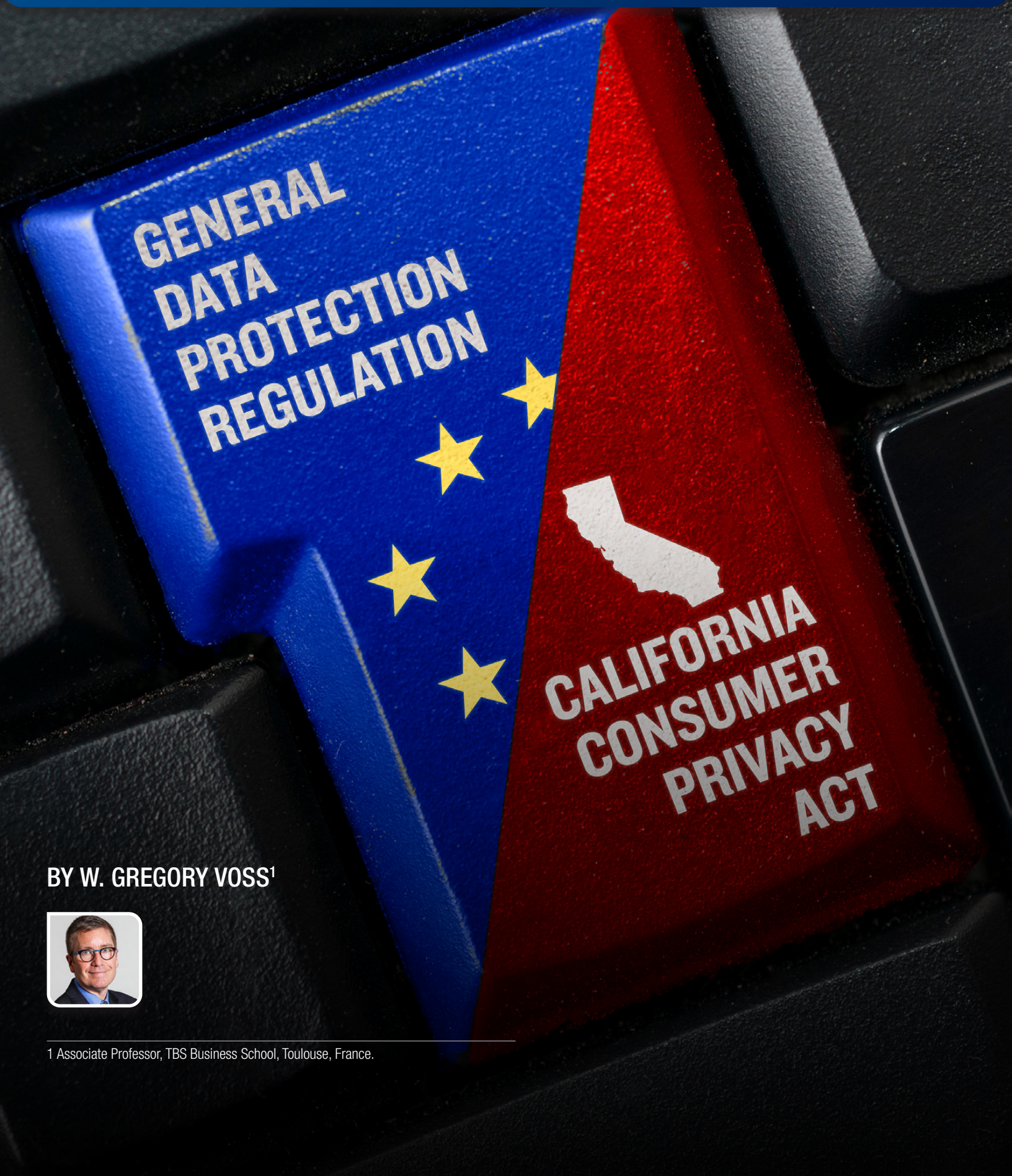
THE CCPA AND THE GDPR ARE NOT THE SAME: WHY YOU SHOULD UNDERSTAND BOTH



BY W. GREGORY VOSS[1]

1 Associate Professor, TBS Business School, Toulouse, France.

CPI ANTITRUST CHRONICLE
JANUARY 2021

I. INTRODUCTION

Within less than two years, on both sides of the Atlantic important data privacy laws became applicable — on the one side, the General Data Protection Regulation ("GDPR") in the European Union and the other countries of the European Economic Area in 2018,[2] and on the other side the California Consumer Privacy Act ("CCPA") as amended, in the United States in 2020.[3] These two data privacy laws have rightly attracted attention outside the borders of their home jurisdictions, due in part to the importance of the markets they cover, and in part to their extraterritorial effect, covering businesses not incorporated in their respective jurisdictions. CCPA is not a "GDPR clone,"[4] as its provisions are not as extensive as those of the GDPR.

Indeed, while there are similarities between the two statutes, there are also differences, with consequences for firms' compliance efforts. For starters, the GDPR is a regulation that is an evolution of an already existing EU directive, and was developed over a period of years, with public consultations followed by the proposal of a draft and over four years of legislative study, lobbying, amendments, votes, and three-way dialogue (trialogue) among the European Commission, the European Parliament and the Council of the European Union, whereas the California statute was hastily adopted and is much shorter than its European cousin. Furthermore, the GDPR requires a legal or legitimate basis prior to the processing of personal data, whereas the CCPA does not, yet both provide for extraterritorial scope which will catch the activities of many corporations. Thus, you should understand both. This article starts with a short study of the extraterritorial scope of the two pieces of legislation.

2 Regulation (EU) 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 personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation [hereinafter, GDPR].

3 Cal. Civ. Code §1798.100 *et seq.* (effective Jan. 1, 2020).

4 Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61(5) Boston College Law Review, at 1687, 1711,

II. EXTRATERRITORIAL SCOPE ON BOTH SIDES OF THE ATLANTIC

Both the CCPA and the GDPR may apply to corporations incorporated outside of, respectively, California and the European Economic Area. Take the case of the CCPA first.

First, to see which entities are covered by the CCPA, the definition of a "business" must be looked to. Broadly, the definition of business is neutral as to the legal form the entity takes, encompassing everything from a sole proprietorship, partnership, corporation, or other for-profit legal entity, which "collects consumers' personal information or on the behalf of which that 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,"[5] and that satisfies at least one of the thresholds identified in the CCPA. The concept of doing business is not defined in the CCPA, but reference to tax and corporate law in California indicates that a broad interpretation of the term should be assumed.[6] For example, in California's Revenue and Taxation Code the term is defined as "actively engaging in any transaction for the purpose of financial or pecuniary gain or profit."[7] Thus, a legal entity does not need to be a California corporation or other California legal entity in order fall under the CCPA, nor does it need to have a physical presence in California in order to fall under the CCPA, as engaging in Internet transactions with California residents should suffice, if one or more of the thresholds are met.[8]

The thresholds, at least one of which must be met for the CCPA to apply, are the following:

(A) Has annual gross revenue 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's 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.[9]

In addition, the definition of "business" extends to include any entity controlling or controlled by a business, as defined with regard to the thresholds above, and that shares a name, servicemark, or trademark with the business.[10]

Next, the GDPR likewise reaches beyond the borders of the European Union (and those of European Economic Area, including the EU member states and Iceland, Norway, and Lichtenstein, which have likewise adopted the GDPR[11]). The GDPR territorial scope is defined in the following terms in its Article 3:

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 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

5 Cal. Civ. Code §1798.140 (c)(1).

6 Rita Heimes, *Top 5 Operational Impacts of the CCPA: Part 1 — Determining if you're a business collecting or selling consumers' personal information*, iapp The Privacy Advisor, July 23, 2018, https://iapp.org/news/a/top-five-operational-impacts-of-cacpa-part-1-determining-if-youre-a-business-collecting-or-selling-consumers-personal-information/.

7 Cal. Rev. & Tax. Code § 23101(a).

8 Erin Illman & Paul Temple, *California Consumer Privacy Act: What Companies Need to Know*, 75 Business Lawyer, Winter 2019-2020, at 1637, 1640.

9 Cal. Civ. Code § 1798.140(c)(1).

10 Cal. Civ. Code § 1798.140(c)(2).

11 *General Data Protection Regulation (GDPR) entered into force in the EEA*, EFTA, July 19, 2018, https://www.efta.int/EEA/news/General-Data-Protection-Regulation-GDPR-entered-force-EEA-509576.

(b) the monitoring of their behavior as far as their behavior 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.[12]

In cases where GDPR Article 3(2) applies, a controller or processor must appoint a representative in the European Union in writing,[13] except if the processing is occasional and does not include either sensitive data or data relating to criminal convictions and offenses and "is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing."[14]

III. CERTAIN MAJOR DIFFERENCES BETWEEN THE CCPA AND GDPR

This section will highlight certain major differences between the CCPA and GDPR, without being exhaustive.

First of all, the CCPA, unlike the GDPR, is not a true omnibus data privacy law. As an illustration, it specifically excludes areas where specified federal legislation exists, for example: certain protected health information ("HIPAA"),[15] certain consumer report data ("FCRA"),[16] and certain financial information ("GLBA").[17] Furthermore, the CCPA covers businesses, as defined using the thresholds indicated above, but not those under such thresholds. While the GDPR takes into account the size of an undertaking for the purposes of the record-keeping requirement for the personal data processing requirement, excluding certain SMEs of fewer than 250 employees,[18] and thus uses what might be described as a risk-based approach, even SMEs that are not subject to the record-keeping requirement are still subject to other provisions of the GDPR.

The CCPA also refers to consumers, making one think it is meant to be a consumer protection act. However, its broad definition of "consumer"[19] means that it ends up being something more. The term "consumer" limits CCPA protection to California residents, while the GDPR applies to persons in the EEA, with no residency or citizenship requirement. In addition, the CCPA only covers for-profit entities, whereas the GDPR also covers non-profits.

Both the GDPR and the CCPA have broad definitions of, respectively, personal data and personal information. While the GDPR does not exclude from its coverage personal data that are publicly available, the CCPA does, providing as follows: ""Personal information" does not include publicly available information. For purposes of this paragraph, "publicly available" means information that is lawfully made available from federal, state, or local government records. "Publicly available" does not mean biometric information collected by a business about a consumer without the consumer's knowledge."[20] Furthermore, while the term that triggers the application of the GDPR, "processing" of personal data, is extremely broad,[21] in the CCPA, one key term used in the definition of business, "sell," "selling," "sale," or "sold," has several carveouts.[22]

The GDPR defines certain personal data as "special categories of data" (sensitive data), meriting protection to a higher standard. These include certain categories of data that might, if disclosed, lead to discrimination, and which may not be treated as sensitive data in the United

12 GDPR, art. 3. Note that the term "Union" refers to the "European Union."

13 GDPR, art. 27(1).

14 GDPR, art. 27(2)(a).

15 Cal. Civ. Code § 1798.145(c)(1)(B).

16 Cal. Civ. Code § 1798.145(d)(1)-(2).

17 Cal. Civ. Code § 1798.145(e).

18 This is subject to the conditions that the relevant personal data processing is not "likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10." GDPR, art. 30(5).

19 "Consumer" is defined 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." Cal. Civ. Code § 1798.140(g).

20 Cal. Civ. Code § 1798.140(o)(2).

21 GDPR, art. 4(2).

22 Cal. Civ. Code § 1798.140(t)(1).

States (such as racial origin). These include "personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation."[23] No such categories exist in the CCPA.

In the GDPR, processors, who act under the instructions of controllers pursuant to a contract, and that are similar to "service providers" in the CCPA, are subject to various obligations, whereas under the CCPA service providers have fewer "direct and detailed obligations."[24] It should be noted that the GDPR provides and requires a whole set of compliance tools, in addition to the processing record-keeping requirement mentioned above, such as the appointment of a data protection officer by many corporations, and the use of data protection impact assessments in many cases, especially for processing of sensitive data or profiling.[25] This forms part of the GDPR's accountability focus, but no such requirements exist in the CCPA.

Next, certain provisions of the GDPR are inimitable in the United States because of differences in the legal culture of the two systems, especially at the constitutional level, notably with the fundamental rights basis for data protection in Europe and the importance of the First Amendment in the United States. This I have described as one of the obstacles to true data privacy law harmonization between the United States and the European Union.[26] One area where this difference may be manifested is that between the opt-in model of the GDPR and the opt-out model of the CCPA, as well as their different takes on the right to erasure (right to be forgotten) in the GDPR and the right to deletion in the CCPA. As one commentator remarked: "Although both jurisdictions have taken steps to increase individual control over personal data disseminated on the Internet, the GDPR's principle-based approach to data privacy establishes a more stringent regulatory environment than the CCPA."[27]

Moreover, another major difference between the CCPA and the GDPR is that the former contains no cross-border data transfer restriction whereas the latter does. Indeed, the GDPR requires that, without an adequacy decision or appropriate safeguards, personal data may not be exported from the European Economic Area to a non-EEA country (including onward transfers).[28] As the United States has not benefitted from an adequacy decision, many American corporations relied on the Privacy Shield framework adequacy decision for cross-border data transfers to the United States up until it was invalidated by the July 2020 *Schrems II* decision of the Court of Justice of the European Union.[29]

Finally, one difference that has existed between the GDPR and the CCPA is set to be gummed by California Proposition 24, voted on November 3, 2020, and referred to as the California Privacy Rights Act (CPRA), which would expand consumer privacy rights and business obligations.[30] Importantly, the GDPR requires member states to provide for "one or more independent public authorities to be responsible for monitoring the application" of the GDPR, known as a supervisory authority[31] (or, more commonly, a data protection authority, or DPA). The notion of independence is important for this regulator to ensure fundamental rights, although this contrasts with the situation in the United States, where there is "no *de jure* independent data privacy authority, in the same sense as the European Union. The *de facto* data privacy authority — the Federal Trade Commission ("FTC") — suffers from many handicaps in its action,"[32] such as limited jurisdiction and the fact that it cannot "engage

23 GDPR, art. 9(1).

24 DataGuidance & Future of Privacy Forum, Comparing privacy laws: GDPR v. CCPA, at 17, December 2019, https://www.dataguidance.com/sites/default/files/ccpa_v_gdpr_latest_edition.pdf.

25 W. Gregory Voss, *Internal Compliance Mechanisms for Firms in the EU General Data Protection Regulation*, 5053) Revue Juridique Thémis de l'Université de Montréal (RJTUM), 2016, at 783, 803-814.

26 W. Gregory Voss, *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, 2019 University of Illinois Journal of Law, Technology & Policy, Fall 2019, at 405, 431-452.

27 Grace Park, *The Changing Wind of Data Privacy Law: A Comparative Study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act*, 10(4) UC Irvine Law Review, at 1455, 1485-1486, June 2020.

28 GDPR, arts. 44-50.

29 W. Gregory Voss, *Airline Commercial Use of EU Personal Data in the Context of the GDPR*, British Airways *and* Schrems II, forthcoming in 19(2) Colorado Technology Law Journal, 2021 (draft available at https://ssrn.com/abstract=3702223).

30 Stacy Gray et al., *California's Prop 24, the "California Privacy Rights Act," Passed. What's Next?*, Future of Privacy Forum, November 4, 2020, https://fpf.org/2020/11/04/californias-prop-24-the-california-privacy-rights-act-passed-whats-next/.

31 GDPR, art. 51(1).

32 *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, *supra* note 24, at 424 (citations omitted).

in broad rulemaking for privacy."[33] Under the CCPA (before the CPRA), the California Attorney General plays the regulatory role.[34] However, once the CPRA becomes operative, which is scheduled to be in 2023, a freshly-created California Privacy Protection Agency will take over from the California Attorney General, provided a dedicated agency considered a "major milestone for privacy in the US," and potentially providing impetus for the adoption of a U.S. Federal privacy law.[35]

IV. RESULTING COMPLIANCE ISSUES

While the CCPA and the GDPR will both apply to many corporations, due to their extraterritorial scope, they are not exactly the same. As the International Association of Privacy Professionals (IAPP) President J. Trevor Hughes said, "The fact is CCPA is not GDPR, and it is different. There certainly are things that you probably built for GDPR that will be helpful, but CCPA deserves its own attention."[36] While determining the "highest bar" in the area of regulation may be helpful, you still need to determine the differences among the various relevant pieces of legislation, according to LinkedIn's senior director and head of global privacy, Kalinda Raina.[37] For example, there may be strategic value to treating customers according to the level of that highest bar, such as Microsoft's proclamation that it would provide GDPR-like rights to its customers worldwide.[38] Such a treatment may result in efficiency and savings.

However, certain specific requirements of laws must be accounted for in the analysis, such as CCPA's "nuanced requirements that go beyond the GDPR," including the requirement of a "Do Not Sell My Personal Information" link.[39] Compliance with both pieces of legislation, if applicable, must be ensured. This requires understanding their provisions and monitoring legal developments, such as the issuance of advisory opinions, supervisory authority actions, and court cases, with respect to the GDPR; and the issuance of regulations, legislative developments, regulator actions, and court interpretations, in the case of the CCPA. Specifically, a co-author and I have warned against modeling compliance risk based on past sanctions in the context of the GDPR, as it is likely fines will increase, thus rendering the results of the modeling incorrect.[40]

Yet, it is true that having various legal standards applicable in the domain of data privacy runs counter to what might be logical in a globalized world economy, especially in the area of internet communications. Harmonization, instead, would have many advantages for international operators.[41] Good data governance practices may help ensure compliance in various jurisdictions,[42] such as California and the European Economic Area, for example in ensuring their respective rights to deletion and right to erasure (right to be forgotten), however, I repeat, divergences in the legislation must be dealt with and compliance ensured.

33 *Id.* (citation omitted).

34 Cal. Civ. Code § 1798.185(a)-(c).

35 *California's Prop 24, the "California Privacy Rights Act," Passed*, *supra* note 28.

36 Bradley Barth, *Meeting GDPR standards doesn't guarantee Calif. Privacy law compliance, experts warn*, SC Media, March 8, 2019, https://www.scmagazine.com/home/security-news/meeting-gdpr-standards-doesnt-guarantee-calif-privacy-law-compliance-experts-warn/.

37 Id. ("The challenge for anyone working in this space is to figure out what that 'highest bar' is and how you will comply with it and then to figure out those differences… and how are you going to operationalize that on a global scale.").

38 W. Gregory Voss & Kimberly A. Houser, *Personal Data and the GDPR: Providing a Competitive Advantage for U.S. Companies*, 56(2) American Business Law Journal, at 287, 334-337, Summer 2019.

39 Caitlin Fennessy, *IAPP FAQs: Are GDPR-Compliant companies prepared for the CCPA?*, iapp, April 17, 2019, https://iapp.org/news/a/are-gdpr-compliant-companies-prepared-for-ccpa/.

40 W. Gregory Voss & Hugues Bouthinon-Dumas, EU General Data Protection Sanctions in Theory and in Practice, forthcoming in 37(1) Santa Clara High Technology Law Journal, 2021 (draft available at https://ssrn.com/abstract=3695473).

41 *Obstacles to Transatlantic Harmonization of Data Privacy Law in Context*, *supra* note 24, at 407-409.

42 W. Gregory Voss, *Cross-Border Data Flows, the GDPR, and Data Governance*, 29(3) Washington International Law Journal, at 485, 527, June 2020.

V. CONCLUSION

The GDPR and the CCPA are milestone pieces of data privacy legislation in their respective jurisdictions. While the EU regulation has been referred to as the "gold standard" and as having had influence on the CCPA and other U.S. state data privacy bills, the CCPA has influence, too, because of the size of its market and its being the home of Silicon Valley. Both are also influential by virtue of their extraterritorial effect.

While there are similarities between the legislation, there are notable differences as well. These differences manifest themselves in many ways, based in part on differences of the legal culture in their home jurisdictions. One area that has been in the news regarding the GDPR is its cross-border data transfer restrictions, which certain commentators have referred to as a "soft" data localization requirement, and which is not present in the CCPA. Also, certain differences are due to the Federal system in the United States, where areas where there is sectoral legislation in the United States, which must be carved out of the California legislation. Moreover, looming on the horizon is the threat of U.S. federal data privacy legislation, which would pre-empt the CCPA.

Nonetheless, corporations dealing internationally will likely be subject to both the GDPR and the CCPA, and this means learning about both, developing compliance strategies with respect to each, monitoring legal developments, and ensuring respect of the law.

CPI COMPETITION POLICY INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.