information could prove to provide important context to the quantitative data as provided by the government institutions, without being distorted by the filters of media outlets.

Lastly, and probably most obviously, the progression of the different data privacy regulations in the different states across the country should be monitored closely. This is especially interesting due to the announced extension on the CCPA, the CPRA, which would once again become the golden standard of

privacy regulations in the country. It will be interesting to see if the regulations will change and shift to one specific direction (e.g. gold plating) altogether due to the CCPA and its extension, or due to other states increased interest in consumer data privacy regulations. After all, around half of the states in the country have not yet made any progress or announced anything in regards to consumer data privacy laws. Therefore it is still anybody's guess to what the future will bring. In contrast, it could also be possible that progression will be indefinitely stalled due to different priorities or external factors such as pressure from interest groups. Maybe, in the future, it does become clear that privacy regulations have a significant impact on a state's economy, and it is decided to not go further with it. This all remains to be seen, and therefore might be worth continuous attention from scholars in the coming years. Research presented in this thesis could be used as guidance for revisiting this topic.

REFERENCES

AccessNow. (2020, May). Two Years Under the EU GDPR. Retrieved November 23, 2020, from https://www.accessnow.org/cms/assets/uploads/2020/05/Two-Years-Under-GDPR.pdf

ADCG. (2020, January 16). New York Privacy Act: It Goes Beyond CCPA. Retrieved September 06, 2020, from https://adcg.org/new-york-privacy-act/

Allen, D., Berg, A., Berg, C., & Potts, J. (2018). Some Economic Consequences of the GDPR. SSRN Electronic Journal. doi: 10.2139/ssrn.3160404

Andenas, M., & Chiu, I. H.-Y. (2014). The foundations and future of financial regulation: governance for responsibility. New York: Routledge.

Aridor, G., Che, Y.-K., & Salz, T. (2020). The Economic Consequences of Data Privacy Regulation: Empirical Evidence from GDPR. doi: 10.3386/w26900

Assembly Committee on Privacy and Consumer Protection (2017, April 28) Bill Analysis, AB-375. Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

Assembly Committee on Privacy and Consumer Protection (2017, March 24) Bill Analysis, AB-375. Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

Assembly Committee on Privacy and Consumer Protection (2018, June 27) Bill Analysis, AB-375. Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

Assembly Floor (2018, June 27) Bill Analysis, AB-375. Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

Ballantine, B., & Devonald, B. (2006). Modern regulatory impact analysis: The experience of the European Union. Regulatory Toxicology and Pharmacology, 44(1), 57–68. doi: 10.1016/j.yrtph.2005.06.016

Ballotpedia. (2020). New York State Legislature. Retrieved November 23, 2020, from https://ballotpedia.org/New_York_State_Legislature

Ballotpedia. (2020). Texas State Legislature. Retrieved November 23, 2020, from https://ballotpedia.org/Texas_State_Legislature

BBC News. (2019, September 18). Trump strips California of power to set auto emission standards. Retrieved April 26, 2020, from https://www.bbc.com/news/world-us-canada-49746701

Bradford, A. (2019). The Brussels Effect. The Brussels Effect, 25–66. doi: 10.1093/oso/9780190088583.003.0003

Bukaty, P. (2019). The California Consumer Privacy Act (CCPA): An implementation guide. Ely, Cambridgeshire, United Kingdom: IT Governance Publishing. Retrieved from www.jstor.org/stable/j.ctvjghvnn

CalChamber: About Us HR Expert & Business Advocate™. (n.d.). Retrieved April 26, 2020, from https://www.calchamber.com/aboutus

California Legislative Information. (n.d.). OVERVIEW OF LEGISLATIVE PROCESS. Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/

California Secretary of State. (2019, December). Statewide Initiative Guide [PDF]. Sacramento: California Secretary of State.

California State Legislature, session 2017-18 (2017, April 27). AB-375, version April 27, 2017.

California State Legislature, session 2017-18 (2017, August 21). AB-375, version August 21, 2017.

California State Legislature, session 2017-18 (2017, February 9). AB-375, version February 9, 2017.

California State Legislature, session 2017-18 (2017, June 19). AB-375, version June 19, 2017.

California State Legislature, session 2017-18 (2017, September 12). AB-375, version September 12, 2017.

California State Legislature, session 2017-18 (2018, June 21). AB-375, version June 21, 2018.

California State Legislature, session 2017-18 (2018, June 25). AB-375, version June 25, 2018.

California State Legislature, session 2017-18 (2018, June 28). AB-375, version June 28, 2018.

California State Senate. (n.d.). Legislative Process. Retrieved June 28, 2020, from https://www.Senate.ca.gov/legislativeprocess

CALPIRG. (n.d.). Advocate for the public interest. Retrieved June 28, 2020, from https://calpirg.org/feature/cap/about-us

Canter, L., Tonsager, L., & Scott, A. (2020, January 10). State Legislatures Are Off to the Privacy Races, With New Hampshire in the Lead. Retrieved September 06, 2020, from https://www.insideprivacy.com/ccpa/state-legislatures-are-off-to-the-privacy-races-with-new-hampshire-in-the-lead/

Caviglione, L., & Coccoli, M. (2011). Privacy problems with Web 2.0. Computer Fraud & Security, 2011(10), 16–19. doi: 10.1016/s1361-3723(11)70104-x

CBS News. (2018, May 04). California now has the world's 5th largest economy. Retrieved November 23, 2020, from https://www.cbsnews.com/news/california-now-has-the-worlds-5th-largest-economy/

Chander, A., Kaminski, M. E. and McGeveran, W., Catalyzing Privacy Law (August 7, 2019). U of Colorado Law Legal Studies Research Paper No. 19-25.

Chiland, E. (2018, November 13). Amazon passes up LA for second headquarters. Retrieved May 11, 2020, from https://la.curbed.com/2018/11/13/18067044/amazon-hq2-los-angeles-headquarters

Clarip. (n.d.). Maryland Considering SB613 / HB0901 – Online Consumer Protection Act. Retrieved September 06, 2020, from https://www.clarip.com/blog/maryland-online-consumer-protection-act/

Clarip. (n.d.). State "CCPA" Privacy Bills in Rhode Island, Hawaii and New Jersey. Retrieved September 06, 2020, from https://www.clarip.com/blog/ri-hi-nj-privacy-bills/

Clement, J. (2020, February 28). Facebook ad revenue 2009-2018. Retrieved April 26, 2020, from https://www.statista.com/statistics/271258/facebooks-advertising-revenue-worldwide/

CMS. (2020). GDPR Enforcement Tracker - list of GDPR fines. Retrieved November 23, 2020, from https://www.enforcementtracker.com/?insights

Coalition of California Businesses, "SUBJECT: SB 1121 (DODD) – BUSINESS COMMUNITY REQUESTS TO BE INCLUDED IN AB 375 CLEAN-UP LEGISLATION" (2018). Historical and Topical Legal Documents. 1785.

Common Sense. (n.d.). Our Mission: Common Sense Kids Action. Retrieved June 28, 2020, from https://www.commonsensemedia.org/kids-action/about-us/our-mission

CompTIA. (2020, April). Cyberstates 2020. Retrieved September 05, 2020, from https://www.comptia.org/content/research/cyberstates-2020

Connecticut General Assembly. (2019). Connecticut SB01108: 2019: General Assembly. Retrieved September 06, 2020, from https://legiscan.com/CT/bill/SB01108/2019

Curia. (2015, October 1). JUDGMENT OF THE COURT (Third Chamber). Retrieved April 26, 2020, from http://curia.europa.eu/juris/document/document.jsf?docid=168944&doclang=EN

Daines, R. (2001). Does Delaware law improve firm value? Journal of Financial Economics, 62(3), 525–558. doi: 10.1016/s0304-405x(01)00086-1

Daniels, J. (2019, February 14). More Californians are considering fleeing the state as they blame sky-high costs, survey finds. Retrieved May 11, 2020, from https://www.cnbc.com/2019/02/12/growing-number-of-Californians-considering-moving-from-state-survey.html

Davis, W. (2020, July 10). California Sends Warning Letters Over CCPA Violations. Retrieved November 23, 2020, from https://www.mediapost.com/publications/article/353549/california-sends-warning-letters-over-ccpa-violati.html

Delaware Department of Labor. (n.d.). Office of Occupational and Labor Market Information - Long-Term Industry Projections. Retrieved September 05, 2020, from https://lmi.delawareworks.com/Content/Information/Projections-QCEW-LT.php

Delaware Division of Corporations - About the Division of Corporations. (n.d.). Retrieved from https://corp.delaware.gov/aboutagency/

DiCamillo, M. (2019). Release #2019-08: Leaving California: Half of State's Voters Have Been Considering This; Republicans and Conservatives Three Times as likely as Democrats and Liberals to be Giving Serious Consideration to Leaving the State. UC Berkeley: Institute of Governmental Studies. Retrieved from https://escholarship.org/uc/item/96j2704t

Difurio, D. (2019, November 30). Schwab is the latest company leaving California for Texas and it won't be the last, expert says. Retrieved May 11, 2020, from https://www.dallasnews.com/business/2019/11/30/schwab-is-the-latest-company-leaving-california-for-texas-and-it-wont-be-the-last-expert-says/

Dort, K. K., & Noordyke, M. S. (2020, May 15). Inside New Jersey's Latest Effort on the Privacy Front. Retrieved September 06, 2020, from https://www.law.com/legaltechnews/2020/05/15/inside-new-jerseys-latest-effort-on-the-privacy-front/

Edelstein, S. (2017, March 7). Which states follow California's emission and zero-emission vehicle rules? Retrieved April 26, 2020, from https://www.greencarreports.com/news/1109217_which-states-follow-Californians-emission-and-zero-emission-vehicle-rules

EDPB. (2020, June 03). Thirtieth Plenary session: EDPB response to NGOs on Hungarian Decrees and statement on Article 23 GDPR. Retrieved November 23, 2020, from https://edpb.europa.eu/news/news/2020/thirtieth-plenary-session-edpb-response-ngos-hungarian-decrees-and-statement-article_en

Employment Development Department of California. (2020). Employment by Industry Data. Retrieved September 05, 2020, from https://www.labormarketinfo.edd.ca.gov/data/employment-by-industry.html

Employment Development Department of California. (2020). Employment Projections. Retrieved September 05, 2020, from https://www.labormarketinfo.edd.ca.gov/data/employment-projections.html

Employment Development Department of California. (2020). Retrieved May 11, 2020, from https://www.labormarketinfo.edd.ca.gov/LMID/Size_of_Business_Data_for_CA.html

European Commission. (2018, January). EU Data Protection Reform: Ensuring its Enforcement. Retrieved November 23, 2020, from https://ec.europa.eu/info/sites/info/files/data-protection-factsheet-role-edpb_en.pdf

European Commission. (2019, May 25). GDPR in Numbers. Retrieved November 23, 2020, from https://ec.europa.eu/info/sites/info/files/infographic-gdpr_in_numbers.pdf

Evans, P. (2019, April 26). 16 mind-blowing facts about California's economy. Retrieved April 26, 2020, from https://www.businessinsider.nl/california-economy-16-mind-blowing-facts-2019-4?international=true&r=US

Fang, L. (2018, June 26). Google and Facebook Are Quietly Fighting California's Privacy Rights Initiative, Emails Reveal. Retrieved April 26, 2020, from https://theintercept.com/2018/06/26/google-and-facebook-are-quietly-fighting-Californians-privacy-rights-initiative-emails-reveal/

FCLCA. (n.d.). Lifecycle of a Bill. Retrieved June 28, 2020, from https://www.fclca.org/news-a-resources/lifecycle-of-a-bill.html

Fenwick, M., Kaal, W. A., & Vermeulen, E. P. (2016). Regulation tomorrow: what happens when technology is faster than the law. Am. U. Bus. L. Rev., 6, 561.

Florida Department of Economic Opportunity. (n.d.). Industry Projections (Long-term) for Multiple Industries in Florida in 2019-2027. Retrieved September 06, 2020, from https://freida.labormarketinfo.com/vosnet/analyzer/results.aspx?enc=9bfxYCUawMEI8NJGd4XMp3BWhc88lC Uyyf5mUqJADg

Florida Senate. (2020). HB 963: Consumer Data Privacy. Retrieved September 06, 2020, from https://flsenate.gov/Session/Bill/2020/963

Fortune Editors. (2020, March 3). Fortune 500. Retrieved April 26, 2020, from https://fortune.com/fortune500/

Frick, T. (2020, May 21). Is GDPR Good for the Environment? Retrieved June 2, 2020, from https://www.mightybytes.com/blog/is-gdpr-good-for-the-environment/

Giftos, M. (2020, February 24). Analyzing the 2020 Wisconsin Data Privacy Act (WDPA): Data Security & Privacy Rights: Husch Blackwell. Retrieved September 06, 2020, from https://www.bytebacklaw.com/2020/02/analyzing-the-2020-wisconsin-data-privacy-act/

Greenberg, P. (2020, January 3). 2019 Consumer Data Privacy Legislation. Retrieved May 11, 2020, from https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx

Hautala, L. (2020, January 3). California's new privacy rights could come to your state, too. Retrieved April 26, 2020, from https://www.cnet.com/news/Californians-new-ccpa-privacy-rights-could-come-to-your-state-too/

Hawaii House of Representatives. (2020). HB2572 A BILL FOR AN ACT RELATING TO PRIVACY. Retrieved September 06, 2020, from https://www.capitol.hawaii.gov/session2020/bills/HB2572_SD1_PROPOSED_.HTM

Heaphy, K. (2020, February 11). Arizona House of Representatives Proposes New Privacy Law. Retrieved September 06, 2020, from https://www.natlawreview.com/article/arizona-house-representatives-proposes-new-privacy-law

Hethcock, B. (2019, January 29). 1,800 Companies Left California In a Year - With Most Bound for Texas. Retrieved May 11, 2020, from https://www.southstarcommunities.com/blog/companies-leave-california-bound-for-texas

Hill, K. (2019, January 29). I Cut Google Out Of My Life. It Screwed Up Everything. Retrieved June 2, 2020, from https://gizmodo.com/i-cut-google-out-of-my-life-it-screwed-up-everything-1830565500

Hines, J. R. (2010). Treasure Islands. Journal of Economic Perspectives, 24(4), 103–126. doi: 10.1257/jep.24.4.103

Hintz, E., Sturm, J., & Kidwell, C. (2020, January 16). Analyzing the 2020 Nebraska Consumer Data Privacy Act. Retrieved September 06, 2020, from https://www.bytebacklaw.com/2020/01/analyzing-the-2020-nebraska-consumer-data-privacy-act/

Hoecke, M. V. (2015). Methodology of Comparative Legal Research. *Law and Method*. doi:10.5553/rem/.000010

Iacono, C. A., & Weiss, G. I. (2019, August 27). Preparing for Pennsylvania's Consumer Privacy Legislation. Retrieved September 06, 2020, from https://www.pietragallo.com/publications/preparing-for-pennsylvanias-consumer-privacy-legislation/

IAPP. (2020). Infographic: CCPA Enforcement. Retrieved November 23, 2020, from https://iapp.org/resources/article/infographic-ccpa-enforcement/

IBIS World. (2020, August 29). Data Processing & Hosting Services Industry in the US - Market Research Report. Retrieved September 05, 2020, from https://www.ibisworld.com/united-states/market-research-reports/data-processing-hosting-services-industry/

Illinois Department of Employment Security. (n.d.). Employment Projections. Retrieved September 06, 2020, from https://www2.illinois.gov/ides/lmi/Pages/Employment_Projections.aspx

Internet drar 10% av världens elanvändning - och andelen stiger. (2019, February 14). Retrieved June 2, 2020, from https://cornucopia.cornubot.se/2019/02/internet-drar-10-av-varldens.html?m=1

Intersoft Consulting. (2018, December 03). GDPR - Consent. Retrieved October 05, 2020, from https://gdpr-info.eu/issues/consent/

Jia, J., Jin, G. Z., & Wagman, L. (2018). The Short-Run Effects of GDPR on Technology Venture Investment. doi: 10.3386/w25248

Johnson, K. (2020, March 13). Washington Privacy Act fails again, but state legislature passes facial recognition regulation. Retrieved September 06, 2020, from https://venturebeat.com/2020/03/12/washington-privacy-act-fails-in-state-legislature-again/

Kalnenaite, D. (2019). Maine Privacy Law Guide. Retrieved September 06, 2020, from https://iapp.org/resources/article/maine-privacy-law-guide/

Katz, D. F. (2020, January 21). Like CCPA, But Make it Virginia: States Scramble to Introduce Data Privacy Legislation of Their Own: News & Knowledge: Adams and Reese LLP. Retrieved September 06, 2020, from https://www.adamsandreese.com/news-knowledge/like-ccpa-but-make-it-virginia-states-scramble-to-introduce-data-privacy-legislation-of-their-own

Kolmar, C. (2020, January 29). These Are The 100 Biggiest Comapnies In California. Retrieved April 26, 2020, from https://www.zippia.com/advice/biggest-companies-in-california/

Kulp, P. (2020, January 09). New Mexico's Data Privacy Efforts Stall, but It's Not Over. Retrieved September 06, 2020, from https://www.adweek.com/digital/new-mexicos-data-privacy-efforts-stall-but-theres-an-appetite-to-pass-legislation/

Lande, J. (2020, June 16). Is Iowa Going to Provide California-Style Data Privacy Rights? Retrieved September 06, 2020, from https://www.jdsupra.com/legalnews/is-iowa-going-to-provide-california-10190/

Louisiana State Legislature. (2019). Louisiana HR249: 2019: Regular Session. Retrieved September 06, 2020, from https://legiscan.com/LA/bill/HR249/2019

Marini, A., Katefides, A., Bates, J., Zanfir-Fortuna, G., Bae, M., Gray, S., & San, G. (2018, November). Comparing privacy laws: GDPR v. CCPA. Retrieved December 2, 2019, from https://fpf.org/wp-content/uploads/2018/11/GDPR_CCPA_Comparison-Guide.pdf.

Massachusetts Department of Labor & Workforce Development. (n.d.). Massachusetts Occupational and Industry Projections. Retrieved September 06, 2020, from https://www.mass.gov/massachusetts-occupational-and-industry-projections

Massachusetts General Court. (2020). Bill S.120 191st. Retrieved September 06, 2020, from https://malegislature.gov/Bills/191/S120

Merryman, J. H. (1974). Comparative Law and Scientific Explanation. *The American Journal of Comparative Law, 22*(Suppl_1), 81-104. doi:10.1093/ajcl/22.suppl1.81

Michigan Department of Labor and Economic Opportunity. (n.d.). Employment Projections. Retrieved September 06, 2020, from https://milmi.org/datasearch/projections

Murugesan, S. (2007). Understanding Web 2.0. IT Professional, 9(4), 34–41. doi: 10.1109/mitp.2007.78

Myers, J. (2019, November 4). Newsletter: California interest groups near the $300-million mark in Sacramento lobbying. Retrieved April 26, 2020, from https://www.latimes.com/politics/story/2019-11-04/essential-politics-newsletter-california-interest-groups-300-million-dollars-lobbying-sacramento

New York State Department of Labor. (n.d.). Employment Projections. Retrieved September 06, 2020, from https://www.labor.ny.gov/stats/lsproj.shtm

Noordyke, M. (2020, July 6). US State Comprehensive Privacy Law Comparison. Retrieved September 06, 2020, from https://iapp.org/resources/article/state-comparison-table/

North Dakota Legislative Assembly. (2019). North Dakota HB1485: 2019-2020: 66th Legislative Assembly. Retrieved September 06, 2020, from https://legiscan.com/ND/bill/1485/2019

NY State Senate. (2019, July 25). NY State Senate Bill S5575B. Retrieved November 23, 2020, from https://www.nysenate.gov/legislation/bills/2019/s5575

NY State Senate. (2020, January 09). NY State Senate Bill S224. Retrieved November 23, 2020, from https://www.nysenate.gov/legislation/bills/2019/s224

NY State Senate. (2020, July 27). NY State Senate Bill S8448D. Retrieved November 23, 2020, from https://www.nysenate.gov/legislation/bills/2019/s8448/amendment/d

Ohio Department of Job and Family Services. (n.d.). Employment Projections. Retrieved September 06, 2020, from https://ohiolmi.com/home/Projections

Olson, E. (2019, August 20). PossibleNOW™ Survey: As California Consumer Privacy Act Enforcement Ap. Retrieved from https://www.prweb.com/releases/possiblenow_survey_as_california_consumer_privacy_act_enforcement_approaches_56_of_businesses_report_they_will_not_be_fully_prepared/prweb16512360.htm

O'Reilly, L. (2020, November 05). Prop 24 - the California Privacy Rights and Enforcement Act - passed by voters. Here's what publishers need to know. Retrieved November 23, 2020, from https://digiday.com/media/prop-24-the-california-privacy-rights-and-enforcement-act-passed-by-voters-heres-what-publishers-need-know/

Our Members. (n.d.). Retrieved April 26, 2020, from https://internetassociation.org/our-members/

Pennsylvania Department of Labor and Industry. (n.d.). Projections, Occupational/Industries. Retrieved September 06, 2020, from https://www.workstats.dli.pa.gov/Products/employment-projections/Pages/default.aspx

Phillips, R., Gardner, M., Robins, A., & Surka, M. (2017). Offshore Shell Games 2017 - The Use of Offshore Tax Havens by Fortune 500 Companies.

Pieters, D. (2009). Functions of comparative law and practical methodology of comparing. Syllabus Research Master in Law, Leuven-Tilburg.

PPIC. (2019, May 15). The Initiative Process in California. Retrieved June 28, 2020, from https://www.ppic.org/publication/the-initiative-process-in-california/

Princen, S. (1999). The California Effect in the EC's External Relations. ECSA Sixt Biennial International Conference Pittsburgh, Pennsylvania, 2-5.

Romano, R. (1985). Law as a Product: Some Pieces of the Incorporation Puzzle. The Journal of Law, Economics, and Organization, 225–283. doi: 10.1093/oxfordjournals.jleo.a036892

Ropek, L. (2019, July 18). NY's Data Privacy Bill Failed; Is There Hope Next Session? Retrieved November 23, 2020, from https://www.govtech.com/policy/NYs-Data-Privacy-Bill-Failed-Is-There-Hope-Next-Session.html?AMP

Rosenkoetter, E. (2020, March 11). Large and Small Privacy Bills Introduced in the Land of 10,000 Lakes (think Mille Lacs vs. Bemidji): The CFS Blog. Retrieved September 06, 2020, from https://consumerfsblog.com/2020/03/large-and-small-privacy-bills-introduced-in-the-land-of-10000-lakes-think-mille-lacs-vs-bemidji/

Rosenkoetter, E. (2020, March 3). 'Consumer Data Privacy Act' Introduced in Mississippi With Expansive Coverage: The CFS Blog. Retrieved September 06, 2020, from

https://consumerfsblog.com/2020/03/consumer-data-privacy-act-introduced-in-mississippi-with-expansive-coverage/

Sanchez, K. (2019, November 7). For 7th Year in a Row, More People Left California Than Moved in: Data. Retrieved May 11, 2020, from https://www.nbcbayarea.com/news/local/Californians-leaving-state-data/2078950/

Schiff, A. (2020, September 28). It May Seem All Quiet On The CCPA Front, But Don't Get Complacent: CCPA Enforcement Has Begun. Retrieved November 23, 2020, from https://www.adexchanger.com/privacy/it-may-seem-all-quiet-on-the-ccpa-front-but-dont-get-complacent-ccpa-enforcement-has-begun/

Scott, A., & Tonsager, L. (2019, June 24). Nevada's New Consumer Privacy Law Departs Significantly From The California CCPA. Retrieved September 06, 2020, from https://www.insideprivacy.com/united-states/state-legislatures/nevadas-new-consumer-privacy-law-departs-significantly-from-the-california-ccpa/

Senate Committee on Energy, Utilities and Communications (2017, July 17) Bill Analysis, AB-375. Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

Senate Floor (2017, September 15) Bill Analysis, AB-375. Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

Senate Floor (2018, June 28). Bill Analysis, AB-375 Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

Senate Judiciary Committee (2017, July 18) Bill Analysis, AB-375. Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

Senate Judiciary Committee (2018, June 25) Bill Analysis, AB-375. Retrieved June 28, 2020, from https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375

Seo, J., Kim, K., Park, M., Park, M., & Lee, K. (2018). An Analysis of Economic Impact on IoT Industry under GDPR. Mobile Information Systems, 2018, 1–6. doi: 10.1155/2018/6792028

Siems, M. (2014). Comparative Law. *SSRN Electronic Journal*. doi:10.2139/ssrn.2512938

Sivas, D. A. (2018, April 4). Rolling Back Green Energy Standards? Retrieved April 26, 2020, from https://law.stanford.edu/2018/04/04/rolling-back-green-energy-standards/

South Carolina General Assembly. (2020). H4812: 2019-2020: South Carolina Biometric Data Privacy Act. Retrieved September 06, 2020, from https://www.scstatehouse.gov/sess123_2019-2020/bills/4812.htm

State of California Department of Justice. (2020, May 06). Ballot Initiatives. Retrieved June 28, 2020, from https://oag.ca.gov/initiatives

Stauss, D., & Rogers, M. (2020, January 14). Analyzing the 2020 Illinois Data Transparency and Privacy Act. Retrieved September 06, 2020, from https://www.bytebacklaw.com/2020/01/analyzing-the-2020-illinois-data-transparency-and-privacy-act/

Subramanian, G. (2002). The Disappearing Delaware Effect. SSRN Electronic Journal. doi: 10.2139/ssrn.345040

Texas Privacy Protection Advisory Council. (2020, September). Texas Privacy Protection Advisory Council Interim Report to the 87th Legislature. Retrieved November 23, 2020, from https://senate.texas.gov/cmte.php?c=990

Texas State Legislature. (2019). Texas HB4390: 2019-2020: 86th Legislature. Retrieved September 06, 2020, from https://legiscan.com/TX/bill/HB4390/2019

Texas Workforce Commission. (2020). Current Employment Statistics (CES). Retrieved September 05, 2020, from https://texaslmi.com/LMIbyCategory/CES

Texas Workforce Commission. (n.d.). Texas Wages and Employment Projections, 2016-2026 Employment Projections. Retrieved September 05, 2020, from https://texaswages.com/Projections

Tørsløv, T., Wier, L., & Zucman, G. (2018). The Missing Profits of Nations. doi: 10.3386/w24701

Tsukayama, H. (2019, September 4). Lawmakers Must Not Listen to the Internet Association and Weaken the California Consumer Privacy Act. Retrieved April 26, 2020, from https://www.eff.org/nl/deeplinks/2019/09/lawmakers-must-not-let-internet-association-weaken-california-consumer-privacy-act

U.S. Bureau of Labor Statistics. (2018, September). Quarterly Census of Employment and Wages - 2018, Q1. Retrieved September 05, 2020, from https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm

U.S. Bureau of Labor Statistics. (2020, September). Quarterly Census of Employment and Wages - 2020, Q1. Retrieved September 05, 2020, from https://data.bls.gov/cew/apps/table_maker/v4/table_maker.htm

UCLA. (2020, February 5). LibGuides: California Legislative Advocacy: Introduction. Retrieved June 28, 2020, from https://libguides.law.ucla.edu/c.php?g=183363

US Bureau of Labor Statistics. (2020, March 4). Business Employment Dynamics in California – Second Quarter 2019 : Western Information Office. Retrieved May 11, 2020, from https://www.bls.gov/regions/west/news-release/businessemploymentdynamics_california.htm

Vehicle Emissions California Waivers and Authorizations. (2020, February 20). Retrieved April 26, 2020, from https://www.epa.gov/state-and-local-transportation/vehicle-emissions-california-waivers-and-authorizations

Virginia Employment Commission. (n.d.). Industry Projections. Retrieved September 06, 2020, from https://virginiaworks.com/industry-projections?page80170=1

Vogel, D. (1995). Trading up: Consumer and Environmental Regulation in a Global Economy. Foreign Affairs, 74(6), 119. doi: 10.2307/20047393

Wicker, R. (2020, May 07). S.3663 - 116th Congress (2019-2020): COVID-19 Consumer Data Protection Act of 2020. Retrieved November 23, 2020, from https://www.congress.gov/bill/116th-congress/senate-bill/3663