Briefing: California Consumer Privacy Act

A year and a half after it was passed and signed, California's much-debated privacy law officially took effect on January 1, 2020.[1] The CCPA was enacted in 2018 and gives consumers in California additional rights and protections regarding how businesses may use their personal information.[2] The obligations imposed on businesses are similar to those required by the General Data Protection Regulation enacted by the EU. It is touted as one of the strictest data protection laws in the US. However the law still has some loose ends and data protection gaps that need to be filled.

No Delay of Enforcement Amidst COVID-19

The CCPA is a state-level law that requires, among other things, that companies inform users of the intention to monetize their information and provide them with an easy way to opt out of such monetization.[3] The Act imposes many obligations on businesses that are similar to those required by the General Data Protection Regulation (GDPR) enacted by the European Union (EU). Nonetheless, a business that already complies with the GDPR[4] may have additional obligations under the CCPA.[5] At a high level, the CCPA imposes strict requirements on companies that must inform users about how their user data is used and monetized, while providing them with simple tools to opt out of the law.

Strict Data Protection With Some Loose Ends

The CCPA is touted as one of the strictest data protection laws in the US. In fact, California's privacy measure is one of the most comprehensive in the US, since most existing laws do little to limit what companies can do with consumer information. No other state has attempted such an ambitious privacy law, and since before the dawn of the internet, Congress hasn't either.[6]

However the law still has some loose ends and data protection gaps that need to be filled. One of the biggest challenges with the CCPA is the question of where the user data is located.[7] For instance, data might be located outside of the database that is being sold, it could be a marketing database or a one-month-programm that provides for special promotion, for which people register with their name and then remain in

[1] https://tcrn.ch/3bpKJSC
[2] https://oag.ca.gov/privacy/ccpa
[3] https://tcrn.ch/2KoAmmf
[4] https://bit.ly/3auIv37
[5] https://bit.ly/2XT5tOC
[6] https://nbcnews.to/2Seg2Zh
[7] https://bit.ly/2VPL4ri

the database. Therefore it can be quite hard to find the data, particularly the older it is.[8]

Rights For California Consumers

As of January 1, consumers in California have a right to know what personal data is collected, used, shared, or sold by businesses. Furthermore, they have a right to delete personal data and to prohibit the sale of personal data. Children under the age of 16 must give explicit consent to have their data eligible for sale, and a parent or guardian must give explicit consent for a child under the age of 13. Consumers exercising their rights under the CCPA are guaranteed not to be penalized with higher prices or lower service levels than those who do not.

Obligations For Businesses

Businesses that meet at least one of the following three criteria are subject to the CCPA:

- Businesses with annual revenues of $25 million or more
- Businesses that purchase, receive, or sell personal data from 50,000 or more individuals, households, or devices
- Furthermore, businesses whose sales of personal data represent 50 percent or more of annual revenues
- Additionally, businesses that handle personal data from more than 4 million consumers eventually may face additional obligations.

Consumers have to be notified in advance of the personal data being collected.

- Businesses will have to make it easy for consumers to exercise their rights under the act, such as by providing links on their websites and mobile apps to prohibit selling their data.
- Furthermore they need to respond within specific time frames to requests made by consumers under the act and they need to verify the identity of consumers making requests under the act.
- Additionally businesses have to disclose any financial incentives offered in exchange for the retention or sale of personal data, as well as how the value of this data was calculated. Also, businesses must explain why they believe such incentives to be permitted under the CCPA and keep records of all requests made under the act and how they responded.[9]
- As a further matter, businesses have to maintain data inventories and map data flows as well as disclose data privacy policies and practices. Under the provisions

[8] https://bit.ly/3eLnsge
[9] https://bit.ly/2KtlhzS

of the CCPA, the Attorney General of California is required to seek input from a broad segment of the public to guide the formulation and implementation of regulations that are designed to further the goals of the act.[10] Pursuant to this provision, the Attorney General held a series of public hearings in early December 2019, and December 6, 2019 was the deadline for written comments from the public. According to estimates prepared by Berkeley Economic Advising and Research, LLC., for the Standardized Regulatory Impact Assessment released in August 2019, the CCPA will protect personal data worth over $12 billion that is used in advertising in California each year.[11] The cost of compliance with the draft regulations, but excluding general compliance costs with the underlying CCPA law, is estimated in the same report to total somewhere between $467 million and $16.454 billion in the period from 2020 to 2030.[12]

The Crux Of The CCPA – Implementation And Concerns

While the CCPA took effect on January 1, 2020, enforcement, including the imposition of fines, will be delayed until June. Internet-based businesses, many of which are based in California, have been among the most vocal opponents of the law, arguing instead for US federal legislation that would set uniform standards across the nation. Part of their concern is that each violation of the CCPA potentially could trigger thousands of dollars in fines, which can add up to massive amounts across perhaps millions of users in California alone.[13]

The crux of the CCPA is this: If a company buys or sells data on at least 50,000 California residents each year, it has to disclose to those residents what it is doing with the data, and, consumers can request the company not sell it. Consumers can also request companies bound by the CCPA delete all their personal data. And websites with third-party tracking are supposed to add a "Do Not Sell My Personal Information" button that if clicked, prohibits the site from sending data about the customer to any third parties, including advertisers.[14]

However, internet companies Facebook and Google are already compliant with the EU's GDPR, which has stronger protections than the CCPA, notably by requiring opt-ins for sharing personal data, rather than merely facilitating opt-outs, as does the new California law. As a result, some observers believe that the CCPA will be more burdensome for smaller players, and thus entrench the leaders in online advertising.[15]

[10] https://bit.ly/3cGN3oG
[11] https://bit.ly/2XTptRo
[12] https://bit.ly/3eGNGAf
[13] https://tcrn.ch/2KoAmmf
[14] https://on.wsj.com/3bFII6h
[15] https://bit.ly/34VJvvQ

Lawsuits Concerning the California Consumer Privacy Act in Times of COVID-19

California companies were busy complying with California consumer privacy laws, but that was before the coronavirus pandemic occurred. Companies are now in a difficult position to compensate for coronavirus-related business disruptions and to respond in a timely manner to consumer inquiries from the CCPA. It is obvious that companies subject to the CCPA may have more urgent matters to deal with these days than responding to consumer inquiries from the CCPA.[16]

Indeed, even before the coronavirus crisis, businesses were navigating how to respond to CCPA consumer requests – and comply with the CCPA in general – given that the California attorney general has yet to finalize the CCPA's implementing regulations. The deadline for enforcement of the CCPA, approached, businesses began to wonder whether the timeframe for implementation was appropriate, especially when the Attorney General's Office issued another round of amended rules in March instead of the final rules. To that end, on March 17, 2020, over 30 trade associations[17], companies, and organizations sent a letter to California Attorney General Xavier Becerra[18] requesting that, in light of the coronavirus pandemic and unfinished status of the regulations[19], he "forebear from enforcing the CCPA until January 2, 2021 so businesses are able to build processes that are in line with the final regulations[20] before they may be subject to enforcement actions for allegedly violating the law's terms."[21]

Zoom Meetings And The Disclocure Of Privacy Policy

The software program known as "Zoom Meetings", has become immensely popular as a means to facilitate meetings amongst employees, team members and other consultants rather than meeting in person. Despite such status, Zoom Video Communications, Inc. has been named as a defendant in one of the first, and certainly the most high-profile, class action lawsuits to be filed in California alleging violations of the CCPA.

The complaint filed alleges that Zoom did not protect the personal information of its users as it collected personal information and then shared such information to third parties, including Facebook, without adequate disclosures to users. The allegations specifically refer to Zoom's boasting about its maintenance of users' privacy and that they can be trusted with user data. Further, it is noted that there is no disclosure

[16] https://bit.ly/3as7dRP
[17] https://on.wsj.com/2VpZAaa
[18] https://bit.ly/3asez7P
[19] https://bit.ly/3cEq7q6
[20] https://bit.ly/2RXi2EK
[21] https://bit.ly/2RZZ4gO

provided in the Zoom Privacy Policy that disclosed that personal information was being shared with Facebook and other third parties.[22]

Upon opening of the Zoom software, a notification is sent to Facebook providing details about, amongst other things, a user's device, phone carrier and a unique advertiser created by the device to provide targeted advertisements. This information is sent for every user even if the user does not have an account with Facebook.[23]

It is further alleged that Zoom may have been aware of this sharing of information when it added a feature to allow users to login with Facebook account information. With such knowledge, Zoom released an updated software version that prevents personal information from being sent whenever the software is opened by users. The complaint notes, however, that Zoom did not force users to upgrade to the newer version and that by continuing to allow use of the prior version, personal information is continuing to be provided to third parties.[24]

The complaint seeks injunctive relief, damages, including statutory damages pursuant to the CCPA, punitive and treble damages and attorneys' fees for alleged violations of the CCPA, Unfair Competition laws, the California Consumers Legal Remedies Act, Negligence, Invasion of Privacy and Unjust Enrichment.[25] Although the company quickly released a new version of the app within seven days, a class action lawsuit was filed in the Northern District of California on March 31.[26]

Other problems, though perhaps not as obvious, are still looming on the horizon. As, for example, offices, large retail stores, restaurants and stadiums gradually come back into our lives, there may be an increasing need to review and collect physiological data from customers and employees entering the room, such as body temperature, previous test results and tracking personal movements based on mobile phone information. In fact, there are reports that certain California grocery stores already measure the temperature of customers as they enter the room. And as more and more companies interact with their customers online during this crisis, many companies are collecting and using customer information, which requires that they have compliant collection and storage policies and practices.[27]

No Additional Time in Light of COVID-19

As these questions about the CCPA are decided in the coming months, the California Attorney General has made it clear at this point that, in light of the COVID-19

[22] https://bit.ly/2KmbQlG
[23] https://bit.ly/3eDI7Tn
[24] https://bit.ly/34VYw0N
[25] https://bit.ly/2xR3n7r
[26] https://bit.ly/2x3jheE
[27] https://bit.ly/34VYw0N

pandemic, he will not give companies additional time to understand and comply with the new law in a meaningful way. The use of the expression “right now” implies that the Attorney General might change his mind during the crisis. However, the fact that his office has stated that the protection of consumers’ privacy has an “increased value” during the crisis suggests that the Attorney General could continue with the 1 July enforcement deadline precisely because of the crisis. It is not yet clear whether the CCPA claims against Zoom will survive. However, this case is one to watch, as the CCPA case law evolves.[28][29]

As a result, companies around the world must be on high alert as they adopt new methods to mitigate the impact of the virus on their business to avoid costly class actions and enforcement actions by the Attorney General.

[28] https://bit.ly/34VYw0N
[29] https://bit.ly/2xR3n7r

Communications and Government Relations
Ann-Cathrin Spranger
Communications Specialist
T +49 69 929104-43
M +49 151 14657924
E aspranger@amcham.de