Seyfarth

LEGAL UPDATE Apr 7, 2020

The Impact of COVID-19 on the California Consumer Privacy Act

Sign up for our Coronavirus roundup email.
Visit our Coronavirus resource page.

Even before the COVID-19 pandemic, businesses around the world had been bracing for the financial and operational impact of the new California Consumers Privacy Act ("CCPA"), which took effect January 1, 2020. Despite existing and ongoing uncertainty around how to comply and interpret the law, the courts had already began seeing private class actions brought under the CCPA (or using the CCPA as a placeholder with Business and Professions Code Section 17200 and tort claims) filed in February—each presenting interesting and far-reaching legal questions about the new law.

But we now live in a very different world than we did back in the old days of February 2020, a post-coronavirus world that brings with it its own new realities, risks, and issues around compliance with the CCPA—and of course lawsuits.

Some of the effects are immediate and obvious. When Zoom became the part of the national lexicon in mid-March, a *Vice* article on March 20 revealed how Zoom's customers' information was allegedly shared with Facebook. Though the company quickly released a new version of the app within seven days, a class action suit was filed in the Northern District of California with swift speed on March 31.

Other issues, though maybe not so obvious, are nevertheless on the horizon. For instance, as offices, large retail outlets, restaurants, and stadiums are phased back into our lives, there may be an increase in the need to screen and collect physiological data of customers (as well as employees) entering the space, for things like body

temperature, prior testing results (including antibody confirmation), and personal movement tracking based on cell phone information. In fact, there have been reports that certain California grocery stores are already taking customers temperature upon entry. And as more companies interact with their customers online (as opposed to in person) during this crisis, many companies are collecting and using customer information, which necessitates that they have compliant collection and storage policies and practices.

This article will discuss some of the legal considerations around compliance with the CCPA under these novel situations and realities, including some of the trickier questions that will confront companies going forward, including the various factors places like shopping malls will need to consider as it seeks to reduce risk and mitigate the effects of the pandemic on it and its retail tenants.

While these (and many other) questions about the CCPA will be determined in the coming months, the California Attorney General has made it clear at this point that he will not be giving companies extra time to make sense of, and comply with, the new law in light of the COVID-19 pandemic. As a result, companies around the world (not just in California) need be on high alert as they employ new methods of mitigating the impact of the virus on their business to avoid expensive class actions and attorney general enforcement actions.

CCPA background and enforcement

As background, the CCPA provides consumers with an express private right of action for unauthorized access and disclosure of their data (further referred to herein as a "security breach"). The two central questions at the heart of this broad catch-all: (1) whether there was a security breach; and (2) whether there was "reasonable security" in place prior to the breach. Separately, the CCPA allows for the state Attorney General to enforce all other requirements under the statute, such as the notice requirements, the right to be forgotten, and the requirement to provide data upon request. The law applies to companies who do business in California, though the scope of that definition leads to inclusion of companies around the world (whether they know it or not). This is a result of California being the world's fifth largest economy, and the CCPA's scope applying to California residents (regardless of where the business is located).[1] Since most businesses do business in California, it follows that they will have data on California residents and thus the CCPA arguably applies.

Last year, *before* the pandemic, an economic impact assessment prepared for the Attorney General's office by the independent firm Berkeley Economic Advising and

Research found that companies could spend up to $55 billion on legal fees, technology and operational costs to become compliant, with smaller firms with less than 20 employees projected to face $50,000 in initial costs, and companies with more than 500 employees projected to see costs on average of $2 million.

While the law passed in 2018, it did not go into effect until January 1, 2020, and the Attorney General was not to begin enforcement of the law until at least July 1, 2020. Numerous trade associations and companies around the world had already been pressing the Attorney General to delay enforcement of the law due the tremendous amount of uncertainty over how companies can comply (and the fact that the final regulations for the law had still not been drafted and published). This group of 60+ international associations and companies just recently sent another letter to the Attorney General in late March urging delay on the basis of businesses needing time to "absorb the shock to the system" the pandemic is having on various industries.

However, in an email to *Forbes*, an "advisor" to the California Attorney General seemingly made it clear that the office intends to stick with the enforcement deadline of July 1, further issuing a stern warning to California businesses: "*We're all mindful of the new reality created by COVID-19 and the heightened value of protecting consumers' privacy online that comes with it. We encourage businesses to be particularly mindful of data security in this time of emergency*." (emphasis added)

In other words, with the "heightened value" of consumer's personal information, companies should not expect any slack from the Attorney General when it comes to immediate enforcement of *every* requirement within the CCPA come July 1, 2020. And as the first few months of the CCPA have displayed, companies should not expect any slack from Plaintiffs' class action attorneys bringing individual class actions based on security breaches and lack of reasonable security measures, particularly with extra time on their hands in light of court closures and restrictions.

CCPA initial action and initial post-pandemic action: *Zooming* to the courthouse

Though many of the early cases filed have used the CCPA as a placeholder to be bootstrapped with B&P 17200 and tort claims[2], the right to bring a private action was quickly availed with the first suit brought on February 3 against an e-commerce platform and the operator of the platform.***[3]*** Interestingly, the alleged security breaches in this case were before the January 1, 2020, triggering date, but Plaintiffs are alleging that the

hackers did not disseminate the information to third parties until after January 1—thus leaving a question of first impression for the court to determine whether or not the action is time barred and otherwise actionable.

Subsequent actions were filed in February and the beginning of March, including an allegation relating to the failure to provide notice of a right to opt-out of the sale of information.

And then COVID-19 came to the States, schools began to shut down, offices began to close, and even our children began to learn what the word "*Zoom*" meant. On March 20, the same day California Governor Gavin Newsom issued the country's first shelter-in-place order, an article was published on *Vice*, which detailed how the Zoom video-conferencing app allegedly exposed users to targeted advertising regardless of whether the user has a Facebook account. Though, as stated above, the Company quickly released a new version of the app without the integration of Facebook within 7 days, that decisive action was not enough to prevent a law suit from being filed on March 30, 2020[4]—only 10 days after the *Vice* article and the shelter-in-place order that made Zoom a ubiquitous name in most households across the country.

The swiftness by which this action was brought after being unearthed to the world is certainly alarming to any company engaging in similar business, and even more alarming to any company looking to change or alter their business practices in light of the COVID-19 pandemic. Adding to this, not only were the allegations related to alleged underlying security breach and dissemination, but they were also focused on the subsequent failure to block prior versions of the app and the failure to assure users that the previously-collected info has been deleted. Thus, even if a company is alerted to an inadvertent security breach and dissemination, it can still face potential liability for its response—regardless of the speed or purpose for which the response is given.

CCPA issues in a post-pandemic world

When society starts getting back to a semblance of ordinary life, and what that looks like, are questions beyond this article's scope. But one thing is for sure: companies will be looking to manage risk and mitigate the impact of the COVID-19 virus on their business. And because the risk associated with the pandemic is a personal risk (someone is sick), it necessarily will relate to personal information subject to the CCPA's reach.

As outlined above, there is a likelihood that the transition from social distancing may lead to an increase in the need to screen and collect physiological data from customers who

enter physical spaces, as well as employees within any office space, for information such as body temperature, prior testing results, and personal movement tracking based on cell phone information. In fact, this is already reportedly happening with supermarkets in the Los Angeles area.

Taking this real world example and broadening it to provide another example to be encountered in the not-so-distant future, there may be a time soon where a shopping mall decides (or is even compelled by a governmental agency) to take the body temperature of all customers entering the mall's physical space, before they enter any of the individual stores. This would be meant to not only reduce the risk that other customers or employees are exposed to the virus on their premises, but also meant to reduce the risk that certain stores within the mall may be forced to shut down or quarantined, thereby resulting in the inability to generate income and make lease payments.

In this scenario, the shopping mall would need to (a) establish process for notice to each consumer, (b) deal with and provide verifiable customer requests, and (c) create a response protocol to account for who is it sent to, and for what purpose. And even if companies keep all of the aforementioned factors in mind, there are still numerous tricky questions to navigate, particularly given the fact that the CCPA does not limit companies to online notification (unlike previous laws), thus creating difficulties about how to provide notice to consumers who are not interacting with the company online.

In an even broader sense, with the unexpected increase in remote workers, e-commerce engagement, and online learning and communication, the associated increase in the sharing of personal information and the susceptibility to hackers cannot be understated. As these changes have occurred in the blink of an eye, many companies are now pushing the limits of their existing remote access technology, or deploying *ad hoc* technology and access solutions as quickly as possible.

Unfortunately, speed and "reasonable security" are usually at odds with each other. Some of those companies are not taking the time to consider potential information security, privacy, and other compliance ramifications for those same remote workers (additional information on this subject can be found in a related Seyfarth article.

All of these questions are surely to increase the projected $50,000 to $2 Million costs of compliance for (both operational and financial) for all qualifying companies, in addition to other costs that may be associated with compliance with other state or federal statutes (e.g. HIPAA or biometric laws).

At least some light should be shed on these and other CCPA-related questions once the regulations finalized and provided to the public, though the litigation ensuing from the CCPA will only increase with time, and with pandemic-related new realities. While we all hope one curve flattens, companies can count on the CCPA litigation curve going sharply in the other direction.

[1] The discussion of whether or not California is capable of regulating interstate commerce or international commerce is a topic for another article and is out of scope of our discussion today. To that end, we are assuming that California will at least attempt to enforce its laws to protect its consumers regardless of political boundary.

[2] The CCPA explicitly provides that “nothing in this act shall be interpreted to serve as the basis for a private right of action under any other law”. The California Senate Judiciary Committee has voiced its opinion that “it appears that this provision would eliminate the ability of consumers to bring claims for violations of the Act under statutes such as the Unfair Competition Law, B&P section 17200.” However, Plaintiffs have already challenged this reading, and have already brought actions based on the collection of personal information is an unlawful and unfair business practice (see *Burke et al. v. Clearview AI, Inc. et al.*, Case No. 20CV0370).

[3] See *Barnes v. Hanna Anderson, LLC et al.*, Case No. 3:20-cv-00812-LB).

[4] See *Cullen v. Zoom Video Communications, Inc.*, Case No. 5:20-cv-02155-SVK)

Authors

John P. Tomaszewski

Partner

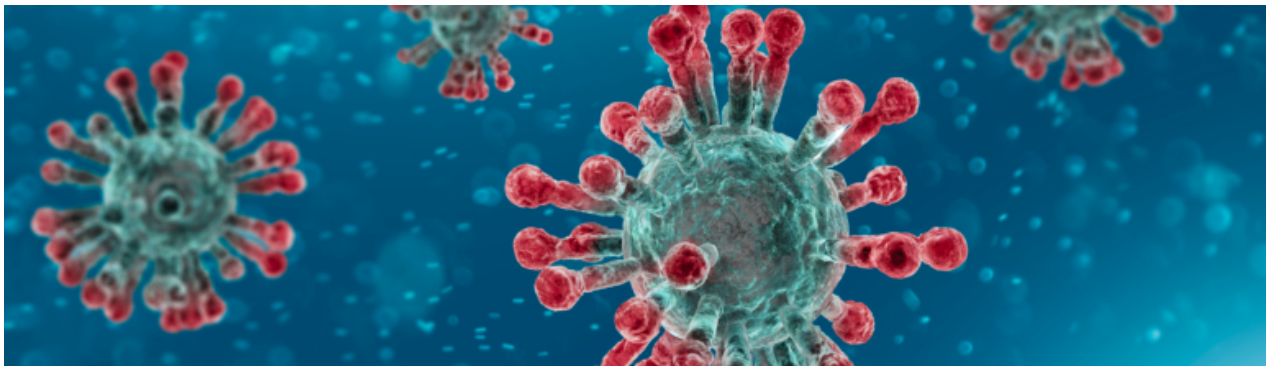
Related Practices

Trade Secrets, Computer Fraud & Non-Competes

Privacy Compliance, Litigation & Cybersecurity

Post-Pandemic Recovery & Renewal

Related Trends



Coronavirus (COVID-19)

Biometrics and Privacy Law