2024

Comparative Analysis of Two Data Privacy Regulatory Schemes: The GDPR and the CCPA

Sean Bradley

Sean Bradley

Startup Counseling

December 15, 2023

Comparative Analysis of Two Data Privacy Regulatory Schemes: The GDPR and the CCPA

I. INTRODUCTION

In 2019, 98 senior executives were asked what is the top emerging risk concerning their business.[1] The majority of respondents listed "accelerating privacy regulation" as their primary concern, with 70% of executives in the financial services, consumer goods, technology, and telecommunications sectors reporting it as their chief concern for the future.[2] The respondents anticipated higher costs of compliance and more privacy regulations to pass in the near future.[3] Four years later, it is clear that these executives were right to anticipate a wave of new privacy legislation, as evidenced by laws recently passed in several US states, China and Brazil.[4] As new privacy laws continue to be passed, companies seek guidance on what their privacy policies should look like, what the risk factors are, and whether it is practical to achieve full compliance with differing legal schemes.

The digital era has been considered to be the fourth industrial revolution, and in this economy, personal data is among the most valuable resources. One of the many technological

[1] *Gartner Survey Shows Accelerating Privacy Regulation Returns as the Top Emerging Risk Worrying Organizations in* 1Q19, Gartner, https://www.gartner.com/en/newsroom/press-releases/2019-04-11-gartner-survey-shows-accelerating-privacy-regulation-returns-as-the-top-emerging-risk-worrying-organizations-in-1q19.
[2] *Id*.
[3] *Id*.
[4] *Data Privacy Laws: What You Need to Know in 2023*, Osano, https://www.osano.com/articles/data-privacy-laws.

advances at the forefront of this new economy is the ubiquity of personal computing devices, such as personal computers, smartphones, and other types of 'smart' devices connected to the internet. As the use of these devices became more widespread, the amount of personal data generated grew as well.

In the wake of Edward Snowden's reporting in 2013 which detailing how the National Security Agency was using Americans' personal data to surveil its own citizens, data privacy became a focal point of political discussion.[5] Following, the Cambridge Analytica scandal of 2018, citizens became increasingly wary that neither the government nor corporations were using personal data in a way that prioritized personal privacy.[6] Consumers recognized that the free flow of information is one of the pillars of the modern economy but should be tempered to prevent misappropriation of their personal information. While most countries had privacy laws dating back to the 20th century, the digital economy and the globalization thereof necessitated laws that are drafted through the perspective of today's technologies. The European Union and the state of California are at the forefront of this new wave of data privacy regulation, enacting laws to address the tension between consumers rights over their personal data and the corporate interest in using that data for commercial purposes. This paper seeks to show how these regulatory schemes address that tension, specifically what rights they grant to consumers and what obligations are imposed on corporations in light of those consumer rights.

A. Historical Development of Data Collection

[5] *NSA Files:* Decoded, The Guardian, https://www.theguardian.com/world/interactive/2013/nov/01/snowden-nsa-files-surveillance-revelations-decoded.
[6] *Facebook's Cambridge Analytica Controversy Could Be Big Trouble for the Social* Network, TIME, https://time.com/5205314/facebook-cambridge-analytica-breach/.

The modern landscape of the digital economy began with the introduction of Google search in 1997.[7] In 2006, Amazon Web Services began offering cloud computing, allowing data to be collected in a more efficient and inexpensive manner.[8] Most notably, cloud computing rendered hard limits on data storage size obsolete, thereby reducing the challenge of finding enough space to store data at scale. When companies began collecting personal data in 1986, the global capacity for data storage was 2.6 exabytes, too little for companies to be storing personal data at scale.[9] That number reached 295 exabytes in 2007 following the advent of Amazon Web Services cloud computing, and in 2020, the amount of available data storage was approximately 6,800 exabytes.[10]

B. Personal Data as a Commodity

There are many ways in which companies profit from the use of personal data, such as direct advertising, predictive analytics, and tailoring products to meet individuals' interests. Companies use data, including age, sex, ethnicity, religion, and personal interests to ensure that advertisements are targeted at individuals who are more likely to interact with a given advertisement.[11] This allows advertisers to market to specific segments of the population, and earn higher returns on investments from their advertising dollars through higher engagement, while also providing some utility to consumers as their needs and interests are more reflected in the advertisements they see.[12] For example, a 25-year-old male who frequently posts to Facebook

[7] *A History and Timeline of Big* Data, Tech Target, https://www.techtarget.com/whatis/feature/A-history-and-timeline-of-big-data
[8] *Id.*
[9] *Id.*
[10] *Id*.
[11] *Principles of Marketing – Advertising and Direct* Marketing, University of Minnesota Libraries, https://open.lib.umn.edu/principlesmarketing/chapter/11-4-advertising-and-direct-marketing/
[12] *Id*.

about his passion for running will likely see advertisements from companies in the running industry which purchase the right to the advertise to those in their target demographic. This benefits the company selling advertising space, the company purchasing the advertising space, and the consumer who now receives advertisements for products he may actually need or want. Companies are able to analyze large pools of data to identify market trends enabling them to craft their products and services in light of these trends.[13] For example, a company in an emerging market such as electric vehicles may collect billions of data points from thousands of people across multiple demographics for insight as to what specific demographics respond positively to their product.

The commodification of personal data is not a novel concept; it is, however, still in a period of exponential growth.[14] In 2013, the global market for data collection reached an estimated ten billion dollars, and in 2020, was estimated to be nearly 200 billion dollars.[15] Among the most valuable forms of personal data are, health care records which sell for $250, credit card details which sell for $5.50 on average, and banking records, which sells for about $4.[16] There are three primary ways by which companies collect consumer data: (1) the company asks the consumer directly, typically when an individual signs up for a subscription, completes a survey, or purchases a product; (2) the company uses tracking technology such as cookies or web beacons which allow them to see what a customer has seen and clicked on; and (3) the company

[13] *What is Predictive Analytics? 5 Examples*, Harvard Business School, https://online.hbs.edu/blog/post/predictive-analytics.
[14] *How Much is Your Data Worth? The Complete Breakdown for 2024,* Invisibly, https://www.invisibly.com/learn-blog/how-much-is-data-worth/.
[15] *Id.*
[16] *How Much is Your Data Worth? The Complete Breakdown for 2024,* Invisibly, https://www.invisibly.com/learn-blog/how-much-is-data-worth/.

purchases the data from a third party such as Oracle, and other companies whose primary business is purchasing and selling personal data.[17]

C. History and Purpose of European Data Privacy Law

The European Union's ("EU") Data Policy Directive (the "Directive"), of 1995 was the first form of privacy regulation to mandate all EU member states to adopt regulatory schemes.[18] However, the Directive did not permit data to be transferred out of the European Economic Area unless the country receiving the data had adequate protective measures, a standard that even the United States could not meet.[19] The Directive was largely ineffective because it was only a directive which, under European law, is not binding on all member states.[20] The European Parliament enacted the General Data Privacy Regulation ("GDPR") which "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data."[21] The GDPR built on the Directive by providing more efficient mechanisms for the flow of data outside of the EU, and binding all 28 member states to achieve a more uniform system of compliance while respecting each member states' sovereignty.

The GDPR was an outgrowth of the 1995 Directive intended to respect individuals' fundamental right to the protection of their data, and to promote the free flow of personal data

[17] *How Do Big Companies Collect Customer Data*, IT Chronicles, https://itchronicles.com/big-data/how-do-big-companies-collect-customer-data/.
[18] Council Directive 95/46/EC, O.J. (L 281) 31.
[19] This was overcome by the US-EU Safe Harbor.
[20] *Types of* Legislation, European Union, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en.
[21] General Data Protection Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data on the Free Movement of Such Data, and Repealing Directive 95/46/EC, 2016 O.J. (L 119) 1, 34 (EU), art. 51(4).

within the EU.[22] The Regulation expressly grants eight rights to European individuals whose data is subject to collection, specifically the rights to: (1) know what data is being collected and its use; (2) access copies of the personal data being collected; (3) rectify inaccuracies in their personal information; (4) compel a company or organization to erase their personal data; (5) restrict processing and the purposes for which a company may use their personal data; (6) obtain and reuse their personal data; (7) object to an official authority's use of their personal data; and (8) reject the use of automated decision making, to make calculated presumptions about individuals.[23] The regulation emphasizes the importance of protecting personal data specifically when it is being transferred outside of the EU. The preamble acknowledges that technological advances have accelerated the information available for use in the public and private sector, and made the implementation of safeguards for data transfers one of the pillars of the GDPR.[24]

D. History and Purpose of California Data Privacy Law

The California Legislature enacted the California Consumer Privacy Act ("CCPA") in 2020 with the intention of providing consumers greater rights over their data.[25] Specifically, the Act provided the rights to: (1) know about the personal information a business collects about them and how it is used and shared; (2) deletion of personal information collected from them (some exceptions apply); (3) opt-out of the sale of sharing of their personal information; and (4) non-discrimination for exercising their rights under the CCPA.[26] Soon after, the California

[22] The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union and Article 16(1) of the Treaty on the Functioning of the European Union provide that everyone has the right to the protection of personal data concerning him or her.
[23] *GDPR* 2016/679 Chapter III
[24] *GDPR* 2016/679 Recital 6
[25] CAL. CIV. CODE §§ 1798.100-80 (West 2023).
[26] *Id.*

Privacy Rights Act ("CPRA") was passed via ballot initiative in 2020 and the majority of its provisions became operative in January, 2023 which modified and amended the CCPA. In addition to the rights provided under the CCPA, the CPRA added additional layers of data privacy, including two additional rights: (5) to correct inaccurate personal information that a business has about them; and (6) limit the use and disclosure of sensitive personal information collected about them.[27]. The CPRA does not create a law separate from the CCPA and the state Attorney General Office refers to the law as "CCPA" or "CCPA as amended," so this analysis will refer to the California legal framework as the "CCPA."

II. LEGAL FRAMEWORKS OF THE GDPR AND CCPA

Both regulations seek to balance the interests of consumers in protecting their personal data and the corporate interest in utilizing that data for profit and transactional efficiency.[28] The differences in the two regulatory schemes are reflective of the jurisdictions' differing legal philosophies, namely, with respect to privacy. Europe considers data privacy as a fundamental human right but is without the ability to ground that aspiration in enforceable law due to the EU governing structure and delegation of police powers to the individual member states. It follows then, that under the GDPR, personal data cannot be used for commercial purposes without the consent of individual consumers.[29] The right to privacy is not expressly granted under American or California law, so corporations, generally, can collect and use personal data, unless there is some law preventing them from doing so. Additionally, United States federal law protects free speech, including that of non-natural persons, such as corporations.[30] The difference in the two

[27] *Id*.
[28] Anupam Chander et. al., *Catalyzing Privacy Law*, 105 Minn. L. Rev. 1733, 1747 (2021).
[29] *GDPR,* 2016/670 Chapter III
[30] 47 U.S.C.A § 230 (West 2020).

philosophies underpinning the GDPR and the CCPA can be summarized by this: the EU takes a proactive stance toward safeguarding personal data while the California framework, is more reactive in its approach. However, it is clear that both regulations seek to provide consumers with more power over the use of their data while imposing a strict obligation of transparency for any company subject to these laws.

A. Scope

The scope of each regulation can be broken down into the material scope and the territorial scope. First, the material scope of the GDPR applies to the processing of personal data which essentially encompasses any activity related to the use of personal data.[31] Processing can be done either by the controller or a separate entity that the controller designates the processor.[32] The former can be thought of as the entity which *obtains* the data while the latter *uses* the data.[33] They are not always two separate entities. It is common for the controller to also be the processor but the opposite is never true.[34] The controller oversees and sets parameters by which the processor must comply with. To summarize, the GDPR regulates entities that collect and process personal data.[35]

Whereas the material scope establishes that the GDPR regulates processing of personal data, the territorial scope clarifies that the processing is only regulated if (1) the controller or processor is in the EU, and (2) the data being processed (a) belongs to individuals within the EU,

[31] *GDPR* 2016/679 Art. (2)
[32] *GDPR* 2016/679 Art. (24)
[33] *See GDPR* 2016/679 Art. (24); Art. (28).
[34] *GDPR* 2016/679 Art. (24).
[35] *GDPR* 2016/679 Art. (2).

or (b) relates to the offering of goods or services in the EU.[36] In addition to controllers and processor in the EU, the regulation imposes an extra-territorial scope, meaning that any controller or processor with no physical presence in the EU but participates in the European market is bound by the regulation.[37] Although extra-territorial jurisdiction is not a novel concept of law, it is significant in the context of privacy law by virtue of the fact that personal data is an intangible commodity that is not easily traceable. This becomes relevant in the context of data transfers where the law imposes stringent requirements that seem to be addressing the difficulty not only from tracing data, but also ensuring that each party in the chain of custody is ensuring the same level of protections as the initial controller and processor.

The scope of the CCPA is substantially similar to that of the GDPR, with some minor difference. First, the CCPA is aimed directly at businesses while the GDPR has a broader aim, that is intended to target any entity, regardless of whether it is used for commercial purposes. Under the CCPA, any for profit entity that collects personal information, or any entity that subsequently process that information, so long as one of the following thresholds is met: (1) annual gross revenues in excess of $25 million; (2) buys, receives, sells, or shares the personal information of 100,000 or more consumers or households annually; or (3) derives 50% or more of its annual revenues from selling consumers' personal information.[38]

B. Consumer Rights

The rights granted to consumers by each legislative body confers obligations on the part of controllers and processors to ensure that these rights are being respected. There is a significant

[36] *GDPR* 2016/679 Art. (3)
[37] *Id.*
[38] CCPA § 1798.140(d).

overlap between those granted by each regulation, so only those which create obligations on controllers and processors will be addressed, and consist of the rights to: (1) *know* that their data is being collected and processed, for what purposes and in the case of transfers, what safeguards are employed; (2) *deletion* when collection and processing is being used beyond the purposes for which the consumer consented to; (3) *correction* of inaccurate personal data; (4) *opt-out* of the sale or transfer.[39]. Once the threshold issue of who or what is within the scope of each regulation, the question then becomes, what obligations are those entities bound by? Before addressing that question, a practical explanation of the timeline of data collection and processing is due. When personal data is collected for commercial purposes, it is rarely just a one-time transaction between the consumer and the controller. The data is almost always transferred to several separate entities, and in the commercial context, there are almost always four types of parties to these transactions: (1) the consumer, (2) the controller, (3) the processer, and (4) subsequent processors. Each transaction carries over the obligations that the initial controller owed and triggers additional obligations specific to the type of transfer. Specific provisions related to personal data transfers will be addressed in subsequent sections.

C. Government Enforcement

The CPRA created a new state agency, the California Privacy Protection Agency ("Protection Agency") to regulate data privacy and is granted the responsibility from the Office of the Attorney General to investigate potential violations of the CCPA, either under a sworn complaint from a private individual or on its own volition.[40]

[39] *See CPRA,* Sec. 24 § 1798.199; *see also GDPR,* 2016/670, Chapter III.
[40] *CPRA,* Sec. 24 § 1798.199.10 (a).

Despite the GDPR being binding on all states, it is merely a framework with certain minimum requirements that member states are not permitted to stray from, which complicates the objective of uniform compliance across the EU.[41] Each member state is required to establish its own supervisory authority with one head of authority, commonly referred to as the Data Protection Authority ("DPA").[42] DPAs have investigatory powers and corrective powers.[43] Investigatory powers refer to conducting data protection audits, accessing all personal data necessary for the performance of its tasks, obtaining access to any premises of the data controller and processor, including equipment and means.[44] Corrective powers involve issuing warnings and reprimands, ordering compliance, compelling a company to report a data breach, and assisting individuals in exercising their affirmative rights under the Regulation.[45] Although enforcement is largely left to the states, the GDPR established the European Data Protection Board ("EDPB") which is tasked with ensuring a requisite level of compliance across all member states.[46] The EDPB is composed of the head of each member states' DPA and an additional officer called the European Data Protection Supervisor.[47] The EDPB exists to ensure consistent implementation of the GDPR and is entitled to carry out any investigation under its own initiative or on behalf of the European Commission.[48] The EDPB has very limited powers and only its only express authority is to investigate whenever it suspects an entity is committing violations and to issue guidance to the member states as well as the European Commission.[49]

---

[41] *See Generally Types of* Legislation, European Union, https://european-union.europa.eu/institutions-law-budget/law/types-legislation_en.
[42] *GDPR,* 2016/670, Art. (51).
[43] *GDPR,* 2016/670, Art. (68).
[44] *GDPR,* 2016/670, Art. (52).
[45] *GDPR,* 2016/670, Art. (51).
[46] *GDPR*, 2016/679 Art. (68).
[47] *GDPR*, 2016/679 Art. (51).
[48] *GDPR*, 2016/679 Art. (70).
[49] *Id.*

Under the CCPA, the Protective Agency can issue fines ranging from $2,500 to $7,500 per affected consumer depending on the type of violation.[50] In assessing fines, the Protective Agency considers whether the violation was intentional, what kind of information was involved, and whether the infraction involved the information of a minor.[51] As previously stated, EU member states retain the exclusive authority to adjudicate claims brought under the GDPR and to issue fines and penalties, but depending on certain violations, the member state may be required to levy fines up to the greater of two to four percent of global annual turnover or 10 to twenty-million Euros.[52] Since the GDPR was implemented, there has been a large gap of enforcement actions, including fines, and litigation across the member states.[53] Ireland has issued almost twice the amount of fines as any other country, issuing over 1.3 billion Euros as of May, 2023.[54] This is due in large part to the number of multinational corporation establishing their European branch there. In comparison, only three other countries have issued fines in excess of one-hundred million Euros.[55] The companies with the ten largest fines include, Meta, Amazon, WhatsApp and Google.[56]

D. Private Right of Action

Both the GDPR and the CCPA provide individuals with private causes of action to seek damages for misappropriation of their personal data.[57] The CCPA allows for individuals to bring

[50] *CCPA,* Sec. 24 § 1798.199.55(a)(2).
[51] *Id*.
[52] *GDPR,* 2016/670, Art. (83).
[53] Countries With Highest Fines Issued For General Data Protection as of May 2023, https://www.statista.com/statistics/1172445/countries-with-highest-fines-issued-gdpr/
[54] *Id.*
[55] *Id.*
[56] **Largest fines issued for General Data Protection Regulation (GDPR) violations as of May 2023** https://www.statista.com/statistics/1133337/largest-fines-issued-gdpr/
[57] *CCPA,* § 1798.150; *GDPR* 2016/670, Art. (79).

private causes of action against companies, but only for specific types of data breaches and only where the breach resulted in unauthorized access to one of the individuals' accounts.[58] The private right of action is much broader under the GDPR than the CCPA allowing, "any person who has suffered material or non-material damage" resulting from a business's violation to file an action.[59] In an initial proceeding brought by an individual the controller is always liable for some of the violations even if it was the processor at fault[60] However, after a judgment is issued and paid in the initial dispute, the controller and processor, or any other party involved in the litigation may initiate a proceeding against the other parties to recover damages from another, similar to joint and several liability under American tort law.[61] As a practical matter, however, litigation in the EU is less common because most member states require the loser to pay the winner's reasonable legal costs.[62]

The elements of a data breach under the CCPA require a plaintiff to show: (1) unauthorized access, and (2) exfiltration, theft, or disclosure, as a result of, (3) a failure to implement and maintain reasonable security procedures and practices to protect the personal information, that are, (4) appropriate to the nature of the information.[63] Damages resulting from a data breach are the lower amount of either the statutory damages or actual damages.[64] Statutory damages are anywhere from $100 to $750, per consumer, per incident.[65] Plaintiffs suing under the GDPR are required to file a complaint against the business either in their state of residence, or the state in which the business is established and the elements required to prove liability vary

[58] *CCPA,* § 1798.150.
[59] Allaire Monticollo, Chelsea Reckell, Emilio Cividanes, *California Privacy Landscape Changes Again with Approval of New Ballot Initiative*, Antitrust, Fall 2020, at 32.
[60] *GDPR,* 2016/670, Art. (82)(2).
[61] *GDPR,* 2016/670, Art. (82)(5).
[62] *GDPR,* 2016/670, Art. (79).
[63] *CCPA,* § 1798; 1789.150(a)(1).
[64] *Id.*
[65] *Id.*

from state to state.[66] The GDPR has strict notification requirements in the case of a data breach. The GDPR requires businesses to report a breach to their DPA within 72 hours of discovering it, unless it is unlikely to jeopardize the rights afforded to those whose data was affected by the breach.[67] In the event a business does report a breach to the DPA, they have a duty to notify the affected individuals of the nature, likely consequences, and measures being taken to mitigate the effects of the breach.[68]

III. COLLECTION AND PROCESSING

A. Initial Considerations for Collection and Consent

The GDPR requires a business to satisfy one of six legal bases in order to collect personal data: (1) vital interest of the individual, (2) public interest, (3) contractual necessity, (4) compliance with legal obligations, (5) unambiguous consent of the individual, and (6) legitimate interest of the data controller.[69] In April, 2023, however, corporations were dealt another obstacle to personal data collection following the European Data Privacy Board's ruling against Meta.[70] Facebook Ireland was contracting with users via the terms of service for purposes of behavioral advertising under the third legal basis.[71] The contract conditioned the use of their platform on the users' agreement to have their data tracked for behavioral advertising.[72] The Board found that, "Meta unlawfully processed user data and such processing was not necessary for the performance of an alleged contract."[73] The decision resulted in a 1.2 billion Euro fine against

[66] *GDPR,* 2016/670, Art. (79)(2).
[67] *GDPR*, 2016/679 Art. (33).
[68] *Id*.
[69] *GDPR*, 2016/679 Art. (6) (1).
[70] Case C-311/18, Maximillian Schrems v. Facebook Ireland, Ltd., ECLI:EU:C:2020:559.

[72] *Id.*
[73] *Id.*.

Meta and is the largest fine levied under the GDPR to date.[74] The ruling put corporations on notice that contractual necessity is no longer a legal basis for data collection as the use of personal data is not necessary for the execution of the terms of service.[75]

In the wake of this ruling, the only legal basis for companies to lawfully collect and process personal data is, effectively, consent. For consent to serve as a valid legal basis, it must: (1) be freely given; (2) it must be informed; (3) be given for a specific purpose; (4) be explicit and given via an affirmative act; (5) use clear and plain language and is clearly visible; and (6) be possible to withdraw consent.[76] After the Meta ruling, the European Commission clarified that consent is not freely given if the individual is not actually given a free choice, such as when a business requires an individual to consent to the processing of personal data as a condition to fulfill a contract or service.[77] The distinction between freely given consent and simply agreeing to the terms of service is that terms of service state that a company is collecting only the information that is necessary for the user to engage in the product or service.[78] Freely given consent, is when a user assents to the processing of their data for purposes outside of what is necessary to use a product or service and may be able to refuse consent without being disadvantaged.[79] Tracking user behavior for the purpose of behavioral advertising is not necessary for consumers to sign up and use the platform, so a business cannot simply circumvent the consent requirement by bundling it with their terms of service.[80]

---

[74] *Id.*
[75] *Id.*
[76] G*DPR*, 2016/679 Art. (7).
[77] *European* Commission, When is Consent Valid? https://commission.europa.eu/law/law-topic/data-protection/reform/rules-business-and-organisations/legal-grounds-processing-data/grounds-processing/when-consent-valid_en
[78] *Id*.
[79] *Id.*
[80] *Id.*

Although the CCPA does have certain consent requirements, it differs from the GDPR with respect to what type of consent is required and when it must be obtained.[81] Opt-in consent refers to an affirmative action one takes to provide their consent. Opt-out is a presumption of consent that requires an individual to withdraw consent. The GDPR requires opt-in consent as a lawful basis as previously stated, while the consent requirement under the CCPA is much weaker, operating under an opt-out rule with the exception that users must opt in to the use of personal data "for any purposes other than those 'necessary to perform the services…reasonably expected by an average consumer' or for otherwise specified business purposes."[82] Contrary to the GDPR, the CCPA permits processing to be made a term and condition if the processing is "reasonably necessary and proportionate" to achieve a business purpose.[83]

Both the EU and the CCPA allow companies to offer financial incentives in exchange for consumers' consent to process of their personal data.[84] The only restraint on businesses offering such an incentive is that users retain the right to withdraw consent without the product or service being downgraded.[85] Similarly, the CCPA, allows businesses to offer financial incentives in exchange for user consent, so long as they are not unjust, unreasonable, or discriminatory.[86] Business may charge a different price, or provide a different level of quality to the consumer, "if that difference is reasonably related to the value provided to the business by the consumer's data."[87] This is one alternative businesses can pursue if they deem the costs of offering financial

[81] Scott Jordan, *Strengths and Weaknesses of Notice and Consent Requirements Under the GDPR, the CCPA/CPRA, and the Fcc Broadband Privacy Order*, 40 Cardozo Arts & Ent. L.J. 113 (2022).
[82] Scott Jordan, *Strengths and Weaknesses of Notice and Consent Requirements Under the GDPR, the Ccpa/cpra, and the Fcc Broadband Privacy Order*, 40 Cardozo Arts & Ent. L.J. 113 (2022) *quoting CPRA*, § 1798.121(a)
[83] *CCPA* § 1798.100 (e).
[84] *See GDPR*, 2016/679 Art (4); *CCPA* § 1798.125(b)(3).
[85] *See GDPR*, 2016/679 Art (4).
[86] *CCPA*, § 1798.125(b)(4)
[87] *Id.*

incentives to be worthwhile, particularly under the GDPR due to the difficulties of obtaining a legal basis for collection.

The EU's proactive attitude toward data privacy is exemplified by the requirement of privacy by design and default.[88] Privacy by design compels companies to keep privacy in mind throughout the development of a given product.[89] Privacy by default, refers to minimum procedures that companies are expected to follow when collecting data, including: (i) only collecting personal information for a specified purpose; (ii) retaining the minimum amount of personal information necessary; and (iii) retaining such personal information only as long as necessary.[90] The CCPA, comparatively, does not mandate businesses to implement privacy by design or default, but requires companies to implement and maintain reasonable security procedures and practices to mitigate against the risk of data misappropriation.[91] Whether or not a company has adequate measures is especially relevant if a company is subject to a data breach as one of the elements requires a plaintiff to prove that the business was without adequate security procedures and measures.[92]

B. Data Transfers

Both the GDPR and the CCPA acknowledge that in order for businesses to participate in the global economy, there must be mechanisms to facilitate the transfer of data but with adequate safeguards to ensure that consumer rights are upheld by all parties involved.[93] One of the core principles common to each regulatory scheme is that consumer rights and protections transfer

[88] *GDPR*, 2016/679 Art. (25).
[89] *Id*.
[90] *GDPR*, 2016/679 Art. (25).
[91] *CCPA*. §1798.150.
[92] *CCPA,* § 1798; 1789.150(a)(1).
[93] *GDPR, 2016/679* Rec. 101

with the data. This amplifies the tension between consumer rights and corporate obligations, as an obvious issue arises when data leaves the jurisdictions protecting it. While both take measures to address this problem, the GDPR goes to great lengths in ensuring that any data transfer to a country or organization outside of the EU will maintain the same level of protection that the consumer was guaranteed upon the initial collection.

i. Transfers Under the GDPR

The GDPR does not place any additional restraints on transfers that occur between two companies within the EU.[94] Even transfers from one company in a one EU country to a different company in a different EU company will not be subjected to the additional obligations present in transfer outside the EU. Data transferred from a controller or processor in the EU to a country outside the EU is considered a third-country transfer, triggering Chapter V of the GDPR.[95] Chapter V, which governs personal data transfers between EU and non-EU states applies if: (1) the controller is subject to the GDPR with respect to the processing in question; (2) the controller made the personal data available to a third-party; and (3) the third-party is located outside the EU.[96] The controller that originally collected the data is responsible for making sure that any transfer to third-party processor is done in accordance with the same laws governing the initial collection.[97] Chapter V also applies where a third-party transferee subsequently transfers data to another transferee for processing outside of the EU.[98] While these types of transfers do not place the third-parties within the GDPR's jurisdiction, they are still subject to the same obligations the

[94] *Id.*
[95] *See GDPR*, 2016/679 Art (44).
[96] *GDPR*, 2016/679 Art. (44).
[97] *Id.*
[98] *Id.*

original controller is subject to.[99] Further, the controller's obligations are not extinguished once the data leaves their hands as they are still liable for any of the third parties' mishandling of the data.[100]

The GDPR approves the transfer of data to non-EU states in two ways, an adequacy decision or specific authorization from the supervisory authority.[101] An adequacy decision involves the European Commission conducting an assessment of the recipient country's ability to adequately protect the data in question.[102] Countries who have been issued an adequacy decision are considered to be substantially in compliance with the GDPR and permits businesses of that country to send and receive data between the EU.[103] However, there have only been fourteen such decisions since the GDPR was enacted, so many businesses are forced to seek alternative legal channels to transfer data to countries who have not been deemed to have adequate safety measures.[104] In the absence of an adequacy decision, a business may transfer personal data outside the EU if they can show some appropriate safeguard has been implemented in advance of the transfer.[105] This is most commonly done through the use of standard contractual clauses or binding corporate rules.[106]

Standard Contractual Clauses

Standard contractual clauses are pre-approved model data protection clauses that allow data transfer between an EU controller or processor and a processor in a third-country to do so

[99] *See GDPR*, 2016/679 Art (46).
[100] *GDPR,* 2016/679 Recital 101.
[101] *GDPR, 2016/679* Art. (44).
[102] *GDPR*, 2016/679 Art. (45).
[103] *Id*.
[104] *Adequacy Decisions, How the EU Determines if a non-EU Country Has an Adequate Level of Data* Protection, European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.
[105] *GDPR*, 2016/679 Art. (46).
[106] *Id*.

while maintaining compliance with the GDPR.[107] In 2019, 88% of business reported that standard contractual clauses were their preferred method for extra-territorial data transfers.[108] There are three formalities of a standard contractual clause: (1) a data transfer agreement providing the terms and conditions; (2) the contents must comply with the mandatory conditions set forth by the EU commission; and (3) a transfer impact assessment which is a system to be established by the exporter documenting what data was transferred, to what countries, and to what entity.[109]

Standard contractual clauses can be used indefinitely so long as the terms and conditions of the transfer remain the same.[110] It is a useful mechanism for recurring transfers, but a significant drawback is they cannot be amended to account for changes in terms or conditions. If a change occurs, the entire document must be discarded and re-executed with the same formalities.[111] The EU Commission employs what is considered a "modular approach" that contemplates whether the transfer is controller-to-controller, controller-to-processor, processor-to-processor and processor-to-controller.[112] The type of module a transfer falls under dictates which obligations extend to which party.[113] The controller is always liable for violations related to the transfer, but when the transfer falls under the fourth module, processor-to-controller, the parties become jointly liable.[114] This mechanism of facilitating transfers is particularly attractive to businesses as it removes the barrier of needing to draft and receive approval every time a

[107] *New Standard Contractual Clauses – Questions and Answers* Overview, European Commission, https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/new-standard-contractual-clauses-questions-and-answers-overview_en.
[108] *IAPP-EY Annual Privacy Governance Report 2022 – Executive* Summary, IAPP, https://iapp.org/resources/article/privacy-governance-report/.
[109] *GDPR,* 2016/679 Recital 109.
[110] *GDPR*, 2016/679 Art (46).
[111] *GDPR*, 2016/679 Recital 109.
[112] *GDPR*, 2016/679 Art (46).
[113] *Id.*
[114] *GDPR*, 2016/679 Art (83).

corporate contract is executed.[115] It also provides for ability to bind all additional, subsequent transferees to one agreement instead of requiring the controller to submit a standard contractual clause for each processor involved.[116]

The use of standard contractual clauses as a method of approving transfers outside of Europe was weakened considerably following the decision in *Data Protection Commissioner v. Facebook Ireland Ltd*. ("*Schrems II"*).[117] Max Schrems is an Austrian privacy advocate who sued Facebook Ireland in light of the Edward Snowden document leak which revealed that American intelligence agencies were working with private companies to access user data for purposes of government surveillance.[118] Schrems argued that the potential for data originating in the EU to be used for such purposes was incompatible with the purpose of the GDPR.[119] The case reached the Court of European Justice which upheld the validity of standard contractual clauses for purposes of data transfers, but not without a significant caveat.[120] The judgment added a requirement that DPAs must suspend data transfers made pursuant to a standard contractual clause where the transfer does not take place under an "essentially equivalent" standard as the GDPR.[121] The court further indicated that standard contractual clauses may necessitate supplemental protections, and they may not be approved if there is any doubt that the rights of the consumers will not be upheld by the third party recipient.[122] In practice, this means that DPAs across member states must ensure that when personal data is transferred to a third-country, measures such as anonymization or pseudonymization must be taken prior to the actual transfer to make it impossible for the data

[115] *Id*.
[116] *Id.*
[117] *Data Protection Commissioner v. Facebook Ireland Ltd*. ("*Schrems II"*).
[118] *Id*.
[119] *Id*.
[120] *Id*.
[121] *Id*.
[122] *GDPR*, 2016/679 Recital 108.

to be misappropriated.[123] Additionally, because standard contractual clauses are agreements solely between the business that collected the data and the third-party recipient, individuals have not assented to the transfer of their data, so they must be notified when their data is transferred pursuant to a standard contractual clause.[124]

Binding Corporate Rules

The second alternative for businesses to effectuate data transfers outside the EU is through the use of binding corporate rules.[125] While similar to standard contractual contracts, binding corporate rules are only available to companies for intercompany data transfers to offices outside of the EU.[126] A business must submit the binding corporate rules with their DPA for approval and once approved, the business no longer has to execute contracts on a case-by-case basis.[127] Businesses seeking approval for binding corporate rules do have to meet fourteen distinct requirements which set forth the rights of individuals and purposes of the transfer.[128] Although they are expensive and time-consuming to draft, binding corporate rules are advantageous for larger, multinational companies, and may be preferred over standard contractual clauses due to the ease of implementation once approved, and the ability to tailor the agreements to specific industry standards, and in light of the *Schrems* ruling, do not require

[123] Andraya Flor, *The Impact of Schrems II: Next Steps for U.S. Data Privacy Law*, 96 Notre Dame L. Rev. 2035, 2050 (2021).
[124] European Data Protection Board, Frequently Asked Questions on The Judgement of The Court of Justice Of The European Union In Case C-311/18 - Data Protection Commissioner V Facebook Ireland Ltd And Maximillian Schrems 3 (July 23, 2020).
[125] *GDPR*, 2016/679 Art. (46)
[126] *GDPR*, 2016/679 Art. (47).
[127] *Id*.
[128] *Id*.

supplemental protections.[129] Businesses who do not have a presence in the EU are not able to use this transfer mechanism, and must still rely on standard contractual clauses.[130]

ii. Transfers Under the CCPA

The CCPA, unlike the GDPR, differentiates between two types of transfers, sales and sharing. Sale refers to the conventional sale transaction while sharing refers to transferring personal data for purpose of behavioral advertising, regardless of whether it is in exchange for money. [131] Most notably, however, is that the CCPA does not place additional requirements on businesses transferring personal data outside the borders of California, or the United States. The same provisions governing the initial collection still apply and a company is free to transfer the personal data, unless the individual exercises their right to opt out. [132]

In the context of transfers, the CCPA disregards the controller-processor distinction and instead, creates three categories of entities: businesses, service providers, and third parties. Businesses are the entities that collect information while service providers and third parties are the entities to which businesses transfer data to. Any transfer from a business to a third party triggers the right to opt-out.[133] Transfers to service providers, by contrast, do not trigger the opt-out requirement because the definition of "service provider" precludes entities which retain personal information for any purpose other than the specified business purpose.[134] The

---

[129] *Binding Corporate Rules* – GDPR, PWC, https://www.pwc.com/ml/en/publications/documents/pwc-binding-corporate-rules-gdpr.pdf (Feb. 18, 2021).
[130] Donna Calia, *Schrems II: The Eu's Influence on U.S. Data Protection and Privacy Laws*, 21 Wash. U. Global Stud. L. Rev. 247 (2022).
[131] *CCPA* Sec. 14 §1798.140 (ad).
[132] Allaire Monticollo, Chelsea Reckell, Emilio Cividanes, *California Privacy Landscape Changes Again with Approval of New Ballot Initiative*, Antitrust, Fall 2020, at 32.
[133] *CCPA* Sec. 14 §1798.120.
[134] *CCPA* Sec. 14 §1798.140.

distinction essentially comes from the fact that a business purpose includes transferring data to a service provider, but a third party does not have the same discretion to use the data, as they are limited to only the uses specified in the contract made at the outset of collection.[135] When the business initially collected the personal data, the consumer would have been notified that their information was collected and the purpose thereof, including whether that purpose included transfer to a service provider.[136] The regulation defines many of the terms by what they are not, and the definition of "sale" being one such example.[137] The definition expressly precludes transfers to a service provider, so when a consumer is notified of collection and the stated purpose does not include transfer to a service provider, and the business later decides to sell the data to a third party, the business must notify the consumer that they wish to use the data for a purpose that was not stated at the outset.[138] It is when the consumer receives this notification that the business must allow the consumer to opt-out.[139]

Regardless of whether a business sells or transfers personal information to another entity, the CCPA mandates a contract between the parties, providing guarantees that the recipient will offer the same levels of protection that the business was obligated by.[140] The concept is similar to the contractual mechanisms provided by the GDPR in that the main purpose of the contract is to ensure that consumer rights flow with the data. Unlike standard contractual clauses or binding corporate rules, the contract requirements here are more streamlined than those under the GDPR, with only five requirements. The contracts must: (1) specify the purposes of the agreement; (2) obligate the recipients to provide with the same privacy protections that the CCPA requires; (3)

---

[135] https://iapp.org/news/a/analyzing-the-cpras-new-contractual-requirements-for-transfers-of-personal-information/
[136] *CCPA* Sec. 14 §1798.115(a).
[137] *CCPA* §1798.120.
[138] *CCPA* §1798.135(a).
[139] *Id.*
[140] *CCPA* Sec. 14 §1798.100.

grant the business the ability to ensure the recipient is able to maintain those protections; (4) require the recipient to notify the business if they can no longer meet their obligations; and (5) allow the business to take reasonable and appropriate steps to remediate uses of information outside the business purpose.[141] Additionally, the CCPA contains a notification requirement to inform consumers any time their personal data is going to be transferred or sold.[142] At or before the time of collection, business must provide: (1) the categories of personal information being collected; (2) the purpose of the collection and how it may be processed; (3) Whether or not they intend to share the information with service providers or sell it to third parties; and (4) how long they intend to retain each category of personal information and the criteria for determining the retention period.[143] In contrast to the GDPR, the CCPA allows organizations to use banners on the website as a method of notification of transfers, so long as the banners contain op-out links.[144] The banners must include the same information as the aforementioned notification requirements.[145] The GDPR and CCPA vary greatly when it comes to cross-border trasnfers as the latter provides for a much more efficient transfer process than the GDPR and does not place any additional duties related to international transfers.

IV. CONCLUSION

Under the GDPR and CCPA Consumers wield significantly more power which confers several duties unto businesses to ensure those rights are being provided for. While the two

[141] *CCPA* Sec. 14 §1798.115(a).
[142] *CCPA* §1798.185(a).
[143] *CCPA* §1798.100(a)
[144] *CCPA* §1798.185(a)(20)(C).
[145] *CCPA* §1798.100(a)

regulatory regimes are arguably the most restrictive laws to date, they may be an indication of regulations to come in other jurisdictions. Due to the novelty of these two laws and the sparsity of case law, the litigation in the coming years will be indicative of how courts interpret the regulations and just how effective they are at striking a balance between consumer rights and protections over their data versus maintaining the free flow of data for commercial purposes. However, it is clear that businesses will have to allocate more resources toward data privacy if they seek to maintain a presence in either jurisdiction or any other that chooses to implement such comprehensive data privacy laws.