LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
TUESDAY, JANUARY 14, 2020

PERSPECTIVE

The California Consumer Privacy Act is not Y2K 2.0

By Tanya Forsheit

New York Times News Service

Alastair Mactaggart in Oakland, May 8, 2018.

For privacy lawyers old enough to remember, December 2019 felt oddly reminiscent of December 1999. There was a lingering sense of danger ahead and fear of the unknown, but also skepticism. Was CCPA to 2019 what Y2K was to 1999? The California Consumer Privacy Act, which took effect on Jan. 1 (now codified at Sections 1798.100-.199 of the Civil Code), is a Frankenstein's Monster of a law. In a short week in the summer of 2018, representatives of the very largest Silicon Valley companies, plaintiffs' lawyers, and state legislators gathered together in Sacramento to cobble together the original typo-ridden bill (Assembly Bill 375) in response to a much-feared ballot initiative launched by wealthy-real-estate-investor- turned-privacy-advocate Alastair Mactaggart, without any hearings or input from other stakeholders (industry, public sector, or scholarly). Legislators passed minor amendments in September 2018 (Senate Bill 1121) and again in October 2019 (AB 25, AB 874, AB 1146, AB 1355 and AB 1564) at the end of a contentious legislative session marked by the failure of almost all business-side attempts to align the law with existing and widely recognized privacy principles used in European law, Federal Trade Commission guidance, and best practices incorporated into industry self-regulatory guidelines.

The CCPA has completely changed the face of the privacy legal profession. While the privacy bar has been growing slowly and quietly for many years, the CCPA set it on fire in late 2018 and 2019. In 2007, fellow lawyers asked me on a weekly basis whether privacy was a real legal practice. Today this publication and others frequently proclaim that privacy is one of the hottest legal practices in the country. And law firms are scrambling to add seasoned practitioners to their ranks.

What does the CCPA change that has everyone scrambling? The law is the first of its kind in the U.S., providing European-style robust privacy rights to California residents. These rights include the right to request a copy of the specific personal information a company holds about you, the right to have your personal information deleted in certain circumstances, and the right to opt out of the "sale" of your personal information (much more on that below). It requires organizations to update their public-facing privacy policies to provide very explicit and detailed notices about their personal information collection, use and sharing practices, despite the fact that all research shows consumers don't read privacy policies and don't understand them, even today. It also calls for the amendment of contracts between organizations subject to the law and vendors who have access to personal information handled by those companies (think cloud providers, advertising agencies, outsourced IT, etc.) to impose additional restrictions on what those vendors can do with the information.

This article provides a top-of-the waves overview of some of the primary challenges presented to organizations struggling with CCPA compliance: (1) the overbroad definition of "personal information" and related consequences; (2) the "Do Not Sell" opt-out right debate; (3) the lack of finalized regulations; and (4) the threat of class action litigation seeking statutory damages with respect to the inevitable - data breaches.

Overbroad Definition of Personal Information

New definitions are at the heart of the challenges presented by the law — commonly understood terms no longer have their commonly understood meanings (to lawyers or laypeople). As Inigo Montoya in "The Princess Bride" would say: "You keep using th[ose] word[s]. I do not think [they] mean[] what you think [they] mean[]."

The most significant such definition is "personal information." This is not your marketing department's PII — you know, the stuff they say they don't have. "Personal information" is defined very broadly to include any information that is "reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Civil Code Section 1798.140(o)(1). The definition includes in a list of examples that might meet this definition items like online identifiers, internet protocol addresses, and internet or other electronic network activity information such as browsing history, search history, and information regarding a consumer's interaction with an internet website, application, or advertisement.

This broad definition of personal information means that a consumer might submit a request to delete or access their personal information, providing a name and email address, but the recipient company would have no way to determine whether they might have other categories of personal information — like those described above — that relate to that person. This is because most companies do not keep records associating consumer names and email addresses with surfing behavior, specifically in order to protect privacy. It would be counterintuitive, and privacy-endangering, to ask that consumer to provide even more information in order to fulfill

their request. Defining personal information so broadly, even more broadly than the European General Data Protection Regulation, is not actually privacy-friendly.

Do Not Sell Opt-Out Rights and Ad Tech

Another problematic definition is "sale." It does not actually mean sale. It means any "making available" or other communication of personal information by a covered business to another covered business or third party for monetary or "other valuable consideration." *Id.* Section 1798.140(t)(1). This matters because, if a company is engaged in such sharing of information (which is not a sale in the traditional sense), it is required to put a link on every page of its website where it collects such information that is named "Do Not Sell My Personal Information." Civil Code Sections 1798.120, 1798.135. If a California consumer invokes that right, the company must stop that sharing.

This sent the digital advertising world into a tailspin. Without getting into the weeds (the Daily Journal only gave me 1,800 words or less for this article), there is a multi-billion dollar advertising technology ("Ad Tech") ecosystem that is based on the likes of Google, Facebook and many others dropping tracking technologies such as cookies on website that gather up online identifiers, browsing history, and consumer interactions with websites and digital advertisements in order to more effectively target those ads. That is how consumers get so much free and low-cost content online.

These Ad Tech companies, their customers, and the many intermediaries involved don't know that Tanya is surfing the web for deals on flights to Mexico. But they do know from the cookies and other trackers that my phone and my laptop and every device that I own has been searching for and checking out those deals on a variety of sites and apps. And they can assign random identifiers to my surfing behavior in order to retarget me when I go to other sites and applications. This is why I get ads for the vacation about which I have been dreaming (thanks to the CCPA) instead of Viagra. I personally appreciate this more targeted advertising, but some people think it is creepy. And it raises many more questions when it involves sensitive information like my health and connects the dots to target me with ads for a middle-aged woman lawyer worried about the dark circles under her eyes (thanks also to the CCPA).

Does this Ad Tech activity involve the making available of personal information to third parties for monetary or other valuable consideration? Reasonable legal minds may (and do) differ. Sometimes dramatically. And if you surf around the web today, post-Jan. 1, you will find some publisher websites that have a Do Not Sell opt-out link, and others that do not. It is enough of a concern that the entire Ad Tech ecosystem — publishers, Ad Tech companies, agencies, and advertisers — has proffered a number of industry solutions, including the IAB CCPA Compliance Framework for Publishers & Technology Companies and the DAA CCPA Opt-Out Tool.

No Final Regulations

It remains to be seen how Attorney General Xavier Becerra addresses this confusion in the CCPA's enforcement. The Attorney General can commence enforcement on July 1, 2020, but Becerra has stated publicly that he expects companies to be in compliance as of Jan. 1.

This provides a helpful transition to the next challenge, and perhaps the most significant — the lack of finalized regulations to govern compliance. The attorney general was charged with promulgating regulations but did not even issue a draft until October 2019. It sought public comment and held a series of hearings in the first week of December 2019. It will be months before the regulations are finalized and, as noted above, the Attorney General can start enforcing on July 1, 2020. This leaves organizations in uncharted seas. There is simply no guidance for businesses seeking uniformity and certainty in the application of the law.

Data Breach Lawsuits

Another completely new feature of the CCPA, first of its kind in the country, is a private right of action providing for statutory damages of $150 to $750 per person per violation in the event that a consumer's nonencrypted and nonredacted personal information (more narrowly defined to include the information subject to California's data breach notification law, Civil Code Section 1798.82), is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain "reasonable security procedures and practices appropriate to the nature of the information to protect the personal information." Civil Code Section 1798.150. The law does not define "reasonable security"; however, in 2016 then-California Attorney General Kamala Harris' 2016 Data Breach Report helpfully identified the 20 Center for Internet Security (CIS) Controls as the baseline for "reasonable security."

The private right of action requires that, "prior to initiating any action against a business for statutory damages on an individual or class-wide basis, a consumer provides a business 30 days' written notice identifying the specific provisions of this title the consumer alleges have been or are being violated" and an opportunity to cure by demonstrating, for example, that the breach occurred despite reasonable security measures. *Id.* Section 1798.150(b). Thus, it would behoove organizations to confirm that their internal information security policies and practices map against the CIS Controls, that they are taking steps to implement security controls appropriate to their industry and the volume and the sensitivity of personal information that they process, and that they are prepared to explain those measures in response to a notice letter from a consumer threatening action.

As I draft this piece, we are in the calm before the storm. It is likely that attorneys for consumers have already begun the process of sending out these 30 day notices, and that we will start to cases filed on or around Jan. 31.

Is the CCPA the new Y2K? Hardly. Jan. 1, 2000, was the end of the Y2K hype. Jan. 1, 2020, was just the beginning of the challenges for organizations grappling with CCPA compliance. It is an interesting time to be a privacy lawyer. ■

Tanya Forsheit *is the Los Angeles office supervising partner of Frankfurt Kurnit Klein & Selz and chair of the firm's nationwide Privacy & Data Security Group. She founded and chairs the inaugural Privacy & Cybersecurity Section of the Los Angeles County Bar Association and is an adjunct professor at Loyola Law School where she is teaching California Privacy Law in 2020 this semester.*