ORANGE COUNTY
LAWYER®
OCBA

WHO'S WHO IN THE OCBA
THE AFFILIATE BARS

www.ocbar.org AN OFFICIAL PUBLICATION OF THE ORANGE COUNTY BAR ASSOCIATION May 2019 Vol. 61 No. 5 $4.00

SHOULD PUTATIVE CLASS MEMBERS OPT IN BEFORE THEIR PERSONAL INFORMATION IS DISCLOSED IN CALIFORNIA CONSUMER PRIVACY ACT LITIGATTION?

by LILY LI and MATTHEW K. WEGNER

In 2020, the nation's toughest data privacy law will take effect in California. The California Consumer Privacy Act of 2018 (CCPA) imposes harsh restrictions on companies seeking to sell consumers' data, including statutory penalties for any breaches of data. This legislation was spurred by public outrage against the Facebook-Cambridge Analytica scandal and Equifax, Target, and Yahoo data hacks, and reflects a growing trend to protect consumer data privacy.

As with so many legislative and judicial movements in California over the course of time, the CCPA is likely to usher in a host of new class action litigation as plaintiffs (and their attorneys) seek to recover statutory damages for data privacy violations.

Meanwhile, long before the California legislature passed the CCPA, a body of law began to develop in California focused on the privacy rights of putative class members in class action cases. It was common to see "class issue" discovery and "merits" discovery separated (a practice that has gradually changed as courts have trended toward finding class and merits issues tend to overlap). But courts found themselves in murky water, attempting to balance the privacy rights of putative class members against the plaintiff's right to class-related discovery.

A decade ago, courts began to strike a balance between the plaintiff's right to "class" discovery—namely, the identities of potential class members—and those potential class members' right to privacy. In *Pioneer Electronics (USA), Inc. v. Superior Court* and *Belaire-West Landscape v. Superior Court* (and their progeny), California courts introduced a compromise: Apprise the would-be class members that the named plaintiff is seeking their private information in a class action, then allow them the opportunity to opt out of having their information disclosed to plaintiff's counsel.

But the process is far from perfect. And when the inevitable wave of class litigation hits following the activation of the CCPA, courts will grapple with new questions concerning the disclosure of putative class members' privacy in class litigation. What should courts do when the issue at the heart of the case is, itself, a privacy breach? How should the courts treat these litigants, whose data privacy is subject to heightened privacy protections above and beyond those that are constitutionally mandated in California? How should courts treat putative class members who are minors, and therefore entitled to even stricter privacy protection under the new law?

Privacy Rights in California Class Actions

Parties to a class action generally have the right to communicate with putative class members who have an interest in, or information relevant to, the dispute.[1] In most class cases, the identity of the putative class members is more ascertainable to the defendant than it is the named plaintiff. For example, in employment class actions, the defendant employer has access to the identities and contact information of its employees, where the named plaintiff (and his or her counsel) may not. In consumer class cases, the defendant (often a seller or manufacturer) is also more likely to have access to information about putative class members' identities than is the plaintiff.

In California, however, a putative class member enjoys a constitutional and common law right to privacy.[2] It is common practice, and in some cases an obligation, for a defendant to object to discovery requests that seek the personal identifying information of putative class members. For decades—operating in the absence of strong guiding authority—superior courts struggled to balance the plaintiff's need for the information against the putative class members' right to privacy in their identities.

Then, in 2007, the California Supreme Court handed down a decision that appeared to strike the balance between these competing interests. In *Pioneer Electronics (USA), Inc. v. Superior Court*,[3] a consumer class action, plaintiff requested the identifying information of all consumers who had complained about the allegedly defective DVD player at the center of the lawsuit. Defendant objected to disclosure of the consumers' identifying information, citing the consumers' right to privacy. Recognizing both the plaintiff's right to relevant discovery and the putative class members' right to privacy in their identities, the court held that the putative class members' privacy rights would be adequately protected if they were given an opportunity to opt out of the disclosure of their personal information. Then, later that year, the Second Appellate District decided *Belaire-West Landscape v. Superior Court*,[4] which pivoted off *Pioneer* and ordered defendant employer to disclose the identifying information for putative class member employees after the members received notice of their right to opt out of that disclosure. The creature of California class action litigation now known as the *Belaire* Notice procedure was born.

> [T]he CCPA is a potential goldmine for class action plaintiffs.

In a *Belaire* Notice procedure, the parties often meet and confer about the content of the notice that putative class members will receive before their identifying information is produced in discovery. The notice generally explains that litigation is pending, and should conspicuously warn the recipient that his or her personal information is at risk of disclosure to plaintiff's counsel. Most notably, the case law trends heavily toward an opt-*out* procedure, whereby the recipients must take affirmative steps to prevent having their personal information revealed. Indeed, attempts to heighten privacy protections by requiring that putative class members opt *in* to disclosure of their personal information have been met with skepticism by the courts.[5]

While *Belaire* Notices have become a common part of the landscape in California class actions, the proper form of, and mechanics for sending, these notices is by no means settled law. Parties to class litigation often spend considerable time and effort arguing over nuances with significant ramifications: Will the notice reach the intended recipients so that their interests are protected? Does the language of the notice improperly condition the recipient to favor disclosure or non-disclosure? Will the recipients appreciate the gravity of what they are reading? Are their privacy interests important enough to warrant specific language? As these questions (and the disputes that often arise from them) suggest, the *Belaire* Notice is far from a perfect method for ensuring that putative class members' privacy rights are protected. One size does not fit all.

The Looming Storm: Conflicts Between Data Privacy Law and Class Action Discovery

California's new privacy law affords consumers unprecedented rights to know how businesses share their information, to control how that information is shared, and to pursue statutory damages in the event of a data breach. The likelihood of increased consumer litigation is almost a given: Starting in January 2020, a successful plaintiff in a data breach case will be entitled to statutory damages of $100-$750 per consumer per incident—or actual damages—whichever is greater. Though this amount may appear

small at first, damages awards can escalate quickly. According to the IBM/Ponemon Cost of Data Breach Study for 2018, the average number of records compromised in a data breach in the United States is 31,465, which would result in a statutory damages award of approximately *$3 million* to *$23 million* under the CCPA—not including attorney's fees and notification costs. Consequently, the CCPA is a potential goldmine for class action plaintiffs.

The CCPA's heightened sensitivity to privacy, however, may present obstacles to a plaintiff's ability to gather the personal information of putative class members. In contrast to the *Belaire* and *Pioneer* opt-out paradigm, the CCPA incorporates several opt-*in* provisions for transfers of personal information. For instance, the CCPA gives consumers the right to opt out of the "sale" of their information. Following the opt-out request, businesses must wait twelve months before they can contact these same consumers to obtain opt-*in* authorization for the "sale" of their personal data.[6] The definition of a "sale" is broad under the CCPA, encompassing all transfers of data to another business or third party for "monetary or other valuable consideration," with limited exceptions. Thus, putative class members who have exercised their opt-out rights under the CCPA have already informed businesses that they do not want their information shared with third parties, and would expect some form of opt-in authorization prior to any disclosures.

This conflict with the *Belaire* and *Pioneer* decisions is even more present when it comes to children. The CCPA requires opt-in authorization for sales of children's data, from the parent or guardian for children under age thirteen, and from the child for children between the ages of thirteen and sixteen. These provisions in the CCPA make a lot of sense. Children are less likely than adults to read the legal disclosures surrounding use of their data, and are susceptible to sharing their information online without understanding the consequences. Similarly, children are unlikely to appreciate the ramifications of participating in a class action lawsuit—let alone the legalese surrounding *Belaire* notices. In these situations, an opt-in approach would more effectively protect their privacy rights.

Could the CCPA Change the Data Sharing Paradigm for All Class Actions?

The CCPA's sensitivity to privacy rights may well extend to the sharing of putative class member information in *all* consumer class actions. For example, the CCPA requires clear and easy opt-out processes for all sales of data, via a toll-free number, accessible web page, and links on a business's homepage and privacy policy. Arguably, a *Belaire* notice should be subject to the same protective measures, regardless of the nature of the action; they should be just as transparent and easy to use for the consumer.

The CCPA also gives consumers the right to know where their data is being transferred. California consumers have the ability to make a request, once every twelve months, to know the categories of third parties with whom the business shares personal information (and identify whether it is a sale of personal information, or disclosure for business purposes). Thus, consumers should have a right to know whether their data is going to be shared with other law firms, litigation funding companies, medical providers, mailing lists, or a whole host of third parties both before and during the litigation process. Though the CCPA provides a carve-out for data sharing designed to "exercise or defend claims"—it is unclear whether all current data sharing practices are necessary for litigation purposes—and in any event, the consumer should be fully informed of where data is going prior to exercising any opt-in or opt-out rights.

Finally, data hackers can target law firms and their vendors just as easily as any other business. The CCPA's statutory damages provisions bolsters previous provisions under the Civil Code, which state that "[a] business that owns, licenses, or maintains personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."[7] This code section also requires businesses to contractually require third-party vendors to abide by the same "reasonable security procedures and practices." Given these requirements, should courts require attestations from attorneys of their data handling practices prior to ordering the disclosure of that data to plaintiffs' counsel? Might class action lawyers be required to affirmatively conduct data due diligence on their vendors, prior to sharing any data? Considering the impositions the law places on those who house sensitive consumer data, and the potential for exposure to significant damages awards in the event of a data breach, future attorneys seeking sensitive information about putative class members may find themselves guided by a principle that long preceded the CCPA and *Belaire*: "Be careful what you ask for."

ENDNOTES

(1) *See, generally, Atari, Inc. v. Superior Court*, 166 Cal. App. 3d 867 (1985).
(2) *See* Cal. Const., art. I, § 1.
(3) 40 Cal. 4th 360 (2007).
(4) 149 Cal. App. 4th 554 (2007).
(5) *See, e.g., Crab-Addison v. Superior Court*, 169 Cal. App. 4th 958 (2008).
(6) CCPA, Cal. Civ. Code § 1798.135 (2018).
(7) Cal. Civ. Code § 1798.81.5 (2016).

Lily Li *is a data privacy lawyer, CIPP/E, CIPP/US, CIPM and owner of Metaverse Law. She can be reached at info@metaverselaw.com.* ***Matthew K. Wegner*** *is a commercial and intellectual property litigator and partner at Brown Wegner LLP. He can be reached at mwegner@brownwegner.com.*

This article first appeared in Orange County Lawyer*, May 2019 (Vol. 61 No. 5), p. 28. The views expressed herein are those of the author. They do not necessarily represent the views of* Orange County Lawyer *magazine, the Orange County Bar Association, the Orange County Bar Association Charitable Fund, or their staffs, contributors, or advertisers. All legal and other issues must be independently researched.*