DATA PRIVACY IN ADTECH: BOON OR BUST?

BY CYNTHIA J. COLE & NICHOLAS PALMIERI[1]

1 Baker Botts L.L.P.

The CCPA and the GDPR Are Not the Same: Why You Should Understand Both
By W. Gregory Voss

Data Privacy in Adtech: Boon or Bust?
By Cynthia J. Cole & Nicholas Palmieri

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

CCPA and Competition: The Value of Consumer Data, Privacy, and Pricing
By Jeewon Serrato & Lawrence Wu

Consumer Choice and Consent in Data Protection
By Pranvera Këllezi

Data Regulation and Technology Venture Investment: What Do We Learn From GDPR?
By Jian Jia, Ginger Zhe Jin & Liad Wagman

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.

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/.

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.

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

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).

9 CCPA § 1798.150(b).

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.

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]

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.

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.

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]

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).

---

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/.

24 *Id.*

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.

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.

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.