New York Law Journal

NEW YORK LAW JOURNAL SPECIAL REPORT

An ALM Publication

E-DISCOVERY

WWW.NYLJ.COM

VOLUME 261—NO. 23

MONDAY, FEBRUARY 4, 2019

Bracing for the Big One: The Impact of the **California Consumer Privacy Act** on E-Discovery

BY PAUL BOND, MARK S. MELODIA AND MARK FRANCIS

The California Consumer Privacy Act of 2018 (CCPA) comes into force on Jan. 1, 2020. The CCPA enshrines the "right of Californians to know what personal information is being collected about them," and "to access their personal information" after it is collected.

The Act confers no generalized private right of action. The CCPA does not directly modify any rule of evidence or civil procedure. Indeed, the Act acknowledges that the obligations to produce information under the Act, "shall not apply where compliance by the business with the title would violate an evidentiary privilege under California law," Cal. Civ. Code 1798.145(b).

Nevertheless, the plaintiffs' bar may attempt to use the access provisions of CCPA as a tool in their discovery arsenal. Litigators and compliance attorneys must work together against the rush to exploit the CCPA for liability purposes.

The CCPA Will Create Honeypots of Personal Information

The CCPA imposes obligations on any business which collects and/or processes "personal information" about "consumers" and meets certain additional financial criteria. In practice, a great many companies that operate in California or nationwide will be subject to the Act.

The Act vests rights in "consumers," natural individuals, resident in California as defined by state law. Cal. Civ. Code §1798.140(g). However, nothing in the Act expressly limits the term to those who obtain goods or services from the company for personal, family, or household uses. Arguably, other individuals may be consumers, including, for example, employees.

In general, CCPA personal information means "information that

identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household." Cal. Civ. Code §1798.140(o). The term is broad.

The Act gives numerous examples. "Personal information" under the CCPA includes the typical data breach fare, such as name plus SSN, driver's license number, passport number, payment card information, bank account numbers, and any other financial information, medical information, or health insurance information. But the CCPA goes much further. It includes, for example, the history of purchases made or considered as well as

PAUL BOND, MARK S. MELODIA *and* MARK FRANCIS *are partners at Holland & Knight.*

information about how a consumer interacted with a given website or ad. The CCPA regulates biometric information and geolocation data. No human sense is beyond the interests of the CCPA—personal information may include audio, electronic, visual, thermal, olfactory, or similar information. Education or employment-related information can be "personal information." Lastly, to the extent that a company has used any of the above to draw inferences about a consumer, that too is personal information. The CCPA covers any "profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes." Cal. Civ. Code §1798.140(o).

Taken together, this personal information encompasses virtually every aspect of the company-consumer relationship.

Such a "consumer" has the right to demand "[t]he specific pieces of personal information" the company has collected about that consumer in the past 12 months, as well as the instances and circumstances under which that information has been shared with third parties. Cal. Civ. Code §1798.110(a)(5).

The company must make available a toll-free number and a website address for such requests. §1798.130(a)(1). Within 45 days of the request, the business must "disclose and deliver the required information to a consumer free of charge." Cal. Civ. Code §1798.130(a)(2). This time period may be extended once by an additional 45 days when reasonably necessary. Cal. Civ. Code §1798.130(a)(2). "The disclosure shall … be made in writing and delivered through the consumer's account with the business … or by mail or electronically at the consumer's option … in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance." Cal. Civ. Code §1798.130(a)(2).

The CCPA Will Allow for Pre-Suit Discovery

Normally, a would-be plaintiff must file a complaint to obtain discovery. As a result, initial complaints tend to be limited to the facts that are readily ascertainable to the plaintiff, as well as informed speculation. A consumer may speculate, for example, that a mobile application is location tracking and sharing it with third parties. An employee may guess that their employer has created internal profiling which has unfairly kept them from promotion at work. Someone calling a helpline may believe that calls are being recorded without any disclosures. But, in most cases, these would-be plaintiffs approach the complaint stage with the barest rudiments of facts.

Starting Jan. 1, 2020, the tables are turned. The consumer can write or call toll-free and obtain a year's worth of "personal information." The app provider would have to say, yes, we collected your geolocation information and shared it, or, we didn't. The employer would have to disclose its data collection and profiling, including the specific segments of profiling applied to the requester. The helpline would have to disclose any audio tapes made. All of this can be obtained—and added to the complaint as an exhibit or admission—without the need for the identification and deposition of a records custodian or person most knowledgeable, or serving a single document demand.

While a business can require an administrative fee if requests "are manifestly unfounded or excessive, in particular because of their repetitive character," Cal. Civ. Code §1798.145(g)(3), the business must demonstrate the burden. If a business keeps records in normal course, the CCPA seemingly will often compel production. Ideally, this sort of pre-suit transparency should benefit both sides by sharpening and clarifying what is truly in dispute. In practice, making so much information available beforehand may

only serve to fill up kitchen sink complaints.

CCPA Compliance Efforts May Set the Table for Class Action Attacks

The CCPA could change class action litigation profoundly. Generally speaking, a court will only certify a litigation class action if class membership can be ascertained through readily-available means. Partial records, fragmentary data, disconnected systems have all helped defendants by creating a chaos not easily tamed. Many putative class actions have failed to be certified because, for example, it was not possible to tell which person made what purchase, or who saw what disclosure, or whether a given person talked with a sales representative within a relevant period. No "easy button" existed to pull together disparate databases.

From the point of view of class action counsel, the efforts that companies make to comply with CCPA data access requests may change all that. The same information that will satisfy mandatory CCPA responses to individuals may hold the key to systematically identifying putative class members. The data may also determine the potential for adequate notice, the predominance of common issues, and the ability to readily ascertain damages.

Of course, parties seeking to certify a class action will retain all their usual discovery options, but the CCPA may provide one more. The CCPA allows representatives to make requests for access on behalf of consumers. "Class action counsel" typically assert that they represent each and every class member, even before a class is certified. Could class action counsel submit CCPA requests en masse for putative class members? Much remains to be determined.

Corporate Counsel Must Act Now to Minimize CCPA Litigation-Related Risk

First, understand the CCPA's requirements, and what impact they will have on litigation and discovery. Stay informed about changes in the law or rules issued by the California Attorney General, as they may impact how the law will be interpreted and implemented.

Second, before applying CCPA-required changes nationwide, factor in the risk of making things too easy—nationwide—for putative class counsel. This is easier said than done, as many organizations engaging in expensive operational changes for GDPR and CCPA compliance will have a competing interest in extending changes to other states in view of likely additional state legislation and possible federal privacy standards finally emerging in 2019.

Third, reconsider current retention practices and double down on defensible deletion efforts. The CCPA will be giving plaintiffs an X-ray machine to view detailed facts before filing a complaint. Class counsel will also say that the changes made by companies looking to comply with the CCPA have effectively built a system capable of sorting for class purposes. The CCPA does not require you to keep any data which you should otherwise delete; what is deleted cannot be produced.

Fourth, ensure that your CCPA production protocol does not produce more than is requested. Each additional piece of information volunteered can later be used against you. At the same time, prepare to defend your response in court.

Fifth, make sure there is some level of human visibility into the CCPA data access process. Look at the frequency of demands, the topics, who is making the requests, and specificity demanded. These may be the warning tremors of litigation to come.