Antitrust Chronicle

JANUARY · WINTER 2021 · VOLUME 1(1)

Privacy Matters: GDPR & CCPA

CPI COMPETITION POLICY INTERNATIONAL

TABLE OF CONTENTS

LETTER FROM THE EDITOR

Dear Readers,

Data protection has emerged as one of the key issues of the 21st Century. Two key pieces of legislation: the EU General Data Protection Regulation ("GDPR"), and the California Consumer Privacy Act ("CCPA") are the keystones in the legislative response to the concerns raised by Big Data, in the so-called digital economy.

Of the two, the GDPR, put into full effect in mid-2018, represented the first blow on behalf of consumer privacy. It was intended to protect EU citizens, but its impact has already been worldwide. The GDPR by its very nature raises very distinct competition law concerns due to its far-reaching effects on issues such as data portability, and its particular effects on industries such as ad technology, investment incentives in technology markets, and myriad other issues.

The timely articles in this edition address these very topical issues, while at the same time drawing out contrasts between the GDPR and the CCPA, as sister pieces of legislation, and their differential effects on competition.

As always, thank you to our great panel of authors.

Sincerely,

CPI Team

SUMMARIES

The CCPA and the GDPR Are Not the Same: Why You Should Understand Both

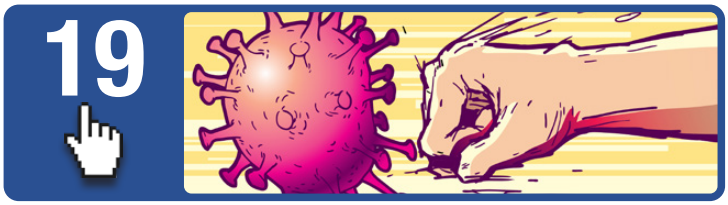
By W. Gregory Voss

The EU General Data Protection Regulation ("GDPR") and the California Consumer Privacy Act ("CCPA") are milestone pieces of legislation, in major markets, one on each side of the Atlantic. While the CCPA has not had the international impact that the GDPR has and is considered to have been influenced by the latter, it is no "GDPR clone." The result is that corporations must understand both pieces of legislation and their differences, in order to formulate compliance strategies going forward. In the context of events such as the passage of the California's Proposition 24, the monitoring of legal developments is likewise of great importance. This study helps in highlighting the extraterritorial effect of both, and certain major differences between the two, as well as noting a couple of important changes to come through Proposition 24.

Data Privacy in Adtech: Boon or Bust?

By Cynthia J. Cole & Nicholas Palmieri

AdTech has ridden the wave of data consumption and movement to exponential revenue growth. At the same time, in 2021, consumer privacy has reached a height of new regulation and on the cusp of varied and more pointed enforcement practices, may or may not impede AdTech's rise. California increasingly seeks to join Europe in its passage of consumer privacy laws and the latest, the California Privacy Rights Act ("CPRA") may show an intent toward altering the AdTech status quo. In this article we will explore what the General Data Protection Regulation ("GDPR"), the California Consumer Privacy Act ("CCPA") and the newly passed CPRA, together, may mean for AdTech and advertising on the internet in general.



The Pandemic, Edtech, and the Tricky Subject of Service Providers and Processors

By Cody Venzke

The European Union's General Data Protection Regulation and the California Consumer Protection Act seem like ideal legislation to address privacy concerns that have arisen as a result of the increased use of education technology during the global coronavirus pandemic. Those laws' application to edtech, however, requires untangling. This paper examines how both laws' geographic reach, substantive scope, and treatment of principals and agents in the data lifecycle apply to edtech vendors. Because the two laws have similar approaches that differ in critical respects, edtech vendors must be cognizant of how the laws address their status as contractors with non-profit or public schools and when they are processing data on behalf of their school partners – and when they are processing it for their own purposes.

CCPA and Competition: The Value of Consumer Data, Privacy, and Pricing

By Jeewon Serrato & Lawrence Wu

Much like how there was debate in the past on whether the goals of antitrust and intellectual property law were incompatible or complimentary, we should anticipate many debates on how the goals of privacy law may affect the way firms compete, particularly when consumers are given a choice of opting in or opting out of providing companies with their personal information and when those choices may be affected by the prices charged and the services offered by those companies. With the passage of the California Consumer Privacy Act ("CCPA"), which went into effect on January 1, 2020, this issue is now front and center. This article provides an overview of the impact the CCPA will have on how businesses calculate the value of consumer data, how consumer choices may affect pricing, and the intersection of privacy law principles and competition.

SUMMARIES

Consumer Choice and Consent in Data Protection

By Pranvera Këllezi

The mechanism of the GDPR limited legal grounds for the collection and processing of personal data, and the narrow and very restrictive interpretation of the same legal grounds runs the risk of limiting consumer choice, instead of reinforcing self-determination. This leads to removing the choice for consumers to pay with their data. The superimposition of competition law with the proposal to introduce dominance into the GDPR analysis is liable to exacerbate this effect by further limiting consumer choice. The GDPR example highlights the risk of introducing general and comprehensive privacy laws for consumer choice: while it reinforces consumer control on their data in general, it puts constraints on self-determination by reducing its choice in terms of features, products or ability to use its personal data to obtain more services.

Data Regulation and Technology Venture Investment: What Do We Learn From GDPR?

By Jian Jia, Ginger Zhe Jin & Liad Wagman

The European Union's General Data Protection Regulation, which governs how businesses manage, process, and handle their European users' data, came into effect in May 2018. Using venture investment data, we examine how the regulation may have affected investors' appetites to invest in European technology ventures, as a function of the investors' locations. Our findings indicate a reduction in the number of investment deals in nascent European technology ventures following the implementation of the legislation, including reductions in repeat investments, and particularly by foreign investors, in comparison to technology ventures in the United States.

WHAT'S NEXT?

For February 2021, we will feature Chronicles focused on issues related to (1) **Gatekeepers**; and (2) **The Music Industry**.

ANNOUNCEMENTS

CPI wants to hear from our subscribers. In 2021, we will be reaching out to members of our community for your feedback and ideas. Let us know what you want (or don't want) to see, at: antitrustchronicle@competitionpolicyinternational.com.

CPI ANTITRUST CHRONICLES MARCH 2021

For March 2021, we will feature Chronicles focused on issues related to (1) **China Edition**; and (2) **2021 Horizons**.

Contributions to the Antitrust Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI Antitrust Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (ssadden@competitionpolicyinternational.com) with the subject line "Antitrust Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers on any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

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.

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.

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]

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,

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).

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
> >
> > (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.

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.

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).

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 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

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).

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.

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 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]

---

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).

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).

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.

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.

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.

DATA PRIVACY IN ADTECH: BOON OR BUST?

BY CYNTHIA J. COLE & NICHOLAS PALMIERI[1]

1 Baker Botts L.L.P.

I. INTRODUCTION

AdTech has ridden the wave of data consumption and movement to exponential revenue growth. At the same time, in 2021, consumer privacy has reached a height of new regulation and, on the cusp of varied and more pointed enforcement practices, may or may not impede AdTech's rise. California increasingly seeks to join Europe in its passage of consumer privacy laws and the latest California regulation, the California Privacy Rights Act ("CPRA") may show a more clearly enunciated intent toward altering the AdTech status quo.

Even as the European Union ("EU") continues to refine enforcement of the GDPR,[2] in the United States California continues developing its own laws, the California Consumer Privacy Act ("CCPA"),[3]and the CPRA, by ballot initiative.[4] While each of these laws are intended to address a number of different issues, they all have (or will have) significant effects on advertising technology ("AdTech") used throughout the digital world. In this article we will explore what the General Data Protection Regulation ("GDPR"), the CCPA and the newly passed, CPRA, together, may mean for AdTech and advertising on the internet in general.

First, we will briefly look at the CPRA and analyze its differences from both the CCPA and the GDPR, examining what further changes to the AdTech industry may result when it comes into effect in 2023. Second, we will investigate early enforcement of the CCPA, and what its constantly evolving regulations and guidelines signal for AdTech companies in not only Silicon Valley, but throughout the world. Finally, we will investigate GDPR enforcement actions, which have targeted some AdTech companies specifically, and what these actions indicate about how each of the Data Protection Offices within the EU plan to tackle the ever-growing nature of AdTech, in view of technological advantages that allow companies to collect and process more data than ever before.

II. CALIFORNIA PRIVACY RIGHTS ACT ("CPRA")

Passed by the citizens of California as a ballot measure during the November 2020 election, the CPRA was specifically designed to close some of the loopholes in the CCPA. For AdTech, there are two changes that are particularly important.

First, the CPRA revises the "do not sell" provisions of the CCPA to include "do not *share*," closing a key loophole that AdTech companies could potentially use to avoid certain particular aspects of the CCPA.[5] Currently, companies may claim that the use of personal information to prepare personal ads is not a "sale" under the CCPA, since that is merely done in the ordinary course of their business. The CPRA removes this ambiguity, requiring companies to provide explicit notice that individual data is being sold or shared with others. This, like the CCPA before it, may cause changes in the behavior of AdTech companies, who will now be subject to the more stringent requirements of the CPRA in order to buy or sell personal data for their advertisements. The proponents of the CPRA have openly stated that part of the intent behind this provision was to alter advertising behavior. However, some of the largest tech companies may be less concerned about these provisions since they usually collect data directly from their users (rather than obtaining it from third parties) and may have less to fear from greater restrictions on sharing data.[6] In fact, this direct relationship might work even more in their favor, as the burden to comply with the CPRA could shift to smaller companies seeking to sell the data they collect for profit.

A second major change is the creation of the California Privacy Protection Agency. This agency, separate from the California Attorney General's Office, and tasked specifically with enforcement of the CPRA, will be given much broader authority than the enforcement mechanisms available under the CCPA. Led by a 5-member board,[7] the agency will be funded with $10 million and given the authority to conduct its own investigations. A notice period of 30 days, similar to that under the CCPA, is required before enforcement actions, but once probable cause is found, the Agency may also hold its own administrative hearing in order to determine whether a violation has occurred.[8] Potential fines are the same as under the CCPA, $2,500 for violations and $7,500 for intentional violations, with the fines being paid to the Consumer Privacy Fund.

2 Regulation (EU) 2016/679, On the Protection of Natural Persons with Regard to the Processing of Personal Data and On the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1 [hereinafter GDPR].

3 Cal. Civ. Code §§ 1798.100–.192 (West 2018) [hereinafter CCPA].

4 During the November 2020 elections, California voters approved Proposition 24, the California Privacy Rights and Enforcement Act of 2020 ("CPRA"), which expanded the protections of the CCPA. See California Secretary of State, *Prop 24: Amends Consumer Privacy Laws. Initiative Statute.*, California SoS: Voterguide (2020), https://voterguide.sos.ca.gov/propositions/24/.

5 See Tim Peterson, *WTF is the CCPA's Definition of Sale?*, DigiDay (Feb. 7, 2020), https://digiday.com/marketing/wtf-ccpas-definition-sale/.

6 See, e.g. Theresa Swiggum, *The Passing of the California Privacy Rights Act (CPRA)*, Collective Measures (Nov. 18, 2020), https://www.collectivemeasures.com/insights/passing-of-california-privacy-rights-act-cpra.

7 Whose members are selected by the California Governor, the Attorney General, the Senate Rules Committee, and Speaker of the Assembly. CPRA § 1798.199.10(a).

8 *Id.* § 1798.199.55(a).

Although the California Privacy Protection Agency is newly created by the CPRA, this is not the State's first experience with an independent agency intended for privacy protection. Created in 2001, the California Office of Privacy Enforcement and Protection was tasked with enforcing the general privacy (not necessarily data privacy) laws of the State. Unfortunately, the Office was disbanded in 2012 due to budget cuts, and folded into the Attorney General's Office as part of their Privacy Unit.

The Board of this Agency, yet to be announced, will wield a lot of power over consumer privacy enforcement. The individuals chosen for the Board will set the tone for possible intended initial targets of enforcement. For the time being, though, the CPRA seems to have been drafted, in part, to address perceived loopholes related to AdTech, so it would not be unexpected if the Agency, given its independence and funding, chooses to target AdTech, similar to how the DPAs of the EU have used their enforcement independence to ply apart certain complex data handling practices.

III. CALIFORNIA CONSUMER PRIVACY ACT ("CCPA")

In its early stages, CCPA enforcement only began as of July 1, 2020. We can, however, observe the current enforcement mechanisms and compare them to those undertaken, so far, under the GDPR.

To begin, unlike the GDPR, the CCPA is not enforced by a separate regulatory body, but rather is enforced by either the Attorney General's Office or, in the case of a data breach, by consumers themselves. Consumers may bring a civil suit only after notifying a business of a breach and waiting thirty days for the business to "cure" the violation. Only if, after 30 days, the business is still in violation can the consumer bring a civil suit, either as an individual or as part of a class action suit, in which case they can seek any appropriate damages.[9] Alternatively, the Attorney General may also bring a civil action (on behalf of the people of California) against companies. The Attorney General must also provide a 30-day grace period to cure any alleged violation, after which the suit may be brought. The Attorney General may assess damages of up to $2,500 for each violation, and up to $7,500 for each intentional violation.

For now, AdTech doesn't appear to be specifically within the CCPA enforcement crosshairs, either by consumers or the Attorney General. Thus far no major AdTech companies appear to have been targeted by the Attorney General's compliance letters.[10] If we look to the list of recent privacy actions brought by the Attorney General's office as well, we see nothing to suggest that AdTech companies are being especially targeted.[11] It would appear the Attorney General is not heavily targeting companies specifically under the premise of "wrongful sale" of user data (as could be the case for AdTech companies). There could be any number of reasons that AdTech companies have not yet been targeted. Perhaps the Attorney General has decided to tackle the issue of data security and address improper personal data protection, rather than focusing on companies that buy and sell data. Alternatively, it may indicate that the CCPA's definition of "sale" of data is too broad to adequately encompass AdTech uses, who may be able to avoid an overt CCPA violation.[12] The broader provisions of the CPRA, discussed above, may support this point as well, as its proponents pointed to the vague definition of "sale" as a weakness of the CCPA.

From a consumer point of view, though, while complaints (and resulting civil suits) are not targeting AdTech companies specifically, they do at least seem to be targeting certain advertising "sharing" practices and in turn affecting AdTech markets.[13] Many of these suits have targeted companies who share data with companies like Facebook, including Zoom[14] and Houseparty,[15] and attack those companies' data sharing practices. Whether these claims are successful has yet to be seen, as the class action against Zoom is still ongoing, while the case against Houseparty has been ordered to arbitration.

---

9 CCPA § 1798.150(b).

10 These have been sent to several business thus far, though their contents and targets are not known with great certainty. See Samuel F. Cullari & Alexis Cocco, *Supervising Deputy Attorney General Offers Insight*, ReedSmith (July 14, 2020).

11 See *Recent Privacy Enforcement Action*, Cal. OAG (2020), https://oag.ca.gov/consumers/actions.

12 See Alexandra Scott, Elizabeth Canter & Lindsey Tonsager, *'Sale' Under CCPA May Not Be as Scary As You Think*, IAPP (Oct. 29, 2019), https://iapp.org/news/a/sale-under-the-ccpa-may-not-be-as-scary-as-you-think/.

13 See Aaron Nicodemus, *Walmart Latest Hit With CCPA-related Lawsuit*, Compliance Week (July 15, 2020), https://www.complianceweek.com/data-privacy/walmart-latest-hit-with-ccpa-related-lawsuit/29192.article.

14 See First Consolidated Class Action Complaint, Cullen v. Zoom Video Comm., No. 5:20-cv-02155 (N.D. Cal. Oct. 28, 2020).

15 See Complaint, Sweeney v. Life on Air, Inc., No. 3:20-cv-00742 (S.D. Cal. Apr. 17, 2020). This case was later directed to arbitration, in August 2020.

On the other hand, perhaps just the specter of enforcement has prompted certain companies to change their practices. For example, Facebook has altered its data privacy practices, which in turn has a ripple effect on the AdTech companies who rely on it to provide data.[16] These changes appear to prevent tying consumer information to previous purchases and internet history, an explicit goal of the CCPA.[17] And while many AdTech companies updated their Privacy Policies, their other practices indicate giving even further control to consumers. Google has introduced restricted data processing, in compliance with the CCPA, which restricts how Google and its partners can use personal information.[18] Google has even integrated the IAB's CCPA framework into its advertising services — seemingly before it integrated the TCF v2.0, in the European Union.[19]

IV. GENERAL DATA PROTECTION REGULATION ("GDPR")

While enforcement of the GDPR has affected a wide range of industries, companies of varying sizes, and myriad behaviors, there have been enough enforcement actions that we are able to glean some information on enforcement trends. Data Protection Authorities under the GDPR, while perhaps not as heavy handed as some may have hoped, are more than willing and capable of bringing significant fines against businesses.[20] Here, our focus is on several large fines related to advertising, but it should be noted that the GDPR has resulted in a wide variety of fines and enforcement actions against both large and small companies, in various industries, and ranging from €1,000 up to €50 million.

The French Data Protection Authority ("CNIL") 2018 enforcement action against Google provides an overview of the elaborate process. Almost as soon as the GDPR became effective, on May 25, 2018, several groups filed complaints against Google before the CNIL, including the Austrian Group *None of Your Business* and the French group *La Quadrature du Net*. Once the complaints were received, together, the CNIL had to first determine which data protection authority within the EU had authority to lead investigations into the complaints. According to the GDPR's "one-stop-shop" mechanism, companies operating within the EU need report to (and be investigated by) a single, lead data protection authority (DPA): the authority of the country where its "main establishment" is located.[21] So first, the CNIL had to coordinate with other DPAs in order to determine under whose authority the complaints and subsequent investigations would proceed.

Google argued that the CNIL was *not* the appropriate DPA to lead the investigation, since Google's main establishment within the EU was Google Ireland Limited (located in Ireland). As such, Google argued that the Irish DPA, not the CNIL, should be the lead supervisory authority in this case. However, the Irish DPA determined that Google's Irish presence was not enough to satisfy the requirement of a "main establishment" within the EU, and thus conceded authority to the CNIL.

Once jurisdiction was established, the CNIL began its investigation in earnest which, resulted in two violations attributed to Google. First, Google allegedly violated its obligations of transparency and information. Second, Google allegedly violated its obligation to have a legal basis for processing personal data in order to personalize ads.[22]

With respect to transparency, the CNIL found that Google required users to perform too many steps before they could access data collected by Google. Not only were several steps required, but the collected information could not be collected all at once, instead requiring users to access several different documents or websites in order to access their data. *Even where* a user could access their data, it was found that some information was not clear or comprehensive. The CNIL concluded that, taken together, these hurdles meant that users would be unable to understand not only the extent of data that Google collected, but also the processing that Google performs on the data.[23]

---

16 See Mike O'Brien, *The Impact of CCPA on Facebook Advertising, In One Stunning Graphic*, MultiChannelMerchant (July 17, 2020), https://multichannelmerchant.com/marketing/the-impact-of-ccpa-on-facebook-advertising-in-one-stunning-graphic/.

17 *Id.*

18 See *Helping Advertisers Comply with CCPA in Google Ads*, Google Ads Help (2020), https://support.google.com/google-ads/answer/9614122.

19 See, e.g. Robert Williams, *Google Will Adopt IAB Tech Lab's Standards for California Privacy Law*, Marketing Dive (Dec. 5, 2019), https://www.marketingdive.com/news/google-will-adopt-iab-tech-labs-standards-for-california-privacy-law/568497/; *Integration with IAB CCPA Framework Technical Specifications*, Google Ad Manager Help (2020), https://support.google.com/admanager/answer/9603027?hl=en.

20 See, e.g. Kate Fazzinii, *Europe's Sweeping Privacy Rule Was Supposed to Change the Internet, But So Far It's Mostly Created Frustration For Users, Companies, and Regulators*, CNBC (May 5, 2019), https://www.cnbc.com/2019/05/04/gdpr-has-frustrated-users-and-regulators.html.

21 *The CNIL's Restricted Committee Imposes a Financial Penalty of 50 Million Euros Against GOOGLE LLC*, CNIL (Jan. 21, 2019), https://www.cnil.fr/en/cnils-restricted-committee-imposes-financial-penalty-50-million-euros-against-google-llc.

22 *Id.*

23 Nat'l Comm'n for Computing & Liberties, *Deliberation SAN-2019-001 of January 21 2019*, Legifrance (Jan. 22, 2019), https://www.legifrance.gouv.fr/cnil/id/CNILTEXT000038032552/.

With respect to Google's legal basis for processing, the CNIL found that Google failed to obtain the informed consent of its users for the purpose of personalizing ads. As mentioned above, the CNIL found that information collected about users is spread across several documents or fields, with users unable to see the full extent of operations which utilize their data. For this reason, the CNIL held that the "consent" acquired by Google is not informed and was neither adequately "specific" nor "unambiguous," because, for the display of "personalized ads" the user's consent button is already pre-ticked, while under the GDPR, unambiguous consent requires a clear affirmative action by the user. The CNIL further concluded consent was not specific because, when creating an account, a user merely checks a single box that states "I agree to the processing of my information as described above"; while under the GDPR, consent must be given for *each* specific processing purpose.[24]

In light of its findings, the CNIL imposed a fine of €50 million (~$59 million).

Google is not the only company to have its advertising techniques scrutinized under the GDPR. In fact, the Italian Data Protection Authority ("Garante") has also issued several large fines, the two largest totaling almost €45 million, against companies for inappropriate "promotional materials" under the GDPR.

First, in January 2020, the Garante fined TIM SpA ("TIM"), an Italian telecommunications company, for €27.8 million.[25] After receiving complaints from 2017 through early 2019, the Garante launched an investigation into TIM's data processing activities. After a months-long investigation, the Garante found numerous violations of the GDPR by TIM, including:

- Contacting "prospective" customers upwards of 155 times a month without the consent of those non-customers;
- Failure to honor the requests of customers and non-customers who asked to be put on a "do not call" list;
- Preserving customer and non-customer related information beyond the scope of TIM's service and using that preserved data for abusive promotional purposes; and
- Not obtaining specific consent from customers and non-customers for each use of personal data.

As a result of these violations, in addition to the fine mentioned above, the Garante also required TIM to implement 20 security measures within 180 days: 6 related to limiting the processing of personal data which must be implemented with 60 days, and the remaining 14 related to modifying TIM's data infrastructure within 180 days, including implementing measures that respect users' right to opt out of promotional materials.

Later that year, on July 9, 2020, the Garante also issued a fine and injunction against Wind Tre SpA, another Italian telecom company, to the order of €16.7 million.[26] Wind Tre had previously been enjoined in 2018 under Italy's previous privacy regulation (pre-dating the GDPR), but the Garante found that it was still in violation of the GDPR, though they only considered complaints received after May 25, 2018. Users' primary complaints were related to receiving unwanted promotional calls, emails, faxes, and text messages from Wind Tre, even after the users had withdrawn their consent to receive such communications. Even where users had not withdrawn their consent, though, the Garante found various issues with the consent that Wind Tre *had* received. For example, some of the consents had been acquired in the 1980's, and thus were no longer compliant with modern regulations. In other situations, the consent was found to not be freely given by the users, who either were unaware that they were providing consent, or in some cases were misled by Wind Tre operators, who thus acquired these consents illegally.

Wind Tre attempted to justify these mistakes by denying responsibility, since most of the promotional communications were not authored or controlled by Wind Tre, but rather by independent operators (to the benefit of Wind Tre). The Garante did not find this reasoning convincing, though, as in its opinion, it stated that Wind Tre should exercise sufficient supervision over these operators to prevent unauthorized communications.

24 *Id.*

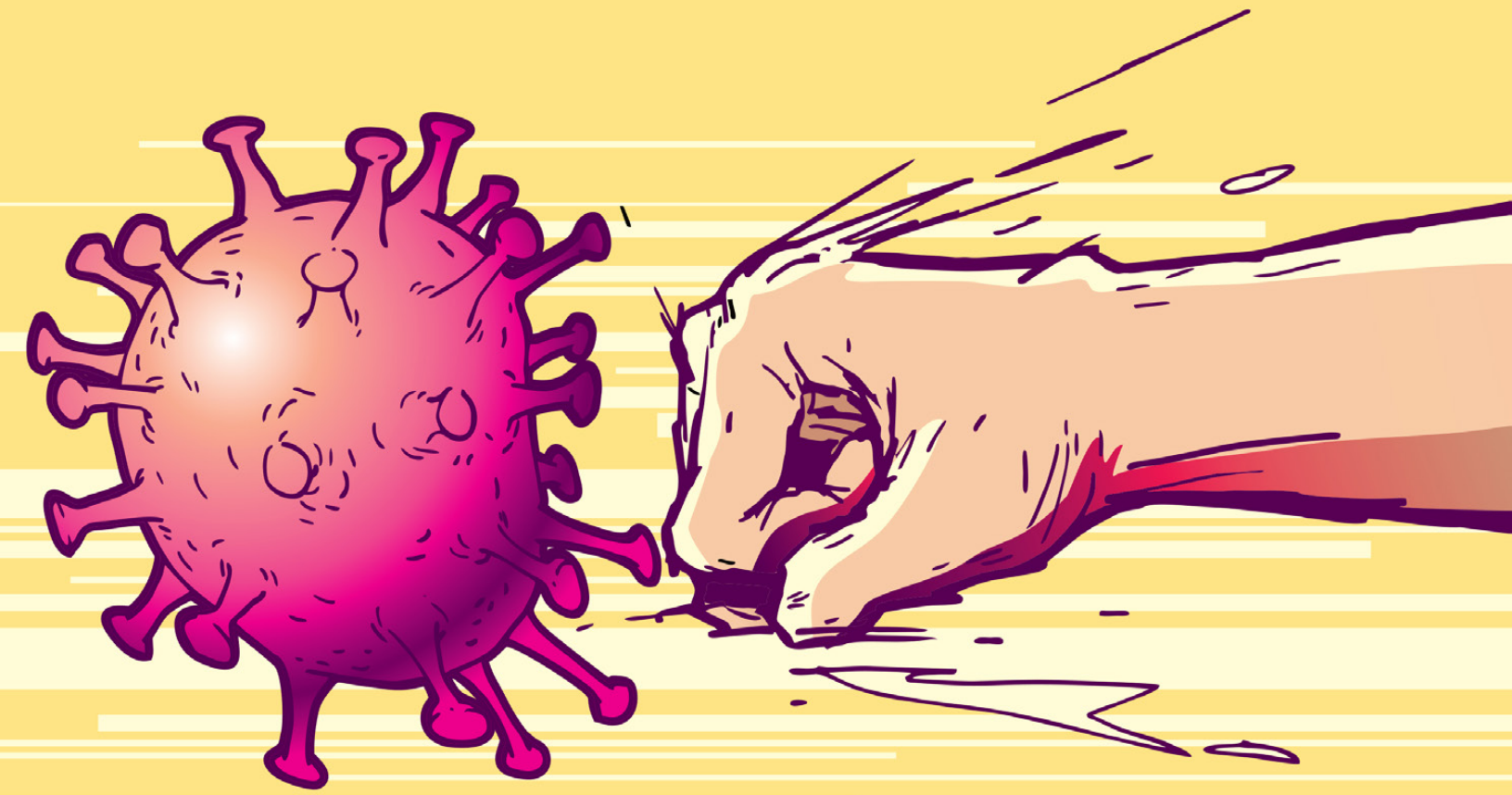
25 Garante per la Protezione dei Dati Personali, *Corrective Sanctioning Measure Against TIM SpA – January 15, 2020 [9256486]*, GaranteePrivacy (Feb. 1, 2020), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9256486.

26 Garante per la Protezione dei Dati Personali, *Injunction Order Against Wind Tre SpA – 9 July, 2020 [9256486]*, GaranteePrivacy (July 13, 2020), https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9435753.

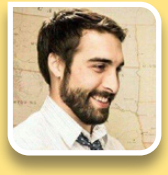
CONCLUSION

It's a dynamic time in data privacy. GDPR enforcement is gaining legs, with DPA decisions affirmed and hefty fines levied against a variety of targets; the CCPA has finally reached the enforcement phase; and the CPRA threatens to further redefine the data privacy landscape. In response, AdTech companies appear to have altered some of their data collection, handling, and sharing practices. Time will tell the long-term implications of these changes and which companies and industries will benefit from increased and more artfully drafted consumer data privacy regulations but in any case, with each investigation, regulators gain more information on technological advantages that allow companies to collect and process more data than ever before. And this information informs more specific consumer data privacy regulation that attempts, openly, to influence larger data handling trends, not just protect consumer privacy.

THE PANDEMIC, EDTECH, AND THE TRICKY SUBJECT OF SERVICE PROVIDERS AND PROCESSORS



BY CODY VENZKE[1]



1 Cody J. Venzke is a Policy Counsel at the Center for Democracy & Technology and focuses on privacy, technology, and data in education. The views expressed in this article are exclusively those of the author and do not necessarily reflect those of the Center for Democracy & Technology. This article has been prepared for informational purposes only and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, a lawyer-client relationship. Readers should not act upon this without seeking advice from professional advisers.

I. INTRODUCTION

With the onset of the global coronavirus pandemic, the use of technology in education has seen a rapid transformation. Schools implemented remote learning in response to the pandemic and, instead of learning in classrooms, children began learning online, a trend that has extended well into the new school year. With the movement of children's learning and data online, privacy concerns began to multiply. Advocates called attention to data use and security vulnerabilities in education technology ("edtech") platforms. That concern was shared by the California Attorney General's Office, which was responsible for the newly enforceable California Consumer Privacy Act ("CCPA").[2] Early in the pandemic, the Attorney General stated, "Whether it's our children's schooling, socializing with family and friends, or working remotely – we are turning to mobile phones and computers as a lifeline. With such a dependency on online connectivity, it is more important than ever for Californians to know their privacy rights."[3]

The CCPA shares a number of similarities[4] with the European Union's General Data Protection Regulation ("GDPR").[5] Both regulations, for example, enable individuals to be notified about companies' data collection and data use practices, to review the data collected, and to seek its correction or deletion.[6] Nonetheless, the two laws are not identical, and untangling their application to schools and edtech vendors can be complicated. As described below, that applicability depends not only on the data these entities collect, but about whom they collect it, where they do business, and their roles as principals or agents in the data processing lifecycle.

This paper examines the landscape of edtech in the pandemic, the geographic and substantive applicability of the CCPA and the GDPR, both laws' tangled provisions governing principals and agents in the data lifecycle, and the significance of those provisions for the exercise of individuals' data rights.

II. LANDSCAPE OF EDTECH BEFORE, DURING, AND AFTER THE PANDEMIC

Edtech vendors provide technology products for schools, families, and parents to help support learning in and outside of the classroom. With the onset of the pandemic, edtech became synonymous with the videoconferencing platforms of Zoom Video Communications, Inc., and other companies as students and teachers increasingly relied on them to connect.[7] Videoconferencing, however, represents only one sliver of the broader edtech market, with products available to aid students' writing, to provide modules for teaching and assessing, to maintain student records and credentials, and to recruit employees and postsecondary students.[8]

The edtech market drives both investment and data collection. In 2018, new U.S. investments in edtech platforms exceeded $1 billion, with $333 million invested in edtech for K-12 institutions, $463 million in edtech for postsecondary institutions, and $437 in informal learning.[9] Within K-12 investment in 2018, $148 million was invested in technology supporting school operations, $95 million in supporting teacher needs, and $90 million in providing curriculum,[10] with the majority of the investment in curriculum-related technology flowing to language arts and language learning.[11] Investment is expected to increase, especially in adult education and outside of the United States as part of the continued growth of the education sector in general and the continued effects of the pandemic specifically.[12] The pandemic in particular has driven a spike

2 Cal. Civil Code. §§ 1798.100-.199.

3 Attorney General Press Office, *Attorney General Becerra Reminds Consumers of their Data Privacy Rights During the COVID-19 Public Health Emergency*, State of California Department of Justice (Apr. 10, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-reminds-consumers-their-data-privacy-rights-during.

4 See DataGuidance & Future of Privacy Forum, *Comparing Privacy Laws: GDPR vs. CCPA* (Dec. 18, 2019), available at https://fpf.org/2019/12/18/comparing-privacy-laws-gdpr-v-ccpa/.

5 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 and on the free movement of such data, and repealing Directive 95/46/EC, General Data Protection Regulation, 2016 OJ (L 119) 1 [hereinafter GDPR].

6 See DataGuidance & Future of Privacy Forum, *supra* note 4.

7 Patrick Wall, *With Cell Phones and Laptops, Newark Teachers Stay Connected with Students During School Shutdown*, Chalkbeat (Mar. 19, 2020), https://newark.chalkbeat.org/2020/3/19/21196078/with-cell-phones-and-laptops-newark-teachers-stay-connected-with-students-during-school-shutdown.

8 See Simran Mahanty, *Top 25 SaaS EdTech Companies in 2020*, SmartKarrot (Sept. 18, 2020), https://www.smartkarrot.com/resources/blog/top-edtech-companies-startups/.

9 EdSurge, *Preparing for Impact: What's Changing in Edtech Investment*, State of Edtech 2019, https://www.stateofedtech2019.com/ (last visited Nov. 30, 2020).

10 *Id.*

11 EdSurge, *K-12 Curriculum*, State of Edtech 2019, https://www.stateofedtech2019.com/curriculum (last visited Nov. 30, 2020).

12 Mike Dolan, *Big Funds Circle EdTech as Post-Pandemic Mega-Trend* (Sept. 25, 2020), https://www.nasdaq.com/articles/column-big-funds-circle-edtech-as-post-pandemic-mega-trend-%3Amike-dolan-2020-09-25.

in edtech adoption, with the number of different edtech tools in use jumping from 703 per month to 1,327 — a ninety percent increase.[13]

The increased investment in and adoption of edtech has driven data collection and usage by schools and vendors — and with it, privacy concerns.[14] Educational institutions have long collected student data to assess and monitor student achievement, but technology has made it possible to collect and connect new dimensions of data. For example, the California Cradle-to-Career Data System will combine data from K-12 schools, colleges and universities, employers, and social services to track the effectiveness of education programs in helping students secure places in the workforce.[15] Data and the edtech that facilitates its collection and sharing may also help schools assess gaps in equity, access to technology, and educational opportunity.[16]

However, privacy concerns have accompanied that data collection and sharing and have prompted calls for policy reforms to address the new challenges of emerging education technology.[17] The primary U.S. federal student privacy law, the Family Educational Rights and Privacy Act (FERPA),[18] was passed in 1974, long before the rise of edtech and big data and in many ways did not anticipate the prominent role of technology and data in education.[19] Consequently, the CCPA and the GDPR, tailored for data collection and sharing by "advanced technologies" and "sophisticated algorithms,"[20] may seem like strong candidates to address the privacy concerns raised by edtech and data collection in schools.

Those laws, however, have specific and sometimes idiosyncratic provisions governing their applicability based on geography, substance, and edtech vendors' relationships to the schools they serve. Schools and vendors should be especially cognizant of the laws' differing applications to principals and agents in the data lifecycle and for- and non-profit entities.

III. GEOGRAPHIC AND SUBSTANTIVE SCOPE

The GDPR and the CCPA both contain provisions governing their geographic reach and substantive scope — that is, the type of entities they apply to and the information and individuals they protect. Those provisions depend not only where individuals subject to data collection are located, but where edtech vendors conduct their business, and on the type of data they are collecting.

A. Geographic & Substantive Scope of the GDPR

The GDPR applies to two sets of entities with ties to the European Union. First, it applies to entities in the European Union that process personal data, regardless of where the processing takes place.[21] That scope includes both entities and their agents — labeled data "controllers" or "processors" — with "an establishment" in the Union.[22] Second, the GDPR applies to controllers and processors outside the Union if they process the data of "data subjects" or natural persons within the Union, so long as that processing is related to either offering goods or services to or monitoring the behavior of data subjects in the Union.[23]

---

13 Michele Molnar, *Number of Ed-Tech Tools in Use Has Jumped 90 Percent Since School Closures*, EdWeek Market Brief (July 8, 2020), https://marketbrief.edweek.org/marketplace-k-12/access-ed-tech-tools-jumped-90-percent-since-school-closures.

14 Alyson Klein, *Here's How Districts Should Handle Privacy Considerations in the COVID Era*, EdWeek (Oct. 27, 2020), http://blogs.edweek.org/edweek/DigitalEducation/2020/10/covid-privacy-districts-technology.html; Dominic Dhil Panakal, *School Stakeholders Navigating Student Privacy*, National Law Review (Oct. 29, 2020), https://www.natlawreview.com/article/school-stakeholders-navigating-student-privacy.

15 WestEd, *California Cradle-to-Career Data System*, California Data System, https://cadatasystem.wested.org/ (last visited Nov. 30, 2020).

16 Sam Peterson, *Why Teachers Need Interoperability—Whether They Know It or Not*, EdSurge (Oct. 27, 2020), https://www.edsurge.com/news/2020-10-27-why-teachers-need-interoperability-whether-they-know-it-or-not.

17 See Cheri Kiesecker, *A Privacy Blueprint for Biden*, Parent Coalition for Student Privacy (Nov. 11, 2020), https://www.studentprivacymatters.org/a-privacy-blueprint-for-biden; Faith Boninger et al, *Asleep at the Switch: Schoolhouse Commercialism, Student Privacy, and the Failure of Policymaking*, National Education Policy Center (Aug. 15, 2017), https://nepc.colorado.edu/publication/schoolhouse-commercialism-2017.

18 20 U.S.C. § 1232g.

19 Owasso Independent School Dist. No. I-011 v. Falvo, 534 U.S. 426. 434-35 (2002) ("Congress contemplated that education records would be kept in one place with a single record of access. . . . FERPA implies that education records are institutional records kept by a single central custodian, such as a registrar . . . .").

20 AB 375 Senate Floor Analysis, S. 2017-2018 at 6 (June 28, 2018), https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201720180AB375#.

21 GDPR art. 3(1).

22 GDPR art. 3(1).

23 GDPR art. 3(2).

The focus of those protections is "personal data." Under the GDPR, "personal data" is any information "relating" to a data subject; a "data subject" is any "identified or identifiable natural person."[24] That definition does not contain a citizenship requirement and consequently, the scope of the GDPR's protections is not limited to residents or citizens of the Union, but any natural person physically in the Union.[25] "Processing" means any "operation" on personal data such as collecting, using, disclosing, or deleting data — roughly analogous to each stage in various formulations of the data lifecycle.[26]

The GDPR's substantive scope encompasses education data. Both schools and edtech vendors will hold personal data that relates to identifiable natural persons such as transcripts, performance metrics, demographic information, applications for admission, employee personnel files, and medical records. Critically, the GDPR applies to more than schools physically *in* the Union but also to schools that collect personal data *from* persons in the Union. That scope might include North American universities that collect applications from prospective students in the Union, maintain files on employees there, or send students to study abroad in the Union.[27] Edtech vendors, however, do not necessarily collect personal data on their own initiative, but do so on behalf of schools. Consequently, their obligations under the GDPR depend on the GDPR's two-tiered distinction between principals and agents in the data lifecycle, or "controllers" and "processors," discussed in detail below.

B. Geographic & Substantive Scope of the CCPA

The CCPA has a similar broad reach beyond the borders of its enacting jurisdiction. The CCPA applies to any "business" that is organized for profit, does business in California, "collects consumers' personal information or on the behalf of which that information is collected," and "determines the purposes and means of the processing of consumers' personal information."[28] Under the CCPA, a "consumer" is any "natural person who is a California resident."[29] Thus, like the GDPR, the CCPA is applicable even to businesses not physically in the state so long as it does business there. Unlike the GDPR, however, the CCPA protects only permanent residents, including when they are temporarily outside the state[30]; its protections do not extend to all natural persons "in" the jurisdiction, such as temporary residents and visitors.[31]

Like the GDPR's "personal data," the CCPA defines "personal information" broadly. Its definition includes information that "could reasonably be linked, directly or indirectly, with a particular consumer," paralleling the standard definition of personal information as information that is "linkable" to a particular person.[32] The CCPA, however, expands this definition, including "information that identifies, relates to, describes, is reasonably capable of being associated with" a household or consumer. Although that definition extends beyond mere identification or linkability,[33] neither the California Attorney General nor the courts have clarified its boundaries. The CCPA's definition of "personal information" includes a non-exhaustive list of examples, including "[e]ducation information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act."[34]

---

24 GDPR art. 4(1); see Laura Jehl & Alan Friel, *CCPA and GDPR Comparison Chart*, BakerHostetler LLP (2018), https://www.bakerlaw.com/webfiles/Privacy/2018/Articles/CCPA-GDPR-Chart.pdf.

25 GDPR rec. 14 ("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.").

26 E.g., UNICEF & Gov Lab, Responsible Data for Children: Synthesis Report at 7 (2019), available at https://rd4c.org/files/rd4c-report-final.pdf (listing planning, colleting, storing and preparing, sharing, analyzing, and using); *Data Lifecycle*, U.S. Geological Survey, https://www.usgs.gov/products/data-and-tools/data-management/data-lifecycle (last visited Nov. 26, 2020) (planning, acquiring, processing, analyzing, preserving, and sharing).

27 See *General Data Protection Regulation (GDPR)*, New York University, https://www.nyu.edu/life/information-technology/it-security-and-policies/general-data-protection-regulation.html (last visited Dec. 1, 2020).

28 Cal. Civil Code § 1798.140(c). The CCPA's definition of "business" also includes three alternative thresholds: annual gross revenues worldwide in excess of $25 million, processing the data of 50,000 or more consumers, or deriving more than fifty percent of its annual revenue from selling consumers' personal information. Id. § 1798.140(c)(1)(A)-(C).

29 Cal. Civil Code § 1798.140(g).

30 Cal. Civ. Code § 1798.140(g) (citing Cal. Code Regs. tit. 18, §17014).

31 Jehl, *supra* note 24; GDPR rec. 14.

32 See, e.g., 34 CFR 99.3 (defining "personally identifiable information" in part as "information that, alone or in combination, is linked or linkable to a specific student"); 45 CFR § 160.103 (defining "individually identifiable health information" in part as information for "which there is a reasonable basis to believe the information can be used to identify the individual); Erika McCallister et al., Nat'l Ins. of Stds. & Tech., Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) at 2-1 (2010), available at https://csrc.nist.gov/publications/detail/sp/800-122/final (defining PII as "any information that can be used to distinguish or trace an individual's identity . . . [or] any other information that is linked or linkable to an individual.").

33 Jacob Rubinstein, *A Close-Up on Deidentified Data Under CCPA*, IAPP (Aug. 27, 2019), https://iapp.org/news/a/a-close-up-on-de-identified-data-under-the-ccpa.

34 Cal. Civil Code § 1798.140(o)(1)(J) (citing 20 U.S.C. § 1232g; 34 C.F.R. Part 99).

Despite its explicit application to education information, the CCPA does not necessarily apply to schools and edtech providers. Most schools in the United States, including in California, are not organized for profit and instead are either nonprofit entities or subdivisions of the state or local government. Those schools, consequently, fall outside the CCPA's definition of "business," which requires an entity to be organized for profit.[35] Most edtech vendors, however, are for-profit entities.[36] Nonetheless, like the GDPR, the CCPA distinguishes between a "business" "on the behalf of which [personal] information is collected" and its agent, a "service provider" that "processes information on behalf of a business." Because edtech vendors collect and process personal information on behalf of schools, the applicability of the CCPA to edtech vendors depends on its treatment of principals and agents in the data lifecycle. We examine that treatment next.

IV. THE TRICKY SUBJECT OF PROCESSORS AND SERVICE PROVIDERS

A. Data Controllers and Data Processors under the GDPR

The GDPR and the CCPA both envision a two-tiered distinction between principals and agents in the data lifecycle. The GDPR categorizes principals and agents in the data lifecycle as "controllers" and "processors," respectively. A controller "determines the purposes and means of processing of personal data," while the processor "processes personal data on behalf of the controller."[37] Unlike under the CCPA, the GDPR's distinctions do not incorporate entities' for-profit status. A processor must be governed by a contract between the controller and the processor or by another legally binding act.[38] That contract must limit the "subject-matter and duration," "nature and purpose, "and categories of personal data and data subjects" of the processing.[39] The processor may "process[] the personal data only on documented instructions for the controller."[40]

Consequently, regardless of their for-profit status, schools and edtech vendors may qualify as controllers and processors, respectively. The relationship between a school and an edtech vendor may be described as one of principal and agent: the school provides student information to the vendor to provide the service such as online course materials or videoconferencing, and the vendor collects information on behalf of the school such as students' assignment submissions.[41] In that relationship, the school will define both the purposes and means of the processing; consequently, the school likely constitutes a controller and the edtech vendor a processor.

Edtech vendors, however, often collect and retain information for their own purposes and not on behalf of a school. For example, Summit Learning's privacy policy allows it to collect "de-identified" data, with all identifying data removed, for any purpose and to retain it indefinitely.[42] Similarly, Google's G-Suite for Education permits schools to allow students to use Google services beyond its core educational services; data collected from students using those "Additional Products" may be used for a variety of non-educational purposes such as customizing or developing new products.[43]

That collection may render an edtech vendor a "controller" under the GDPR. The European Data Protection Board ("EDPB") has suggested a processor acting "on behalf of" a controller "means that the processor may not carry out processing for its own purpose(s)."[44] The GDPR recognizes that processors might also collect or use data for their own purposes and provides, "[I]f a processor infringes this Regulation by

35 However, schools receiving funding from the U.S. Department of Education, usually public schools, are subject to the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g, and myriad state student privacy laws, see *State Student Privacy Laws*, Student Privacy Compass, https://studentprivacycompass.org/state-laws/ (last visited Dec. 16, 2020).

36 See *List of EdTech Companies*, Crunchbase, https://www.crunchbase.com/hub/edtech-companies (last visited Nov. 20, 2020); Tony Wan, *Dozens of Venture-Backed Startups Among Edtech Recipients of PPP Loans*, Ed Surge (July 24, 2020), https://www.edsurge.com/news/2020-07-14-dozens-of-venture-backed-startups-among-edtech-recipients-of-ppp-loans.

37 GDPR art. 4(6), (7).

38 GDPR art. 28(3).

39 *Id.*

40 *Id.* art. 28(3)(a).

41 Privacy Technical Assistance Center, U.S. Dep't Ed., Protecting Student Privacy While Using Online Educational Services: Requirements and Best Practices at 2 (Feb. 2014), available at https://studentprivacy.ed.gov/resources/protecting-student-privacy-while-using-online-educational-services-requirements-and-best.

42 *Data Privacy Addendum* § 4.5, Summit Learning, https://www.summitlearning.org/privacy-center/data-privacy-addendum (last visited Dec. 1, 2020).

43 *G Suite for Education Privacy Notice*, Google, https://workspace.google.com/intl/en/terms/education_privacy.html (last visited Nov. 23, 2020).

44 European Data Protection Board, Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR ¶ 79 (Sept. 2, 2020), *available at* https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/guidelines-072020-concepts-controller-and-processor_en [hereinafter Guidelines 07/2020].

determining the purposes and means of processing, the processor shall be considered to be a controller in respect of that processing."[45] In such cases, the edtech vendor may qualify both as a processor and a controller, depending on if the data is processed on behalf of the school or for its own purposes.[46]

The GDPR also recognizes that two data controllers may qualify as "joint controllers." Edtech vendors and their school partners, however, may not qualify as a "joint controllers," due to divergent purposes and means of processing personal data. Under the GDPR, a "joint controller" is when "two or more controllers jointly determine the purposes and means of processing."[47] Joint controllers must provide a "transparent" determination of responsibilities to comply with the GDPR, including in providing notice to data subjects.[48] The EDPB envisions that jointly determined purposes will either entail "the same, or common, purposes" or purposes that are "closely linked and complementary."[49] Similarly, jointly determined means requires each entity to "have exerted influence over the means of the processing," such as by agreeing to use a means of processing provided by one of the parties.[50]

An edtech vendor's use of student data for its own purposes is unlikely to meet those requirements, as the school and the vendor do not jointly determine either the purposes or the means of the processing. Instead, the schools merely utilize the data collected and forwarded by the vendor. The EDPB has suggested that merely "send[ing] personal data" is not sufficient to establish joint controllers.[51] For example, the EDPB describes an arrangement in which a "travel agency sends personal data of its customers to the airline and a chain of hotels, with a view to making reservations for a travel package"; each entity "processes the data for carrying out their own activities and using their own means."[52] Because there is no joint determination of means, the travel agency, airline, and hotel chain are likely not joint controllers. The same is likely true of an edtech vendor to the extent it uses student data for its own purposes and through its own means.

B. Service Providers under the CCPA

Although it makes a similar distinction between principals and agents, the CCPA's regime of "businesses" and "service providers" differs from the GDPR because it depends on an entity's for-profit status. As described above, a business under the CCPA is, among other requirements, a "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 that information is collected."[53] Because most schools are not operated for profit, they do not fall within the scope of the CCPA.[54]

Edtech vendors, however, present a more complicated picture for two reasons. First, many edtech vendors would qualify as a business under the CCPA. As described above, many edtech vendors are for-profit entities and collect personal information. The collection is often for the vendor's own purposes, including research and the development of new products — non-educational uses that would likely be for the vendor's benefit rather than "on behalf of" its school partners. Similarly, a "business" under the CCPA must have annual gross revenues exceeding $25

45 See GDPR art. 28(10).

46 *Data Processing Amendment to Google Workspace and/or Complementary Product Agreement (Version 2.3)* ¶ 5.3, Google, https://workspace.google.com/terms/dpa_terms.html (last visited Nov. 23, 2020) ("[T]his Data Processing Amendment does not apply to the processing of personal data in connection with the provision of any Additional Products.").

47 GDRP art. 26(1).

48 *Id.*

49 Guidelines 07/2020 ¶¶ 57-58.

50 *Id.* ¶¶ 62-63.

51 *Id.* ¶ 66.

52 *Id.*

53 Cal. Civil Code § 1798.140(c)(1).

54 Center for Analysis of Postsecondary Education and Employment, *Trends in Enrollment*, Columbia University (Feb. 2018), https://capseecenter.org/research/by-the-numbers/for-profit-college-infographic/.

million,[55] which the California Attorney General has clarified is worldwide revenue.[56] Many edtech vendors, especially the largest, clear that threshold.[57]

Second, that conclusion is complicated by the fact that edtech vendors are also working as agents on behalf of schools, which are not businesses. Like the GDPR, the CCPA recognizes a two-tier system of compliance for principals and agents. Whereas businesses are the primary focus of the CCPA, a "service provider" is a legal entity that "is organized or operated for the profit or financial benefit of its shareholders or other owners, that processes information on behalf of a business and to which the business discloses a consumer's personal information."[58] A business may disclose personal information to a service provider only pursuant to a written contract that, among other things, prohibits the service provider "from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified."[59]

Under those provisions, a service provider must process information "on behalf of a business." Thus, many edtech vendors would not qualify as "service providers" because the schools on whose behalf they process personal information do not qualify as businesses.

That conclusion, however, is altered by regulations recently promulgated by the California Attorney General, which alter the scope of a "service provider." Three of those regulatory provisions are relevant here.

First, the regulations provide that a business processing personal information on behalf of a nonprofit or public entity shall still be deemed a service provider. The regulations state, "A business that provides services to a person or organization that is not a business, and that would otherwise meet the requirements and obligations of a 'service provider' under the CCPA and these regulations, shall be deemed a service provider."[60] The Attorney General explained that this provision was necessary to avoid businesses providing services to nonprofits and public entities from being bound by the obligations the CCPA places on "businesses."[61] The Attorney General explained:

> For example, a public school district may use a service provider to secure student information, including each student's grades and disciplinary record. Without this regulation, service providers used by public and nonprofit entities may be required to disclose or delete records in response to consumer requests because they may constitute businesses that maintain consumers' personal information. Service providers for public and nonprofit entities could also be asked to disclose personal information maintained by a government agency, despite the fact that such files may be expressly exempt from disclosure under the Public Records Act.

Notably, this explanation assumes that entities that meet the CCPA's definitions of both "service provider" and "business" are only obligated to meet the obligations imposed on service providers, an assumption that is not expressly stated in the CCPA itself.[62] Thus, an edtech vendor providing services to a school may still qualify as a service provider and is likely not bound by the obligations imposed on businesses — at least to the extent the vendor is providing services to a school.

---

55 Cal. Civil Code § 1798.140(c)(1)(A). Alternatively, a business that "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" or derives "50 percent or more of its annual revenues from selling consumers' personal information" will qualify as a "business." *Id.* § 1798.140(c)(1)(B)-(C).

56 Office of the Attorney General, Summary and Response to Comments Submitted During 45-Day Period, resp. 5 (June 1, 2020) [hereinafter 45-Day Response], available at https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-fsor-appendix-a.pdf.

57 Tony Wan, *Earnings Roundup: How Public Edtech Companies Fared Following the Outbreak*, EdSurge (May 12, 2020), https://www.edsurge.com/news/2020-05-12-earnings-roundup-how-public-edtech-companies-fared-following-the-outbreak.

58 Cal. Civil Code § 1798.140(v) (emphasis added).

59 *Id.*

60 Cal. Code Regs. tit. 11, § 999.314(a).

61 Office of the Attorney General, Final Statement of Reasons at 30 (June 1, 2020) [hereinafter Final Statement of Reasons], *available at* https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/oal-sub-final-text-of-regs.pdf.

62 See 45-Day Response, resp. 555; Office of the Attorney General, Initial Statement of Reasons at 23 (Oct. 11, 2019) [hereinafter Initial Statement of Reasons], https://www.oag.ca.gov/sites/all/files/agweb/pdfs/privacy/ccpa-isor-appendices.pdf.

Second, the regulations clarify that an entity that collects data from or about consumers at the direction and on behalf of a business may still qualify as a "service provider."[63] The CCPA required entities to have personal information "disclose[d]" to them by a business to qualify as a service provider.[64] The Attorney General determined the statutory language was "incomplete" and added this regulatory provision to ensure that entities that collect information "as directed by or on behalf of a business" may still qualify as service providers, even if information is not disclosed to them by their business partners.[65]

The third regulatory provision clarifies "how entities that are both a service provider and a business are to handle consumer requests and other obligations under the CCPA."[66] The provision states, "A service provider that is a business shall comply with the CCPA and these regulations with regard to any personal information that it collects, maintains, or sells outside of its role as a service provider."[67] Thus, an edtech vendor that collects or processes information for its own purposes will be deemed a business under the CCPA for that collection or processing, subject to the corresponding obligations. The implication from this provision is that an entity is not bound by the CCPA's business provisions[68] with respect to the processing it provides as a service provider.

The sum result of these regulatory provisions is that for-profit edtech vendors may still qualify as service providers even if they (1) are processing personal information on behalf of not-for-profit entities, (2) are collecting information from or about consumers, so long as they do so on behalf of and at the direction of a business, and (3) otherwise qualify as a business under the CCPA, but any information processed outside the scope of their functions as a service provider is subject to the CCPA's business obligations.

V. IMPLICATION FOR DATA RIGHTS

Ultimately, the geographic scope, substantive applicability, and principal-agent distinction determine who is responsible for ensuring that individuals can exercise their data rights. Both the GDPR and the CCPA provide persons with rights to data deletion, disclosure of collection and sharing practices, opt-out or objection to certain data uses, and nondiscrimination for exercising their rights. Both also require businesses or controllers to obtain affirmative consent regarding certain processing of personal information from children younger than 16.[69] The GDPR carries additional rights to data minimization, rectification, portability, and disclosure of automated decision making.

Under both laws, the principal in the data lifecycle — the "controller" under the GDPR and the "business" under the CCPA — carry the primary responsibility for exercising those rights. Both laws require the controller or business to notify data subjects and consumers of their statutory rights and to facilitate requests for data access, deletion, opt-out or objection, and correction, among others.

In contrast, the responsibilities of processors and service providers are more limited and more contractual in nature. The GDPR requires that processors "be governed by a contract . . . that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller."[70] With respect to data subjects' data rights, however, a processor must merely "assist[] the controller . . . for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights."[71] The CCPA regulations specifically permit service providers to decline to honor requests made by consumers or to direct the consumers to the corresponding business.[72] Like the GDPR, the CCPA requires the service provider to operate under a written contract that "prohibits the entity receiving the information from retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract."[73]

63 Cal. Code Regs. tit. 11, § 999.314(b).

64 Cal. Civil Code § 1798.140(v).

65 Initial Statement of Reasons at 21.

66 *Id.* at 23.

67 Cal. Code Regs. tit. 11, § 999.314(f).

68 Cal. Civil Code § 1798.100-.135.

69 Cal. Civil Code § 1798.120(c) (affirmative consent to opt-in to the sale of PI); GDPR art. 8(1) (parental consent must be provided for any processing for children under 16).

70 GDPR art. 28(3).

71 GDPR art. 28(3)(e).

72 Cal. Code Regs. tit. 11, § 999.314(e).

73 Cal. Civil Code § 1798.140.

Thus, under either law, an edtech vendor must be cognizant of when it is processing data as a "business" under the CCPA or as "controller" under the GDPR; in those cases, it must provide consumers with the required notices and respond to requests by consumers to exercise their data rights. As a "service provider" or "processor," the vendor does not necessarily have those responsibilities, but must still operate within the contractual requirements imposed by the laws.

VI. CONCLUSION

Technology and data have played an increasing role in education, a trend that has been amplified by the pandemic and remote learning. Although the GDPR and CCPA may seem uniquely suited to the privacy concerns posed by edtech, their application depends on a number of factors, and edtech vendors should be aware of the laws' geographic reach, substantive scope, and distinctions between principals and agents in the data lifecycle.

CCPA AND COMPETITION: THE VALUE OF CONSUMER DATA, PRIVACY, AND PRICING

BY JEEWON KIM SERRATO & LAWRENCE WU[1]

1 Jeewon Kim Serrato is a Partner and Co-lead of the Digital Transformation and Data Economy team at BakerHostetler. Lawrence Wu is an economist and President of NERA Economic Consulting. A portion of this article was originally published in the Competition Journal of the Antitrust and Unfair Competition Law Section of the California Lawyers Association. See Jeewon Kim Serrato & Lawrence Wu, "Privacy, Pricing, and the Value of Consumer Data: The Complex Nature of the CCPA's Non-Discrimination Requirement," *Competition*: Fall 2020, Vol 30, No. 2, available at https://calawyers.org/publications/antitrust-ucl-and-privacy/chairs-column-36/.

I. INTRODUCTION

With the passage of privacy laws like the EU General Data Protection Regulation and the California Consumer Privacy Act ("CCPA"), there is increasing debate around whether the goals of antitrust and privacy laws are incompatible or complimentary.[2] Privacy laws affect the way firms compete, particularly when consumers are given a choice of opting in or opting out of providing companies with their personal information and when those choices may be affected by the prices charged and the services offered by those companies.

The CCPA, which went into effect on January 1, 2020, is a first-of-its-kind law that requires businesses to calculate the value of consumer data. While it includes several new consumer rights, such as the right to know, right to delete, and a right to opt-out, this article will focus on the right to non-discrimination and the complexities that businesses will face as they navigate three things: the need to ensure consumers' right to privacy and non-discrimination under the CCPA; the ability to offer competitive prices and marketing incentives to meet consumer demands; and the opportunity to earn revenue from the consumer data they may be able to collect, sell, and retain.

These three interrelated objectives complicate what businesses may have to do to meet one of the fundamental requirements under the CCPA, which is this: if a business offers financial incentives or a price or service difference as compensation for the collection, sale, or retention of consumer data, the business must explain how the incentives or price or service difference are reasonably related to the value of the data to the business. This is uncharted territory; and while we wait to see what enforcement actions the California Attorney General brings under this law, which began on July 1, 2020, we cannot underestimate the lasting impact the law may have on the global privacy discourse and how regulators view the respective rights and powers the consumers and businesses have in controlling the use of personal data that is collected about individuals.

II. THE RIGHT TO NON-DISCRIMINATION UNDER THE CCPA

One of the most groundbreaking aspects of the CCPA is the notion that consumers have a right to non-discrimination, under which businesses are prohibited from discriminating against consumers who exercise their privacy rights, such as the right to know, delete, or opt-out of the sale of their personal information. To comply with the CCPA, businesses must include a statement in their privacy policies informing consumers that they have a right "not to receive discriminatory treatment" for exercising their CCPA rights.

While the CCPA does not define what it means to "discriminate," it provides a non-exclusive list of practices that may qualify as discriminatory, if the business responds to a consumer who exercised the consumer's rights under the CCPA by:

- Denying goods or services;
- Charging different prices;
- Providing a different quality of goods or services; and
- Suggesting that the consumer may receive a different price or rate.[3]

Because enforcement of the CCPA has only begun on July 1, 2020, we have yet to see how the Office of the Attorney General of the State of California ("OAG"), which has the sole authority to bring an enforcement action under the law, interprets this provision. According to the Frequently Asked Questions that were published by the OAG, "Businesses cannot deny goods or services, charge you a different price, or provide a different level or quality of goods or services just because you exercised your rights under the CCPA."[4] This does not mean, however, that consumers have an unlimited right to non-discrimination without consequences.

---

2 There was debate in the past on whether the goals of antitrust and intellectual property law were incompatible or complimentary. See U.S. Dep't of Justice & Federal Trade Comm'n, Antitrust Enforcement and Intellectual Property Rights: Promoting Innovation and Competition (2007), available at https://www.ftc.gov/sites/default/files/documents/reports/antitrust-enforcement-and-intellectual-property-rights-promoting-innovation-and-competition-report.s.department-justice-and-federal-trade-commission/p040101promotinginnovationandcompetitionrpt0704.pdf.

3 See Cal. Civ. Code § 1798.125 (a) (1) (A-D) (2018).

4 California Consumer Privacy Act (CCPA), State of California Department of Justice, https://oag.ca.gov/privacy/ccpa#sectionf (last visited Aug. 31, 2020).

The OAG provides two examples of potential consequences: (1) "if you refuse to provide your personal information to a business or ask it to delete or stop selling your personal information, and that personal information or sale is necessary for the business to provide you with goods or services, the business may not be able to complete that transaction";[5] or (2) "[i]f you ask a business to delete or stop selling your personal information, you may not be able to continue participating in the special deals they offer in exchange for personal information."[6] Not being able to complete the requested transaction or not allowing customers to participate in special deals, however, are often not the desired outcome for businesses, so how can businesses offer promotions, discounts and other deals in exchange for collecting, keeping or selling your personal information?

The CCPA provides certain exceptions to the general prohibition on discrimination. Businesses may charge different prices or offer different levels of service if the difference is "directly related to the value provided to the business by the consumer's data."[7] The CCPA also permits businesses to offer financial incentives — including payments to consumers as compensation for the collection, sale, or deletion of personal information — as long as the programs are not "unjust, unreasonable, coercive, or usurious in nature,"[8] and if businesses notify consumers of these financial incentives, obtain opt-in consent prior to enrolling a consumer in a financial incentive program, and provide consumers with the opportunity to revoke consent for such programs at any time.[9]

This has generally been interpreted to mean that the CCPA was intended to allow businesses to offer tiered pricing or service levels so long as the financial incentive or price or service difference is reasonably related to the value of the consumer's data. However, any business that is seeking to rely on this exception must first calculate a good-faith estimate of the value of the consumer's data or show that the tiered pricing or service levels are reasonably related to the value of the consumer's data. For example, this means companies need to prepare a good faith estimate of the value of the data that is the basis for the financial incentive, price difference, product difference, or service difference that they may offer to consumers in order to incentivize them to not exercise their right to opt-out from the sale of their personal information. Companies will also need to describe the methodology they are using to calculate that value.

III. NOTICE OF FINANCIAL INCENTIVE UNDER THE CCPA

Because in a data economy, the volume, accuracy, and integrity of a data set are important drivers for calculating the value of a certain data set, businesses may be motivated to discourage any consumer actions that would result in the data not being as complete as it can be. Once a business identifies a data processing activity that may be a sale under the CCPA, it may incentivize consumers to not exercise his or her consumer rights, including the right to opt-out or the right to delete, by offering a financial incentive.

Although the right to non-discrimination is not solely about the consumer's right to opt-out, much debate about this new privacy right has centered around what it means to "sell" personal information under the CCPA and from what data sets a consumer may opt-out. Under CCPA, "sell," "selling," "sale," or "sold," are defined as "selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other valuable consideration."[10] Given this broad definition, it is possible that many "use case" scenarios involving the transfer of data from one party to another may constitute a sale, and thus be subject to the consumer's right to opt-out from such sale of personal information.

To incentivize a consumer to not opt-out, businesses may provide financial incentives. A notice of financial incentive must be provided to consumers before they opt-in to any "financial incentive" program, benefit, or other offering that is related to collection, retention, or sale of personal information. For example, businesses that want to incentivize consumers to not opt-out, payment in the form of customer loyalty points, coupons, or discounts may be offered.

The financial incentive notice must include all information a consumer would want to know before consenting to participate in such a program, specifically:

5 *Id.*

6 *Id.*

7 See Cal. Civ. Code § 1798.125 (b)(1) (2018).

8 See *id.* § 1798.125 (b)(4) (2018).

9 See *id.* § 1798.125 (b)(2) (2018).

10 See Cal. Civ. Code § 1798.140(t)(1) (2018).

- A succinct summary of the financial incentive or price or service difference offered;
- A description of the material terms of the financial incentive or price or service difference, including the categories of personal information that are implicated by the financial incentive or price or service difference and the value of the consumer's data;
- How the consumer can opt-in to the financial incentive or price or service difference;
- A statement of the consumer's right to withdraw from the financial incentive at any time and how the consumer may exercise that right; and
- An explanation of how the financial incentive or price or service difference is reasonably related to the value of the consumer's data, including:
    1. A good-faith estimate of the value of the consumer's data that forms the basis for offering the financial incentive or price or service difference; and
    2. A description of the method the business used to calculate the value of the consumer's data.[11]

The requirement that companies explain how the financial incentive or price difference is reasonably related to the value of the consumer's data is an important one. This is for two reasons. First, the explanation is part of the notice requirement, which ensures transparency so that a consumer can make an informed decision about whether to accept the incentive. Second, the explanation is needed to ensure that the company can meet the non-discrimination requirement. Specifically, a company cannot treat a customer differently based on whether he or she is opting in or out of the sale of personal information. Both requirements are met if a company can show that the financial incentive (or the product that has a price or service difference) that is offered for the collection or disclosure of consumer information is reasonably related to the value of the consumer's data.

IV. THE TERMS OF THE FINANCIAL INCENTIVE AND THE PRICE OR SERVICE DIFFERENCE OFFERED FOR THE DISCLOSURE OF CONSUMER DATA

Once a business has determined that it seeks to provide a financial incentive for the collection and use of personal information, the incentive offered can be structured in a number of different ways. For example, a company could offer a premium service for $5 per month where users who elect to pay the $5 premium would be able to opt-out from the sale of their personal information, as long as the business can show that the $5 per month payment is reasonably related to the value of the consumer's data to the business. Another type of incentive is a loyalty program where a company might offer a $5 coupon or discount for purchases of $100 or more. The coupon or discount could be expressed as a percentage discount (e.g. a five percent discount off the price paid) or a dollar amount ($5 off of a $100 purchase). For consumers who join a loyalty program where the personal information is necessary in order for the consumers to enjoy the benefits (e.g. email address and transaction history to provide loyalty benefits), the consumer's request for deletion maybe denied by the business, as long as the information is necessary for the business to provide the loyalty program requested by the consumer and is reasonably anticipated within the context of the business's ongoing relationship with the consumer. Indeed, these are two of the examples that appear in the regulation itself.[12] Complying with the regulation will be no easy task for businesses.

Even if it is relatively easy for a company to describe the terms of the financial incentive initially, changes in the marketplace or consumer behavior may make it difficult for the company to describe specifically what those terms are, particularly given certain unknowns. A company may not know in advance how many coupons or discounts it will offer, how many consumers will redeem those coupons or take advantage of those discounts, what types of discounts or coupons are most attractive to consumers, and whether and by how much the coupons and discounts were successful in generating new sales and ultimately, where and how much new revenue was generated by the sale of that data. Moreover, depending on the volume, accuracy and integrity of the data set at large, the value of the individual consumer's data to the business also may change as a result of market dynamics. Yet the regulation appears to require the company to describe with some reasonable certainty how the financial incentives and any price and service difference offered might be related to the value of the consumer's personal information that the company may collect, sell, or retain.

11 Cal. Code Regs. § 999.307(b)(1)-(5).

12 See Cal. Code Regs. § 999.336(d).

To estimate the value of any proposed financial incentives and price or service differences, companies may need to draw on market studies, their prior experience with coupons, and other market data that may shed light on the effectiveness of discounts in promoting sales and the use of coupons by consumers of similarly-situated companies, as well as any revenues and expenses related to the collection and sale of personal information.

V. ESTIMATING THE VALUE OF CONSUMER DATA

The regulations offer a number of considerations that a company may use to calculate the value of consumer data to the company. These factors include:

- The marginal, average, or aggregate value to the business of the data collected, sold, or deleted;
- The revenue generated by the business from the sale, collection, or retention of consumers' personal information;
- The expenses that the business may incur in connection with the sale, collection, or retention of the data or with the offer or provision of any financial incentive or price or service difference; and
- The profit generated by the business from the sale, collection, or retention of consumers' personal information.[13]

While these factors may appear straightforward at first blush, there are a number of considerations that may come into play as previewed above. First, the value of an individual consumer's personal information may depend on what other data are being collected. For example, if the data are being sold, the value of an individual's personal information may not be all that important by itself, but important when aggregated with other individuals' data. It is also important to think about the different types of data that could be collected. The collection of email addresses is likely to be more valuable if there is associated data on consumers' home or work zip code location, income category, or age, but less valuable without such data. Thus, it may not be enough for businesses to consider the value of the specific piece of personal information that will be collected by this one particular data processing activity. Businesses also may need to think about how this specific piece of data will be combined with other databases, either internally to be used by the same business or transferred to a third party to be used for a different purpose.

This brings us to our second point. The value of having the data will depend on how the data are used. For example, if the data collected are to be sold to an advertiser, the value may well depend on the value of the data to that advertiser, and the company selling that data may not know this value at the time of data collection. The value of the data to be sold could easily vary from one advertiser to another, based on which other sources of data are available to the advertiser at the time of the sale and which other advertisers are in the market for the company's consumer data, among other factors. How much an advertiser is willing to pay for the company's data will affect the price that the company will be able to charge for access to its data, and as the questions above indicate, determining the revenues that the company may earn from selling or licensing its personal data may involve an inquiry into the nature of the personal data being sold and the market in which its buyers of the company's data may operate.

Third, the regulation asks for the value of the data to the business from selling, collecting, or deleting the data. Consider, for example, the value associated with collecting personal information on one more consumer versus the value associated with deleting that consumer's personal information. These values may be the same if the individual's data are sold to an advertiser with many other consumers' data. But if the company is in the business of selling a product or service to the consumer, it is possible that the added value of obtaining a new consumer's information is higher than the loss in value associated with deleting that consumer's information. In the case of gaining consumer information, the company could well be gaining a new customer. In the case of deleting consumer information, the company may have lost that person's data, but there may be no loss in sales if the expectation is that the consumer is likely to continue purchasing products or services from the company.

Fourth, the regulation suggests that the company may consider the costs incurred by the company to collect, sell, or retain the data, or to offer the financial incentive or price or service difference when estimating the value of consumer data. For many companies, these costs are likely to be comprised of IT, marketing, and other fixed costs that do not significantly vary depending on how many consumers are served by the company and how many consumers opt-in or opt-out of providing consumer information. In these circumstances, costs may not be useful in determining the value of the consumer's information to a company, particularly when thinking about the value of any particular individual's data. However, it may be useful to consider the incremental cost associated with collecting and selling a larger increment of personal data (e.g. data on consumers in a new city or state or new data that had not been collected before), the incremental cost associated with generating an

13 See *id.* § 999.337(a).

appropriate incremental increase in sales, and/or the incremental cost associated with producing the content that may be available in a premium content offering.

The profit generated by holding or selling consumer data is another factor that may be useful in calculating the value of consumer information. In addition to the complexities associated with estimating the incremental sales revenue associated with collecting or selling the data or the revenue associated with offering the incentive, consideration should be given to the complexities that can arise when assessing the relationship between terms of a financial incentive and profitability.

The relationship may be straightforward in certain cases. Suppose a consumer pays $5 per month for a premium product in order to opt-out of the sale of personal information. This would generate an incremental profit of $5 per month to the company if there is little or no marginal cost associated with serving that one additional consumer. The $5 per month fee for the premium product might make sense if the company is able to sell access to its consumer data for $5 per consumer per month, so the justification for the $5 fee would be the opportunity cost of not being able to sell that consumer's data. However, the scenarios below highlight some of the issues are likely to complicate the justification for the $5 fee:

- Scenario 1: Suppose the company faces competition from a new rival that is also selling its consumer data. As a result, the company discovers that it cannot continue selling its data at a price of $5 per consumer per month. Instead, the company has to lower the price to $3 per consumer per month. But the company continues to charge consumers $5 per month for its premium product because the value of the premium product and the cost of producing content for the premium product has not changed. In other words, will businesses be expected to have dynamic pricing where the cost of a premium service to consumers change based on the ups and downs of the cost to purchase that piece of personal information in the data marketplace? Is it sufficient if that change in price is reflected after periodic review (i.e. annually) or will consumers be able to make a claim that businesses need to offer real-time pricing?

- Scenario 2: Suppose a company that offers a free product decides to introduce a premium product for $5 per month. However, after it introduces its premium product, the company discovers that many of the consumers who were using the free product begin purchasing the premium product. As a result, the company has less data to sell because more of its consumers are buying the premium product and opting out of disclosing their personal information. Because fewer consumers are opting into disclosing their data, advertisers are only willing to pay $3 per consumer per month for the data. With the reduction in the price that the company can charge for its data, is the $5 fee for the premium product still reasonably related to the value of the data collected and sold? What analyses would the company need to do to assess this question?

Complexities also may arise in the situation where a business may have to change the terms of the financial incentives that it offers to its consumers. For example, consider a company that is offering a five percent discount to consumers who are members of its loyalty program (for which they have agreed to disclose their personal information).

- Scenario 3: Suppose the company faces additional competition from the entry of a new rival. In response to that entry, the company decides its best approach is to increase the percentage discount that it offers to its loyalty program members from five percent to ten percent. Suppose, however, that the revenues that the company can generate by selling its consumer data has not changed — the number of loyalty members did not change and the amount and type of data collected by the company did not change. The only change was the increase in the financial incentive that the company is offering its members. After the increase in the percentage discount offered to consumers, is the financial incentive still reasonably related to the value of the data collected and sold?

- Scenario 4: Suppose a retail store discovers that its loyalty program customer retention rates and purchase volume per person over a three-year period are not much different from the customer retention rates and purchase volume per person that the retailer experienced before introducing its loyalty program. As a result, the retailer decides that it may be able to improve customer retention rates by offering additional financial incentives. However, because the data collected and sold by the retailer has not changed, the revenues generated by the retailer for its data has not changed. With the introduction of the new financial incentive, is the amount of the financial incentive still reasonably related to the value of the data?

These scenarios illustrate how competition and market dynamics may make the relationship between the financial incentive (or price and service difference) offered and the value of the data more complex. Scenarios 1 and 2 highlight situations where a company has not lowered the price that it is charging its premium service customers, even though the personal data of these customers has become less valuable to parties interested in purchasing or getting access to the company's data. Scenarios 3 and 4 highlight situations where the company may appear to

be offering greater discounts to encourage consumers to disclose their personal data when, in fact, the change was motivated by competitive reasons. In all four scenarios, it was a change in market conditions that led to either a change in the value of the data or a change in the terms of the financial incentive (or price or service difference) offered. Indeed, because competitive conditions in the market for the consumer data sold by the company may not be linked to competitive conditions in the company's product or service market, complying with the regulation may require the company to explain the nature of competition and pricing in multiple markets — the market(s) for which the data may be used and the market(s) in which the company competes.

On the surface, explaining how a financial incentive or price or service difference is related to the value of the consumer's data may seem complex, but it is similar to economic and business analyses that companies undertake in the ordinary course of business. Companies set and adjust the prices of their various products all the time. A company that sells a low-end, mid-range, and high-end product will have to choose the price of each product based on costs, supply, demand, and other competitive market conditions. Companies also study the relationship between their marketing incentives and outcomes all the time. When complexities arise, evidence from these economic and market studies may be more important as part of the compliance process.

VI. CONCLUSION

The CCPA is new and compliance with the regulation raises complex legal and economic issues. This is particularly true with respect to the non-discrimination requirement in the law, which allows companies to offer tiered pricing or service levels along with the opportunity to opt-in or opt-out of providing consumer information as long as they can explain how the financial incentive or price or service difference is reasonably related to the value of the consumer's data.

The regulation recognizes the basic issues that companies have to address, which is that companies have to (a) explain the terms of the financial incentive or price or service difference; (b) calculate the value of the consumer's data; and (c) explain how the two are reasonably related. On the surface, this may seem straightforward, but in practice, the terms of the financial incentive may not be easy to explain, particularly if there are unknowns that relate to how often the incentives will be given, how much the incentive will be, how frequently a discount or coupon will be redeemed, or what data the business is collecting and what it's worth.

There are challenging economic issues that companies must address when they explain how the financial terms that are being offered relate to the value of the consumer data collected. First among these issues is the need to consider the effect of market conditions and competition on the value of the data to the company, the financial terms offered to consumers, and the revenues that a company may earn from the data they collect. Value and price are complex economic concepts and they are central to the compliance process. For example, there is the price of the data sold and the price of a premium product that a company may charge consumers along with the option to opt in or opt out of disclosing personal information. The regulation would seem to require that these two elements be reasonably related, yet the underlying factors that determine the price at which a company may be able to sell its data may be quite different from the factors that determine the price that the company may have to charge its consumers for opting into a loyalty program or some premium product. These are challenging issues because in today's competitive, dynamic, and fast-moving markets, market changes could easily affect both the value of the data to the company and the financial terms that a company may need to offer consumers who want to participate in a loyalty program or purchase a premium product. As the CCPA has become law, these are issues that companies must be prepared to navigate.

More broadly, these pricing-related data issues will only broaden the intersection of privacy law and antitrust law. For example, questions related to nascent competition, the acquisition of data in adjacent markets, data grabs, and the role of data in potentially facilitating collusion are all examples of ways the lines between antitrust and privacy objectives and thus enforcement are increasingly becoming blurred.[14]

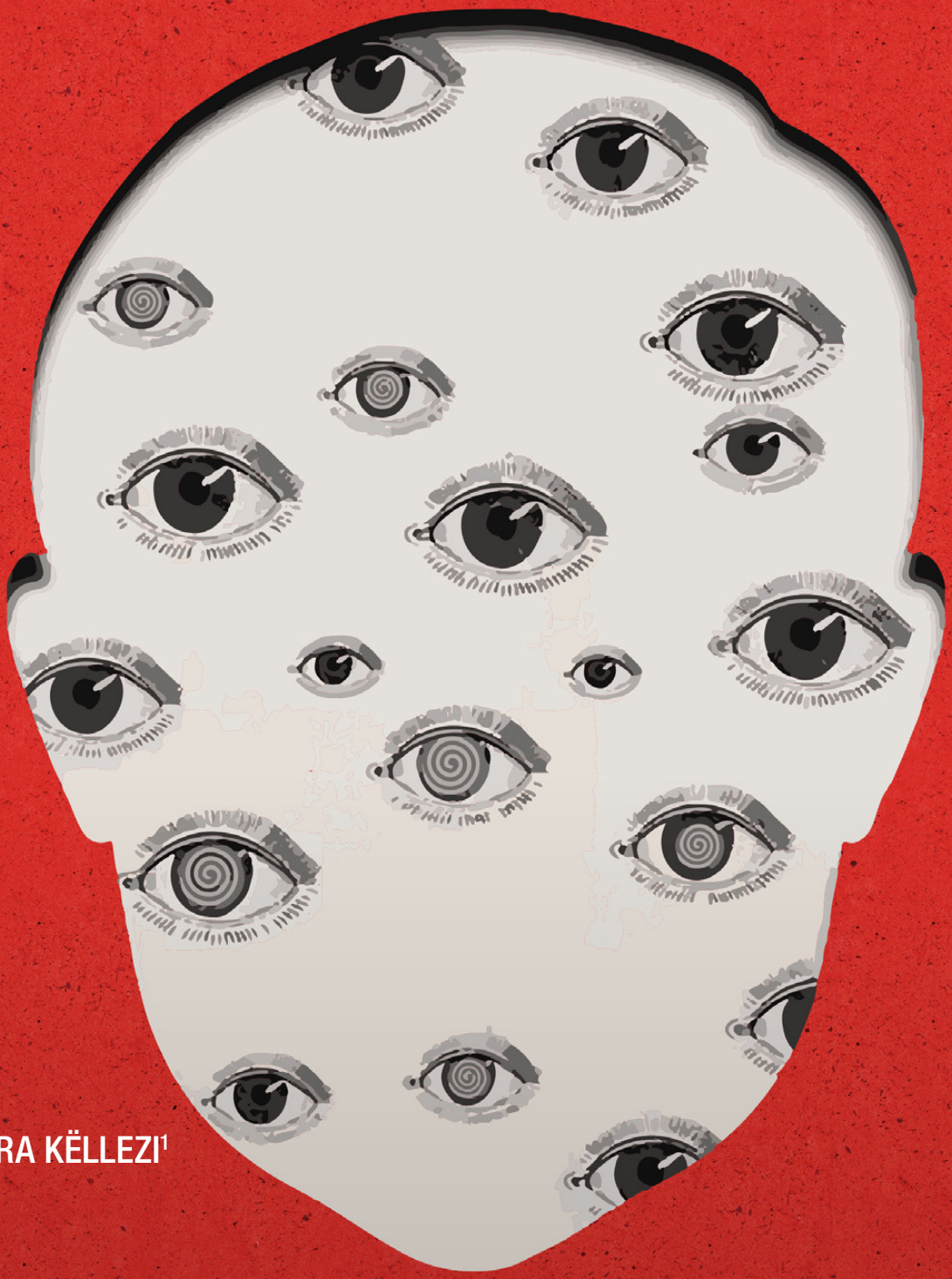
California Attorney General Xavier Becerra stated in his press release while announcing the approval of the Final Regulations that "privacy is an inalienable right" and "Californians should control who possesses their personal data and how it's used."[15] By requiring businesses to provide notice and obtain opt-in consent if they wish to offer a different price, rate, level, or quality of goods or services to the consumer based on the collection and use of personal information, the CCPA in essence becomes a first-of-its-kind law that requires businesses to calculate and disclose the value of the consumer's data. This step of calculating the value of the consumer's data is an important one, but it will be a complex undertaking due to the interrelationships that touch on consumers' right to privacy and non-discrimination under the CCPA, the need for busi-

14 See generally Alyse F. Stach, Ann M. O'Brien & Jeewon Kim Serrato, *The thin line between privacy and antitrust*, The Privacy Advisor, IAPP (June 23, 2020), https://iapp.org/news/a/the-thin-line-between-privacy-and-antitrust/.

15 Press Release, State of California Department of Justice, Attorney General Becerra Announces Approval of Final Regulations under the California Consumer Privacy Act (Aug. 14, 2020), https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-approval-final-regulations-under-california.

nesses to compete and to be able to price and market their products in response to market conditions, and the revenues that a company may be able to earn by collecting, selling, and retaining consumer data. The first step to interrogating the value of consumer's data may need to begin with the businesses understanding what data they collect, retain or sell.

CONSUMER CHOICE AND CONSENT IN DATA PROTECTION



BY PRANVERA KËLLEZI[1]

1 Attorney at law, Geneva, Switzerland, CIPP/E, CIPM; member of the Swiss Competition Commission. The author expresses her personal opinion, which in no way engages the Swiss Competition Commission or its Secretariat.

I. INTRODUCTION

Consumer choice and consent go together in data protection, where the consumer has a choice when it consents on how the data are collected and processed. Express or implied, opt-in or opt-out: these requirements are there to qualify consent and consequently determine the choice of the consumer. Granularity of consent gives more choice to consumers on the collection and processing of their data. By contrast, strict conditions on the validity of consent reduce the ability of the consumers to consent and therefore their choices.

Consumer choice between substitute products makes competition work. Consumers benefit from a wider choice of new or improved goods and services in a competitive market. Choice depends on what is offered on the market, and what products are available to the consumer. To preserve the offer on the market, competition enforcement is focused on how the markets work, not on the conditions under which a product is put on the market.

Consumer choice and self-determination are important aspects in competition law and data protection. On what account may competition or data protection increase or decrease consumers' choice? And independently of the justification, what is the impact of regulation on consumer choice? This brief paper is an attempt to go beyond legal semantics to articulate the mechanisms and consequences of a consumer choice entitlement, focusing on the GDPR and with a few references on the CCPA.

II. THE REQUIREMENT OF LEGAL GROUNDS FOR COLLECTION AND PROCESSING

One of the special features of the GDPR[2] is that it authorizes the collection and processing of personal data only for a limited number of legal grounds provided by law, the relevant legal grounds for businesses being consent, contract, and legitimate expectation.[3] Personal data collection and processing outside those legal grounds is unlawful. Consent is the expression by excellence of consumer choice. Contract too incorporates consumer consent, since the consumer consents to the contract and its general terms. However, consenting to a contract is not the same thing as consent as a separate legal basis to the processing of personal data.[4] If the contract does not justify the collection and processing of personal data, the business can use the legal basis of consent or legitimate interest. The consumer can, however, withdraw consent at any time, which makes this legal ground an unstable basis to grow a business. Legitimate interest, on the other hand, cannot override fundamental consumer rights and is, therefore, a rather narrow justification.[5] Restricting the use of contract as a legal basis has, therefore, far-reaching consequences. The scope of the three legal grounds is construed narrowly, which runs the risk of making unlawful the collection and the processing of personal data. From a consumer perspective, this comes down to fewer opportunities to consent to the collection and processing of data in exchange for services.

Collection and processing of personal data under the GDPR must satisfy other general principles, the most important being data minimization: personal data collected must be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.[6] This requirement further restricts the scope of the above-mentioned legal bases.

By contrast, the CCPA does not provide a list of legal grounds.[7] Companies must inform consumers of the purposes of collection and processing in a privacy notice; only the collection and the processing of personal information that does not respect the purposes defined by the business itself in the notice would be considered as a deceptive practice and therefore unlawful. Under CCPA, information is key and that is what makes the consumer decide whether to enter a contract or consent to the collection of personal information. Consent is regulated, however, in relation to specific use of data, such as the transfer, sharing, or sale to third parties.

2 Regulation 2016/679 of the European Parliament and of the Council of April 27, 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

3 See article 6 GDPR.

4 Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0 of October 8, 2019, para. 20.

5 Article 6 (f) GDPR reads "processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child."

6 Article 5 (c) GDPR.

7 Privacy laws in the United States are generally based on tort and the harm principle. There is no need for a specific legal ground to collect data. CCPA only requires the consent in the form of opt-out for the sale of data, not for the collection of data. In November 2020, California approved a revised version (CPRA, see Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021).

III. CONSUMER CHOICE AND RULES ON THE VALIDITY OF CONSENT

The GDPR defines consent as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her."[8]

Consent should be freely given, and this is not the case if the consumer faces detriment.[9] Detriment covers any cost or disadvantage for the consumer that refuses or withdraws consent.[10] Downgrading services is a form of detriment and is not allowed,[11] but not sending personalized discounts or offers is not a disadvantage, since the refusal of consent does not impede the consumer from getting the product itself.[12] Detriment is therefore the mere denial of the service requested by the consumer.

In relation to the conclusion of a contract, Article 7 GDPR adds further conditions on the validity of consent. First, it conditions how to include consent in contractual documentation: if consent is included in general terms and conditions, "the request for consent shall be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language."[13]

Second, the provider cannot bundle consent for non-necessary personal data with the conclusion of a contract for a product.[14] While consent to contract implies consent to collection and processing of personal data objectively necessary for the performance of the contract,[15] contract cannot serve as a basis to collect and process non-necessary data; the consumer must, therefore, consent separately to their collection and processing.[16] In other words, the contractual conditions or general terms cannot bundle necessary personal data for the performance of a contract and personal data that are not necessary for the performance of that contract. The following examples are considered in EDPB Guidelines:

- A mobile app for photo editing collects GPS localization activated for the use of its services and for behavioral advertising purposes, which advertising is not necessary for the provision of the photo editing service. Since users cannot use the app without consenting to behavioral advertising, the consent cannot be considered as being freely given.[17]

- Website provider blocks access to the website content if consumer refuses cookies. Since the data subject is not presented with a genuine choice, the consent is not freely given.[18]

The "inappropriate pressure or influence"[19] comes from the refusal to provide the service or a certain functionality to the consumer. The absence of freely given consent is, therefore, transformed into an obligation to give access to a product, and in a corresponding "right" for the consumer to have that functionality or that product, or a "genuinely equivalent" one, from the same provider.[20] In other words, the company cannot refuse

8 Article 4(11) GDPR.

9 GDPR, recital 42: "Consent should not be regarded as freely given if the data subject has no genuine or free choice or is unable to refuse or withdraw consent without detriment."

10 EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020, paras. 46ff.

11 *Idem*. para. 48.

12 See examples given at paras. 50 to 54 of EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020.

13 Article 7(2) GDPR. See also Recital 42: "In particular in the context of a written declaration on another matter, safeguards should ensure that the data subject is aware of the fact that and the extent to which consent is given. In accordance with Council Directive 93/13/EEC [of April 5, 1993 on unfair terms in consumer contracts] a declaration of consent pre-formulated by the controller should be provided in an intelligible and easily accessible form, using clear and plain language and it should not contain unfair terms."

14 Article 7 (4) GDPR. See also Recital 43: "Consent is presumed not to be freely given […] if the performance of a contract, including the provision of a service, is dependent on the consent despite such consent not being necessary for such performance."

15 "Objectively necessary" means that the provider cannot decide on its own that certain data are necessary by simply mentioning them in the privacy notice or the terms of the contract. See Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0 of October 8, 2019, para. 27: 'Necessary for performance' clearly requires something more than a contractual clause."

16 Or the company must assess whether the collection and processing is covered by legitimate expectations legal ground.

17 EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020, para. 15.

18 *Idem*. paras. 40 and 41.

19 *Idem*. para. 14.

20 *Idem*. para. 37.

premium features or functionalities because the consumer refused the collection or processing of personal data, which also means that the consumer cannot pay with its data for premium features.

The fact that consumers can choose another equivalent service available in the market does not change the conclusion: the consumer is deemed to be disadvantaged by the refusal of a specific service, even though there is sufficient choice of equivalent (or substitute) products in the market.[21] In the end, the condition of "freely given" aims to grant consumers access to services and functionalities.

CCPA includes a right for consumers not to be discriminated against because of exercising their rights. What is of relevance for us is the right to request that personal data not be sold to third parties.[22] The right not to be discriminated against is, therefore, limited to consumers rights and to a type of processing of personal data, and not related to the ability to collect personal data by the business. While the CCPA used ambiguous language on the prohibition of discrimination, the newly adopted CPRA makes explicit that non-discrimination provisions do not prohibit a business from offering premium features in exchange for personal data.[23] In other words, consumers may pay with their data.

The issue in the GDPR lies in the very idea expressed in Article 7 (4) GDPR: businesses and consumers do not benefit from the contractual freedom in relation to personal data considered *not necessary* for the contract. The Advocate General's opinion in *Planet49* is an attempt to resolve the issue by construing widely what data are *necessary*.[24] Taking into account that the prohibition of bundled consent is not absolute, the Advocate General considered that, since the provision of personal data constitutes the user's main obligation to be able to participate in a service (a promotional game), the processing of such personal data by third-party companies (sponsors) should be considered as *necessary* for participation in the service, which in turn makes consent valid.[25] In other words, consumers can "pay" with their data. It is in the end the only sustainable solution to enable consumers to benefit from free services and functionalities, and to broaden their choice.

21 *Idem*. para. 38. EDPB disagrees with the Italian Supreme Court which ruled that Article 7 para. 4 GDPR does not apply if the service is not essential and other interchangeable services exist on the market; in such a case, consent to the general terms of use is valid. See Judgment of the Italian Supreme Court of July 2, 2018, 17278/2018.

22 CCPA or Cal. Civ. Code § 1798.125 entitled "Consumers' Right of No Retaliation Following Opt-Out or Exercise of Other Rights," whose para. (a) (1) reads "A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, Including, but not limited to, by: (A) Denying goods or services to the consumer. (B) Charging different prices or rates for goods or services, Including through the use of discounts or other benefits or Imposing penalties. (C) Providing a different level or quality of goods or services to the consumer. (D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services."

23 Amendments to The California Privacy Rights and Enforcement Act of 2020, Version 3, No. 19-0021, § 1798.125 on Consumers' Right of No Retaliation Following Opt-Out or Exercise of Other Rights, was amended to add § 3 "This subdivision does not prohibit a business from offering loyalty, rewards, premium features, discounts, or club card programs consistent with this title." § 1798.125 already included a provision on financial incentives: "A business may offer financial incentives, including payments to consumers as compensation, for the collection of personal information, the sale or sharing of personal information, or the *retention* of personal information. A business may also offer a different price, rate, level, or quality of goods or services to the consumer if that price or difference *reasonably* related to the value provided to the *business* by the consumer's data." (amendments in italics)

24 Opinion of Advocate General Maciej Szpunar in case C-673/17 (*Planet49 GmbH*) of March 21, 2019, pt 98. The ECJ judgment of October 1, 2019 in this case does not address the issue (C-673/17, pt 64).

25 Opinion of Advocate General Maciej Szpunar in case C-673/17 (*Planet49 GmbH*) of March 21, 2019, pt 99. The scope of the offer on the market was not relevant for its analysis.

IV. WHAT ARE THE IMPLICATIONS FOR CONSUMER CHOICE?

The strict interpretation of Article 7 (4) GDPR and consent means that individuals cannot "pay" with personal data considered as unnecessary for the service or functionality provided.[26] The main concern here is the use of personal data by the consumer to have more functionalities and services, which is expressed in the form of denial of services that consumers have requested.[27]

Starting from self-determination, with the aim of giving consumers control on their own personal data, the rules on consent are transformed in a regulation that gives consumers a kind of – virtual or shadow – right to specific functionalities or services, and not only without paying, but also prohibiting them from paying. This might look like an increase in consumer choice (and welfare). However, good economic principles tell us that functionalities or services of good quality cannot be free: the provider will either increase the price of the services or will not make available additional functionalities or services for cheap products. The ability for consumers to benefit from quality or price discrimination is also reduced. In all cases, consumer choice (and welfare) seems to be degraded, not improved.

V. CONSUMER CHOICE, AND THE CRITERION OF DOMINANT POSITION IN DATA PROTECTION

One of the proposals to further restrict the ability of businesses to collect and process personal data is to use the criterion of dominant position. In one decision of a European competition authority,[28] the dominant position of the controller was used to disqualify the application of any legal ground (consent, contract or legitimate interest) for a particular type of data processing. Under this proposition, it would become more difficult for consumers to consent or conclude a contract with dominant companies in exchange for the collection and processing of personal data. As a result, dominant companies will find it more difficult to expand their services based on the collection of personal data, and their market power would allegedly be reduced.

But the main problem with that strategy is that consumer choice is reduced, too. If the consumer finds the services of the dominant company useful, every hurdle on the business model of the dominant company also has a negative impact on consumer choice.

Forcing dominant companies to comply with GDPR under the threat of competition law fines can also raise barriers to other privacy-enhanced products: why would consumers turn to a product that better respects their privacy and their personal data, when competition law forces dominant undertakings to do the same? As with price caps, forcing dominant companies to improve their data protection practices only makes it more difficult for other competitors to offer more and enhanced privacy-friendly products. Challenging dominance will, therefore, take more time.

Reducing consumer choice to reduce the market power of companies is not a measure envisaged by competition law. Offering a right to obtain a product is also not a legitimate measure under competition law. Consumer choice expresses the choice consumers have among various substitute products. It is a simple component of the demand side of final consumers. More choice means consumers will be able to choose the best and the cheapest products in a relevant market, but it does not mean that the consumer has the right to shape the product, nor that it can force the producer to conclude a deal. Neither competition law, nor consumer or contract law, offers that remedy.

26 EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020, paras. 26 and 27: "In doing so, the GDPR ensures that the processing of personal data for which consent is sought cannot become directly or indirectly the counter-performance of a contract. The two lawful bases for the lawful processing of personal data, i.e. consent and contract cannot be merged and blurred." EDPB goes on to say that "there is a strong presumption that consent to the processing of personal data that is unnecessary, cannot be seen as a mandatory consideration in exchange for the performance of a contract or the provision of a service." See also Guidelines 2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects, Version 2.0 of October 8, 2019, para. 54 and its footnote 30, where the EDPB explains that processing of personal data is conceptually different from monetary payments, since "money is countable, meaning that prices can be compared in a competitive market, and monetary payments can normally only be made with the data subject's involvement. Furthermore, personal data can be exploited by several services at the same time. Once control over one's personal data has been lost, that control may not necessarily be regained."

27 EDPB Guidelines 05/2020 on consent under Regulation 2016/679 of May 4, 2020, para. 28: "Hence, whenever a request for consent is tied to the performance of a contract by the controller, a data subject that does not wish to make his/her personal data available for processing by the controller runs the risk to be denied services they have requested."

28 For a discussion of the Facebook decision, see Pranvera Këllezi, Data protection and competition law: non-compliance as abuse of dominant position, *sui-generis* 2019, p. 343.

There can be circumstances in which consumer choice is a criterion of intervention that forces dominant companies to offer separately an additional product or functionality, such as in tying cases. Since lack of consumer choice is a criterion of tying, the remedy under competition law is forcing the dominant company to offer separately each of the separate products, in addition to offering the bundle.[29] In this case, competition law intervenes at the offer side, not by prohibiting the bundle, but by forcing the company to offer the individual components separately as an additional offer. In all cases, the intervention criterion is not the consumer choice, but the anti-competitive effects on competition. It is the anti-competitive effect of the practice that impairs the competitive process.

Finally, the text of the GDPR does not mention the choice or availability of competing products to judge whether consent was freely given. It does not refer to market power, dominance or monopoly; it refers only to the concept of "clear imbalance between the data subject and the controller," giving the example of public authorities.[30] In addition, a concentrated market may limit the choice of products available when concluding contracts, but the market structure does not determine the business model based on the collection and processing of personal data: in other words, the removal of the dominant position will not bring a business model into line with the GDPR, nor will it remove any imbalance in contractual relations. In the end, it seems to us that using dominant position to narrow down the scope of legal grounds is neither efficient nor desirable from the consumer's perspective.

VI. ARE GDPR AND COMPETITION LAW INCREASING CONSUMER CHOICE?

The adoption of GDPR has dramatically improved the situation in Europe in relation to the collection and processing of personal data. We see now additional services specifically designed to offer consumers a higher degree of data protection and privacy. The choice for consumers is offered by these additional services that not only give individual consumers more privacy but also introduce more competition in the market by focusing on privacy as a distinct product feature. The trend is supported by consumer demand.

It is doubtful whether the same can be said of the general impact of GDPR on consumer choice. The very idea of a limited number of legal bases for the collection and processing of personal data has the potential to limit the range of products offered to consumers. In addition, strict conditions for the validity of consent and for contract as a legal basis reduce not only the ability of consumers to consent, but also their ability to trade their personal data for more services and features. This simply limits consumer choice. The fact that the regulation is justified on account of the fundamental rights and self-determination of individuals risks perverting the aims pursued by the very fundamental rights and delegitimizing public action.

The other proposition to restrict consumer choice in relation to the collection and processing of personal data by dominant companies uses consumers as a means to reduce market power. Yet the right to self-determination aims precisely at treating the individual as an end in itself, and not as a means to another end. In this respect, too, confusing data protection and competition laws may lead to a loss of legitimacy in the eyes of the consumer.

In view of the above, it seems to us that every general and comprehensive privacy law should be crafted to leave the consumer with a better choice. In general, every comprehensive data protection or privacy law must genuinely put the consumer at the center of the law and consider the impact of the legislation on consumer choice not only about its personal data but also by considering the broader choice that the consumer will have in terms of products or features. It is in the end the wider choice in terms of products that will empower the self-determination of the consumer.

29 See *Microsoft*, T-201/04, ECLI:EU:T:2007:289, paras. 864 and 1150. Consumer choice was also a criterion in the refusal to supply interoperability information to competitors of other competing products. See paras. 639, 652, 662, or 663.

30 Recital 43 of the GDPR. The GDPR explicitly regulates the case of public authorities in the performance of their tasks as a particular case of clear imbalance, to the point where public authorities cannot use the legitimate interest as a legal basis (Article 6 para. 1 GDPR, last sentence).

DATA REGULATION AND TECHNOLOGY VENTURE INVESTMENT: WHAT DO WE LEARN FROM GDPR?

BY JIAN JIA,[1] GINGER ZHE JIN[2] & LIAD WAGMAN[3]

1 This work was completed while Jian Jia was a doctoral student in finance at the Stuart School of Business, Illinois Institute of Technology, Chicago, IL. Email: jjia5@hawk.iit.edu.

2 Department of Economics, University of Maryland, Baltimore, MD. Email: ginger@umd.edu.

3 Stuart School of Business, Illinois Institute of Technology, Chicago, IL. Email: lwagman@stuart.iit.edu.

In a fast-evolving industry driven by technology, government policies have the potential to unleash innovation or create barriers that stifle market access. The stark contrast of these potential effects is particularly acute in data regulation.

On the one hand, data is a key input in technology-driven innovation and production. Data is also a key input in the matching processes between consumers and products, and is increasingly important for efficiently servicing consumers. On the other hand, data-driven operations have raised concerns about privacy intrusion and misuse of data without the knowledge or consent of the data source.[4] In response to growing consumer privacy concerns, the European Union began enforcing the General Data Privacy Regulation ("GDPR") on May 25, 2018, and the State of California rolled out the California Consumer Privacy Act ("CCPA") in 2020. Both regulations aim to enhance data protections.

These data regulations differ from their predecessors in important ways. First, the definition of 'personal data' has been arguably broadened to cover items ranging from pseudonymized data to advertising identifiers on consumers' phones. In addition, recent regulations have explored new mechanisms of enforcement, and included more significant penalties for violations. For instance, fines under the GDPR can be up to 4 percent of a firm's global annual revenue, and CCPA (specifically, Proposition 24) calls for the establishment of the California Privacy Protection Agency.

Data protections, however, entail tradeoffs. On the positive side, a strengthening of consumer privacy rights could offer some benefits to individuals who value privacy, data security, and the ability to more readily exercise control over personal data. On the negative side, restricting firms' access to data can result in outcomes that those same consumers do not like, such as higher prices (Taylor & Wagman, 2014).[5] To the extent that data regulations increase firms' compliance costs, existing economic theories also show that compliance costs can disproportionately impact nascent firms (Campbell et al., 2015)[6] and reduce new venture formation (Krasteva et al., 2015).[7]

In two recent papers, we empirically investigate whether a sweeping data regulation such as the GDPR has had an impact on technology venture investment and, thus, on current and future innovations (Jia et al., 2020a and 2020b).[8] From Crunchbase and VentureXpert, our dataset covers technology-oriented venture deals taking place between 2014 to 2019 in the EU, U.S., and the rest of the world (primarily comprising venture deals in Australia, Canada, China, Israel, India, Japan, Russia, and South Korea). Because GDPR was enacted in April 2016 and implemented in May 2018, our data includes 2+ years before the enactment, 2 years interim, and 1.5 years following the actual rollout of GDPR.

We find negative differential effects on EU ventures after the rollout of GDPR relative to their counterparts in the U.S. and in the rest of the world. The negative effects manifest in the number of financing rounds, which, after GDPR's rollout, exhibit a 26.1 percent reduction in the number of monthly venture deals by EU ventures compared to their U.S. counterparts. A comparison between EU ventures and their counterparts in the rest of the world not including the U.S. also points to a similar large negative effect. The negative effects are larger in the 6-month period immediately after GDPR's rollout in 2018, but some of them are sustained in 2019. Furthermore, our analysis suggests that consumer-facing ventures in the EU incur larger deal reductions than their business-facing counterparts, though deal reductions apply to both types of ventures.

One explanation is that the regulation may have introduced compliance costs and uncertainties for new technology ventures. For investors, GDPR may have increased due diligence costs with respect to EU venture deals, raising risks and uncertainty. And these costs may be particularly heightened for foreign investors who are less familiar with European institutions.

This latter concern is the focus of our second study, where we empirically investigate how an investor's home location interfaces with the effects of GDPR on investments in technology ventures (Jia et.al., 2020b).[9] To do so, we divide investors into three groups: group 1 refers to foreign investors, who belong not only to different states or countries, but also different unions (e.g. U.S. or EU); group 2 refers to investors in the same-union but different member states (e.g. California or New York in the U.S., and Germany or France in the EU); group 3 refers to domestic investors, who belong to the same member state. These three groups help capture a measure of "foreignness." Following Bertrand et al. (2004),[10] we use a difference-in-differences framework to compare technology venture investment activities in the EU, U.S. and the rest of the

4 Acquisti, A, C Taylor and L Wagman (2016), "The economics of privacy," *Journal of Economic Literature* 54(2): 442–492.

5 Taylor, C. & L. Wagman (2014), "Consumer privacy in oligopolistic markets: Winners, losers, and welfare," *International Journal of Industrial Organization* 34(1): 80–84.

6 Campbell, J., A. Goldfarb & C. Tucker (2015), "Privacy regulation and market structure," *Journal of Economics & Management Strategy* 24(1): 47–73.

7 Krasteva, S., P. Sharma & L. Wagman (2015), "The 80/20 rule: Corporate support for innovation by employees," *International Journal of Industrial Organization* 38(1): 32–43.

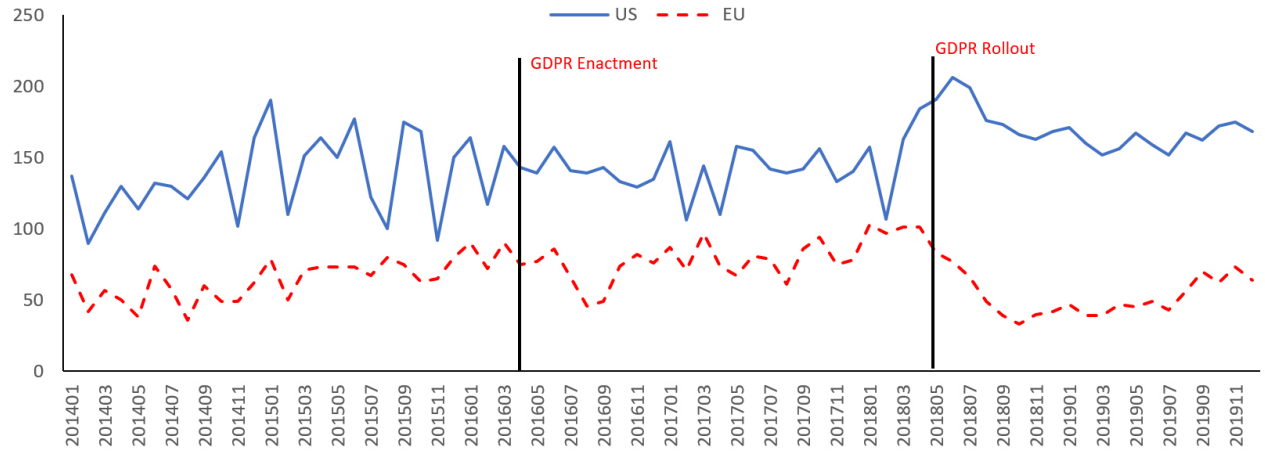
8 Jia, J., G. Z. Jin & L. Wagman (2020a), "The short-run effects of GDPR on technology venture investment," *Marketing Science*, forthcoming; Jia, J., G. Z. Jin & L. Wagman (2020b), "GDPR and the Localness of Venture Investment," SSRN working paper # 3436535.

9 Jia, J., G. Z. Jin & L. Wagman (2020b), "GDPR and the Localness of Venture Investment," SSRN working paper # 3436535.

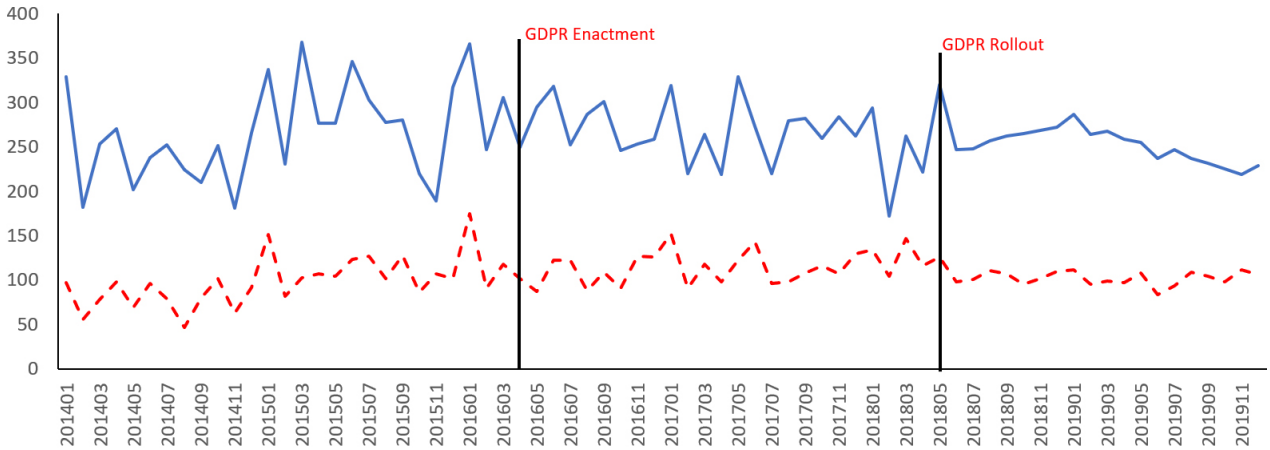
10 Bertrand, M., E. Duflo & S. Mullainathan (2004), "How much should we trust differences-in-differences estimates?" *Quarterly Journal of Economics* 119(1): 249–275.

world before and after GDPR. Put simply, we find that foreign investors pulled back from investing in EU technology ventures after GDPR, more than non-foreign investors.

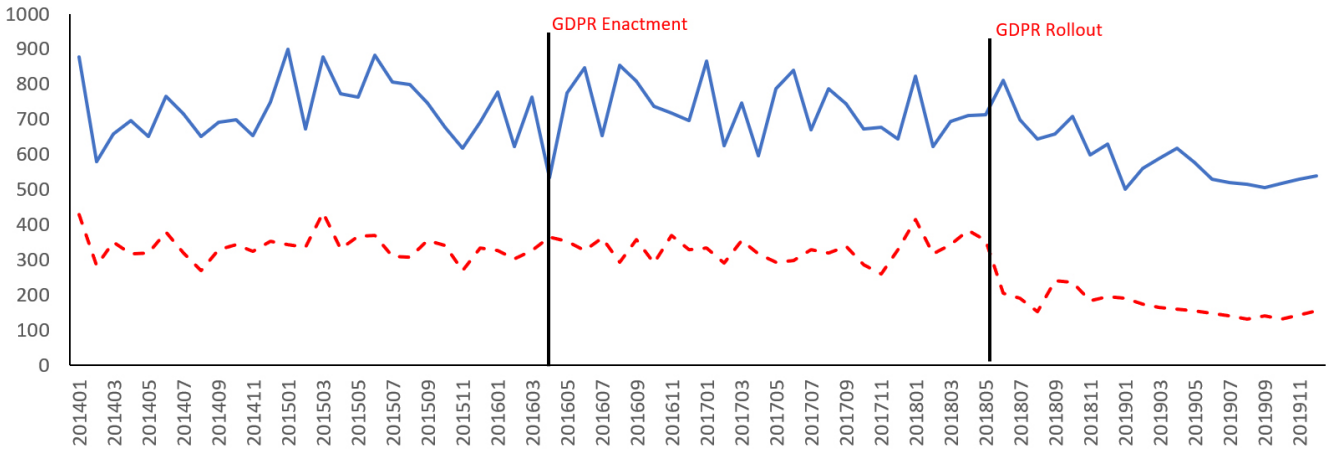
More specifically, we find that EU tech firms, relative to their U.S. counterparts, experienced an average 22.20 percent decline in the number of venture deals from foreign investors and a 41.89 percent reduction in their corresponding per-deal amounts after the rollout of GDPR. In comparison, the reductions were of 15.80 and 35.77 percent for same-union EU deals, and 12.1 and 28.08 percent for domestic EU deals. We also find that the effects are more pronounced for foreign investors who invested in more data-related ventures, in younger ventures, in early funding stages, and in consumer-facing ventures.



(a) Monthly # of foreign deals per member state in the EU and U.S.



(b) Monthly # of same-union deals per member state in the EU and U.S.



(c) Monthly # of domestic deals per member state in the EU and U.S.

Figure 1. Aggregate level trends of the average # of monthly deals per state (U.S.) and member state (EU)

To get a visual sense of our aggregate findings, Figure 1 depicts monthly trends for the average monthly number of deals of each type (foreign, same-union, and domestic in subfigures a, b, and c, respectively) per state (in the U.S.) or member state (in the EU). Note that there are no noticeable differential trends between the EU and the U.S. prior to the legislative enactment of GDPR in 2016. Figure 1(a) indicates a significant divergence between U.S. and EU ventures in the number of foreign investment deals after the rollout of GDPR in May 2018. Figures 1(b) and 1(c) suggest lesser effects for same-union and domestic venture investments.

One may wonder how the considerable reductions in venture investments, particularly foreign investments, affects the ability of European entrepreneurs to get new ventures started. Our analysis indicates that the number of *first-round* EU venture deals in our sample (i.e. the initial funding rounds that can help ventures get off the ground) incur a 17.8 percent decline after GDPR's rollout in May 25, 2018. This reduction affects primarily consumer-facing ventures (a decline of 22.7 percent) but also business-facing ventures (a decline of 12.4 percent). A large portion of the decline appears to be driven by foreign investors pulling back from investing in new EU ventures – more than twice as much as domestic EU investors. These findings suggest negative effects from GDPR on nascent European technology ventures, particularly *vis-à-vis* foreign investors.

If foreign investors are indeed pulling back, one would anticipate a shrinkage in the geographic distance between investors and ventures in the EU. Our results indeed confirm this conjecture. Relative to their U.S. counterparts, the geographic distance between EU ventures and their lead investors shrinks by between 12.4 and 27.5 percent, on average, after the rollout of GDPR, if the venture has raised investment both before and after GDPR. Furthermore, lead investors in previous EU venture deals, relative to their U.S. counterparts, are less likely – a 31.7 percent decrease – to continue to be the lead investors in subsequent rounds for the same ventures after GDPR. Again, the negative effect is more pronounced for foreign investors.

In short, our analyses suggest that, no matter how we cut the data, GDPR appears to be driving distant investors to pull back more from investing in EU technology ventures, particularly younger ventures, independent of whether those investors have previously invested in a particular venture or not, and independent of whether the venture is business-facing or consumer-facing.

Why do domestic investors and others located closer to EU ventures appear to be more optimistic post GDPR? Local investors may be more confident in their information about the extent of local enforcement and compliance costs. They may be able to reduce or better handle risks and uncertainty due to their localness to their portfolio ventures. They may also have worse outside options relative to investors located in the U.S. and in the rest of the world.

Short of these local "advantages," foreign investors could syndicate more with local investors to dampen potential concerns about the information asymmetries and due diligence costs. To explore this possibility, we group deals in our dataset into three subsamples: (i) deals with foreign lead investors and domestic or same-union co-investors (deals with only foreign investors are relatively sparse in our sample, comprising about 1.3 percent), (ii) deals with non-foreign lead investors and foreign co-investors, and (iii) deals with only non-foreign investors. Our results suggest a more pronounced negative effect from GDPR on the first group – deals with foreign lead investors – indicating that our findings continue to hold even when foreign lead investors syndicate with local investors.

As similar data regulations roll out in other states and countries, would we expect to see similar consequences? It is difficult to generalize the results outside our statistical framework. Every jurisdiction has its own considerations and may thus adopt different regulatory approaches and enforcement plans. The recently enacted California Consumer Privacy Act, for example, in contrast to GDPR, utilizes an opt-out approach whereby firms, by default, can collect customer data. The difference between opt-in and opt-out default regimes, while seemingly subtle, may have significant market consequences as shown in other contexts (Kim & Wagman, 2015).[11]

That being said, our findings do send a general message about data regulation: Policymakers considering any regulatory policy that aims to alleviate privacy and data concerns need to be cognizant of its potential effects on different investor types. For instance, a country that relies more on foreign investment may suffer larger decreases in venture capital upon implementing stricter data protections. By contrast, another country that tends to export larger amounts of investment may benefit from the perspective of retaining more venture capital for its own domestic firms once the other country adopts more stringent data policies. Our results thus point to a Prisoner's Dilemma situation in some sense, where, under some objectives, each country may unilaterally have a dominant strategy to implement lax data policies in its home market, even if a more stringent data ruleset across the world may be welfare enhancing if all countries could commit to this ruleset.

11 Kim, J. H. & L. Wagman (2015), "Screening incentives and privacy protection in financial markets: A theoretical and empirical analysis," *RAND Journal of Economics* 46(1): 1–22.

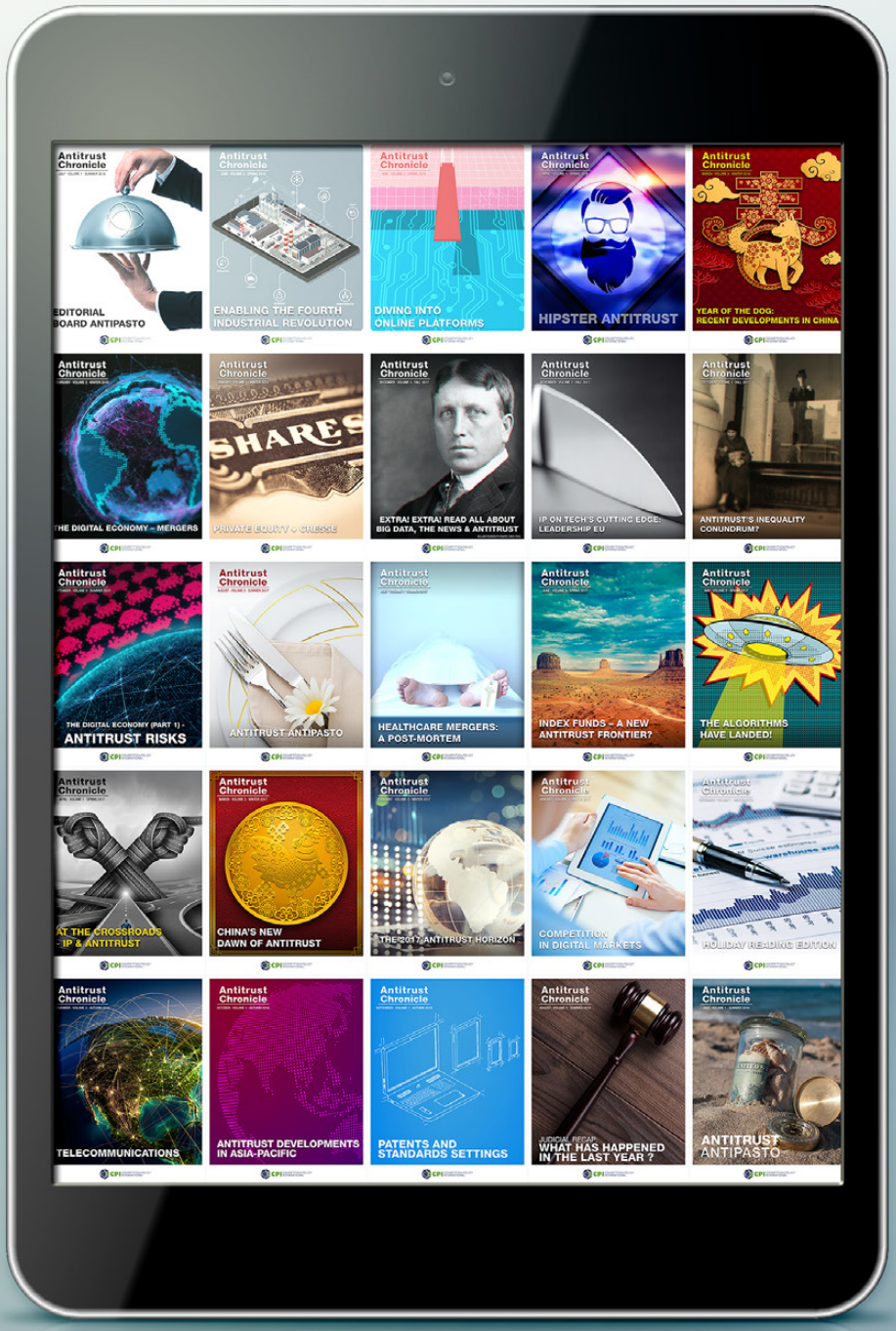
While our sample comprises technology venture investments made up to a year and half after GDPR was rolled out, the effects we identify may have longer-run consequences: European technology ventures that could have benefited from access to foreign investors' networks, marketing and revenue channels, as well as mentoring and expertise, may have failed to realize those benefits and opportunities, or ceded ground as a result to foreign competitors. Technology is a fast-moving market, with newer ventures often offering products and services that layer on top of their older counterparts' products and platforms; consequently, short-run disruptions can have long-term effects, particularly if foregone benefits and opportunities translate to more of those older platforms being offered by foreign firms further down the line.

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.




CPI
COMPETITION POLICY
INTERNATIONAL