**Contrast of the General Data Protection Regulation (GDPR) vs. California Consumer Privacy Act (CCPA)**

Barrett Franks

IST618 Syracuse University

Professor Raed Sharif

February 22, 2022

The General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) are data protection laws put in place by the European Union (EU) and the State of California respectively to govern the protection of personal data. While broadly speaking the baseline “person” and the subject matter covered are similar the implementation, application and scope of the law sets differ substantially. I intend to dive into the background, who is protected, what data is protected, who has to comply, rights afforded to individuals and penalties under both law sets. Finally, based on the aforementioned assessment, an opinion on whether either set of data privacy laws have practical application for expansion in other states within the United States of America.

The GDPR went into effect in 2018 and is currently recognized as law across member countries (note: since Brexit the United Kingdom follows “UK GDPR” and principalities of Europe like Monaco generally follow the GDPR; however, they seem to be afforded more flexibility to cherry pick applicability). Simply put, the GDPR was implemented to give EU citizens more rights and control over their personal data in an age of what is overwhelmingly a digital economy. With much commerce conducted online private individual data is shared with a variety of businesses - which if unregulated can be sold to third parties. While often this is somewhat harmless (advertising, etc.) personal data in the wrong hands can be used maliciously (fraud, identity theft, etc.) - under GDPR protection companies have to ensure they collect personal data in a controlled manner as well as manage and protect personal data from misuse. Penalties are defined to help enforce these regulations.

The CCPA went in effect in 2020 and similarly affords residents certain rights over their personal data. The CCPA applies to companies operating in California that either a) make at least $25 million in annual revenue b) gathers data on more than 50,000 users or c) derives more than fifty percent of annual revenue from selling user data. The CCPA allows residents to be able to see what data companies have gathered about them, have that data deleted, and opt out of those companies selling it to third parties. The enforcement of the CCPA is primarily upheld by the California Attorney General and can include civil penalties that differ depending on whether the breach was intentional or unintentional.

The logical place to start is to understand who is covered under both sets of laws. Under California code 1798.140(g) the CCPA defines “Consumer” as *“a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier.”[1].* Whereas, under Recital 14 the GDPR defines who is protected as *“The protection afforded by this Regulation should apply to natural persons, whatever their nationality or place of residence, in relation to the processing of their personal data”[2]*. Interestingly, neither law set uses the term “citizen” - therefore, all persons residing in the region are covered under the respective law set. So although the language surrounding the laws are different the broad reach and focus appears to be the same in that both sets of laws seek to cover identifiable natural persons within the jurisdiction in question.

In terms of what information is protected both sets of laws are somewhat similar - although not identical. Under California code 1798.140(o) the CCPA defines “Personal Information” as *“information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household”[1]*. Whereas, under Article 4(1) the GDPR defines this as *“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” {2]*. The GDPR is more explicit in terms of examples - which is likely helpful from a legal perspective. It could be argued that the CCPA covers all the same things as the GDPR; however, in my opinion the CCPA leaves grey area due to the language “reasonably capable of being associated with”. For example, (assuming all other conditions are met) under the CCPA if a company tags me at a conference in California it could be argued that this doesn’t necessary identify me individually - even though someone could use this information to infer that I am not at my house. Under the GDPR this same example is explicitly blocked. Further, it is interesting that under the CCPA “household” is included in the scope of personal information - whereas in the GDPR the extent is limited to an individual / natural person. While the spirit of both sets of laws seem to be substantially similar I believe, based on the above points, it is a misread to call the scope of definition for personal information anything more than “somewhat similar” between the two sets of laws. The GDPR is clearly more explicit where the CCPA leaves room for interpretation.

After understanding who is protected and what data must be protected it is important to understand who is regulated. Under California code 1798.140(c) the CCPA defines “Business” that must uphold the CCPA as *“A sole proprietorship, partnership, limited liability company, corporation, association, or other legal entity that is organized or operated for the profit or financial benefit of its shareholders or other owners, that collects consumers’ personal information, or on the behalf of which such information is collected and that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information, that does business in the State of California, and that satisfies one or more of the following thresholds:(A) Has annual gross revenues in excess of twenty-five million dollars ($25,000,000), as adjusted pursuant to paragraph (5) of subdivision (a) of Section 1798.185.(B) Alone or in combination, annually buys, receives for the business’ commercial purposes, sells, or shares for commercial purposes, alone or in combination, the personal information of 50,000 or more consumers, households, or devices.(C) Derives 50 percent or more of its annual revenues from selling consumers’ personal information.”[1]*. Whereas, the GDPR offers two definitions for different standards to match the above CCPA definition. Under Article 4(7) the GDPR defines “Controller” as *“the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law” {2]*. And under Article 4(8) defines “Processor” as “*a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller” {2].* Before jumping into the comparison of the two sets of laws it is important to draw a line between “Controller” and “Processor”. Under Article 5(2) the GDPR states “*The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ‘accountability’.”[2]*. This is to say that the controller is the main party responsible for data governance.

In terms of coverage of responsible parties these laws are vastly different. The GDPR is far more extensive in coverage and incorporates all persons (natural or legal) - by contrast the CCPA has conditions that must be met before a business qualifies to be regulated. The blanket coverage of the GDPR, while more extensive, actually simplifies the applicability in my opinion. Even though the conditions of the CCPA are straight forward there obviously are many companies (and individuals) that do not meet the criteria. For example, a section 501(c)(3) company does not meet the criteria, small business do not always meet the criteria, similarly a partially owned subsidiary of a major corporation may not meet the requirements to be regulated. Data breaches and / or selling and sharing of personal data is no less harmful because a company does not meet the criteria of the CCPA. Given the spirit of each of the law sets is to protect personal information it makes more sense to hold accountable any person (natural or legal) who is in the position of control over the data. For this reason I think the blanket coverage of the GDPR provides more protection to the individual / data subject.

Under both law sets there is a lot to unpack regarding rights of the individual including security, privacy notice, opt-out, disclosures, deletion, etc. Given the theme of the IST618 class it feels most appropriate to focus on privacy notice and security. Under California code 1798.100(b) the CCPA describes privacy notices due to an individual as *“A business that collects a consumer’s personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section”*[1]. 1798.100 continues on to describe what the individual needs to be notified of. Under Article 13(1) the GDPR defines this as “*Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information: (a) the identity and the contact details of the controller and, where applicable, of the controller’s representative; (b) the contact details of the data protection officer, where applicable; (c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing; (d) where the processing is based on point (f) of*[*Article 6*](https://gdpr-info.eu/art-6-gdpr/)*(1), the legitimate interests pursued by the controller or by a third party; (e) the recipients or categories of recipients of the personal data, if any; (f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in*[*Article 46*](https://gdpr-info.eu/art-46-gdpr/)*or*[*47*](https://gdpr-info.eu/art-47-gdpr/)*, or the second subparagraph of*[*Article 49(*](https://gdpr-info.eu/art-49-gdpr/)*1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available[2].* Note: Article 13(2) continues to talk about further notification to ensure fair and transparent processing. This is probably the first portion I have analyzed that has near parity between the two sets of laws. Both law sets are very thorough and explicit in definition of what privacy notices need to be provided to individuals about their personal data collection. In the case of privacy notification it is fair to say the laws are very similar in intent, scope and method of execution.

In terms of security under California code 1798.100(e) *“A business that collects a consumer’s personal information shall implement reasonable security procedures and practices appropriate to the nature of the personal information to protect the personal information from unauthorized or illegal access, destruction, use, modification, or disclosure in accordance with Section 1798.81.5.”*[1]. And under Article 24(1) the GDPR defines this as “*Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, the controller shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*”[2]. Both laws center around “appropriate” or “reasonable” security measures. While these laws are very similar in construction I believe both miss the mark. In this day and age of security it is fairly common to be explicit about what data is accessible by employees of organizations, encryption standards, two factor authentication, disaster recovery, etc. Typically this is demonstrated by a company having SOC 2 controls in place - which I believe is not an unreasonable standard for the CCPA or the GDPR to require. So while the basis of the laws around security are similar I believe they are not sufficient to govern personal data security.

Finally, penalties under California code 1798.155(b) are defined as *“A business shall be in violation of this title if it fails to cure any alleged violation within 30 days after being notified of alleged noncompliance. Any business, service provider, or other person that violates this title shall be subject to an injunction and liable for a civil penalty of not more than two thousand five hundred dollars ($2,500) for each violation or seven thousand five hundred dollars ($7,500) for each intentional violation”[1]*. Penalties under the GDPR are described under Articles 83 & 84 - the wording is lengthy, however, in summary the fines can reach up to 20 million Euro or 4% of annual global revenue (whichever is higher). Clearly the fines that can be levied under the GDPR are far more excessive than that of the CCPA. In my opinion it is difficult to put a price on personal data breaches; the damage is probably dependent on what happens after the fact and over time - so while the GDPR seems excessive it could be argued it is appropriate in some cases. The only thing in my opinion that is evident from the comparison of the two law sets is that the CCPA is far too light in terms of penalties - these fines would be a drop in the bucket for any company and would not necessarily dis-incentivize future data breaches.

After analyzing both sets of regulations it is apparent the CCPA is fairly broad, but often under specific when compared to the GDPR. The GDPR does a much better job of being explicit and extensive to ensure better coverage to protect personal data. This is most clearly demonstrated when analyzing what data is protected and who is regulated. The GDPR additionally has the ability to levy far harsher punishments to ensure personal data is protected. So while both sets of laws start from a place of agreement about what data is protected, they deviate vastly in approach and scope. In my opinion the CCPA is better than nothing; however, does not seem sufficient to protect such important and often sensitive data. The CCPA is often written like it was composed by lawmakers; opposed to the GDPR that feels more like it was written in conjunction with technology professionals. My only criticism of the GDPR, based on the analysis I completed, was around security. Neither law set did a good job of defining security practices. While this is likely intentional as it is tough to blanket impose security standards it was surprising to not see any guidance offered in the GDPR. In conclusion, if I were tasked with implementing data privacy laws in another state I would try to model the regulations around the GDPR as it is a much more thorough law set that really supports the intent of the regulation - to protect personal information.