Coblentz
Patch Duffy
& Bass LLP

Spring 2021 Privacy Law Report

A Comprehensive Look at CCPA, CPRA, State Laws, and Recent Court Cases

Coblentz Patch Duffy & Bass LLP
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com

May 2021

Contents

Introduction

Although we are just a few months in, 2021 has already been another busy year for data privacy developments. From new regulations and legislation, to court decisions impacting privacy rights, this report takes a look at a few of the key data privacy developments so far this year.

New CCPA Regulations

Just when you thought the California Consumer Privacy Act ("CCPA") regulations were finalized, on March 15, 2021, the California Attorney General ("AG") approved additional regulations intended to enhance consumer protections for opt-outs. Most significantly, the regulations ban "dark patterns" that complicate the opt-out process, and prohibit businesses from burdening consumers with confusing language or unnecessary steps.

The revisions implement the following changes:

- *Offline Collection and Notices*: Businesses that sell personal information collected offline are now required to inform consumers in an offline method of their right to opt-out. This includes providing instructions on how to submit an opt-out request.

- *Ban on Dark Patterns or Complications to the Opt-Out Process*: Opt-out requests must "be easy for consumers to execute and shall require minimal steps to allow the consumer to opt-out." The new regulations prohibit businesses from using any method that is designed to, or has the effect of, preventing a consumer from opting out. Specifically, businesses cannot require consumers to scroll through a privacy policy or listen to reasons why they should not opt-out before confirming their request. Additionally, the opt-out process cannot require more steps than the process to opt-in to the sale of personal information after having previously opted out, or use confusing language.

- *Opt-Out Icon*: Businesses may use an opt-out icon in addition to, but not in lieu of, notice of a right to opt-out or a "Do Not Sell My Personal Information" link.

- *Requests from Authorized Agents*: A business may require an authorized agent who submits a request to "know" or "delete" to provide proof that the consumer gave the agent signed permission to submit a request.

- *Children's Information*: The regulations added the word "or" to section 999.332. As a result, businesses that sell personal information ("PI") of children under the age of 13 "and/or" between the ages of 13 and 15 are now required to define in their privacy policies how consumers can make an opt-in to sale requests.

CPRA Preparation and Compliance

In November 2020, Californians voted to enact Proposition 24, also known as the California Privacy Rights Act ("CPRA"). The CPRA[1] expands on the CCPA of 2018, establishes a new privacy regulatory agency called the California Privacy Protection Agency ("CPPA"), provides new rights for consumers, and imposes new obligations on businesses.

The CPRA's enforcement is set to begin on July 1, 2023, but the act has a look-back period to January 1, 2022. This means that data collected from January 1, 2022 is subject to the act, so businesses shouldn't wait to develop the requisite policies and procedures in response to new requirements. CPRA compliance should be a priority for every covered business. Here are a few key points that businesses need to be thinking about:

Modification to the Scope of the CCPA
The CPRA modifies the CCPA's scope in that it applies to businesses that (1) have annual gross revenue over $25 million in the preceding calendar year; (2) buy, sell, or share personal information of 100,000+ consumers or households; or (3) derive at least 50% of their annual revenue from selling or sharing consumer PI. Notably, the CPRA's threshold of 100,000 consumers or households doubles the previous threshold under the CCPA of 50,000 consumers, households, or devices, and therefore could significantly reduce the scope of the act and its impact on smaller businesses.

Cross-Context Behavioral Advertising
The CPRA introduces the concept of data "sharing," which is defined as "sharing, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration, including transactions between a business and a third party for cross-context behavioral advertising for the benefit of a business in which no money is exchanged." (Emphasis added.) The CPRA explicitly requires businesses to provide notice to consumers about data sharing practices and extends consumer opt-out rights to the sharing of personal information by a business to a third party.

Data Minimization
The CPRA introduces data minimization principles similar to those in the GDPR by prohibiting businesses from collecting more personal information than "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed . . ."[2] The CPRA also requires that businesses not retain personal information for longer than is reasonably necessary for the purpose for which it was collected, as well as to identify retention periods of data in the privacy notice to consumers.[3] Thus, all businesses should focus on making changes to limit data collection and processing of personal information to only what is reasonably necessary for the business.

[1] Read more: https://www.coblentzlaw.com/cpra-is-coming-prop-24-passes/
[2] CPRA, Section 1798.100(c).
[3] CPRA, Section 1798.100(a)(3).

Creation of California Privacy Protection Agency (CPPA)

The CPRA establishes a new enforcement agency, the CPPA. As the first agency of its kind in the United States, the CPPA will have the authority to investigate potential breaches and violations, draft enforcement regulations, and issue fines. This transfers the current CCPA and CPRA responsibilities from the Office of the Attorney General to the CPPA. Importantly, the CPRA cancels the grace period of 30 days that businesses have after being notified of an alleged breach or violation and raises the maximum on fines for violations.

Expanded Consumer Rights

Expansion of the Private Right of Action

The CPRA has expanded the scope of the private right of action by adding a cause of action for the unauthorized access and exfiltration, theft, or disclosure of an email address in combination with a password or security question and answer that could permit access to content. The act also clarifies that the implementation and maintenance of reasonable security procedures and practices following the breach do not constitute a cure.

New Consumer Rights Under the CPRA

- *Right to correct*: California residents have the right to correct inaccurate personal information the business holds about them. This mirrors the right to correction under the GDPR.

- *Right to know about and opt-out of automated decision making*: California residents can request access to and knowledge about how automated decision technologies work and what their outcomes are, and have a right to opt-out of the use of their PI for automated decision making.

- *Right to opt out of data "sharing"*: In addition to being able to opt out of data "selling," consumers will be able to opt out of data "sharing" for cross-context behavioral advertising purposes.

- *Right to limit use of sensitive personal information*: The CPRA introduces a new category of personal information called "sensitive personal information." This includes precise geolocation data, race, religion, sexual orientation, social security numbers, and certain health information outside the context of HIPAA. Consumers may limit the use and disclosure of sensitive personal information by businesses. Businesses may also need to add another link to their website homepage to allow consumers to exercise their rights to limit the use of their sensitive information.

Next Steps For Businesses

Update Website Links

Covered businesses will need to (1) update their "Do Not Sell My Personal Information" links to read "Do Not Sell or Share My Personal Information," and (2) include a separate link titled "Limit the Use of My Sensitive Personal Information" where such information is collected. The CPRA encourages businesses to make "a single, clearly-labeled link" that allows a consumer to swiftly and simultaneously opt-out of sale or sharing of PI and limit the use or disclosure of the consumer's sensitive PI. If a business complies with automated opt-out signals sent from browsers or other extensions then a business will not need to provide such links.

Update Contracts

Businesses will need to impose expanded duties on their service providers and contractors to protect information, comply with audit requests, and assist businesses in responding to consumer requests or other obligations. The CPRA requires all sales, sharing, and disclosures of personal information for a business purpose to be made pursuant to a contract. Even disclosures of deidentified information to any recipient will require a contract setting out clear restrictions on attempts at reidentification. To comply with these new CPRA provisions, businesses will need to (1) develop the necessary contracting materials in preparation for a contracting exercise; (2) assess all transfers of personal information to identify which provisions are

required for which recipients; and (3) begin the process of updating and negotiating the required agreements.

Conduct Additional Data Mapping
Businesses will need to identify any information that is shared, not just sold. To meet the CPRA's data minimization requirements, businesses will need to establish and comply with document retention periods. Additionally, businesses need to understand what algorithms or automated decision-making processes are being performed on personal information collected and maintained by the business.

Adjust Responses to Data Subject Access Requests
The CPRA now requires businesses to use commercially reasonable efforts to correct inaccurate personal information in response to a verifiable consumer request. As a result, businesses must be prepared to adjust their response procedures or be ready to explain why they cannot meet a consumer request because, "doing so proves impossible or would involve a disproportionate effort."

Businesses should also start preparing processes for how they will respond to California consumers who exercise their new privacy rights which include "do not share" requests, correction requests, and requests to limit the use of sensitive data. Finally, with more state privacy laws looming, many businesses will need to consider whether a "California versus everyone else" approach still makes sense for their business.

Assess High-Risk Activities
Per the CPRA, the California AG will at some point issue regulations requiring businesses whose processing poses "significant" risks to consumer privacy and security. These "high-risk" businesses will then need to perform annual security audits and submit regular risk assessments to the new CPPA. Companies that collect large volumes of sensitive data should start designing internal audit procedures in anticipation of this requirement. More details on this to come.

Update Do-Not-Track and Advertising Models
Businesses will need to anticipate and prepare their models for what advertising looks like with fewer cookies, tags, and pixels. They will also need to start reacting to Do-Not-Track signals and may need to adopt new opt-in marketing strategies. Given the volume of work this may entail, businesses should commence this earlier rather than later so as not to run into compliance issues when enforcement of the CPRA begins.

More State Legislation Regarding Data Privacy

The landscape of privacy law and compliance issues are changing rapidly as many states beyond California are enacting or contemplating new, more comprehensive privacy legislation similar to the CCPA/CPRA.

Virginia Privacy Law
Virginia became the second state to pass comprehensive data privacy legislation when it enacted the VCDPA on March 2, 2021. The VCDPA applies to entities that conduct business in Virginia or produce products or services that are targeted to Virginia residents and either (1) control or process the personal data of at least 100,000 consumers during a calendar year, or (2) control or process the personal data of at least 25,000 consumers and derive at least 50% of gross revenue from the sale of personal data. The VCDPA provides consumers rights of access, correction, deletion, data portability, appeal, and exclusion. Because the Act does not provide for any exceptions to these rights, businesses are expected to comply regardless of the hardship posed or the impractical nature of the request.

To best prepare for these eventualities, businesses will need to update their policies that address the new obligations imposed upon them under the VCDPA including data minimization, purpose limitations, security controls, express consent requirements, and data protection assessments. Given that the VCDPA goes into effect in two years, businesses are strongly advised to start evaluating their current data processing activities and begin developing a compliance program that meets the requirements of the VCDPA.

Other States Introducing Privacy Laws
As the internet and new technologies continue to raise questions about privacy and use of PI, state lawmakers are trying to keep up by addressing novel privacy issues through legislation.

California's and Virginia's legislatures are not the only ones paying attention to these shifting tides in the privacy law landscape. Several states, including Washington, Oklahoma, Connecticut, Florida, Illinois, and New Jersey currently have active bills awaiting committee hearings or votes. Other states such as Alabama, Arizona, Colorado, Kentucky, Maryland, Massachusetts, Minnesota, New York, Rhode Island, South Carolina, Texas, Utah, Vermont, and West Virginia recently introduced comprehensive privacy acts to state legislatures. Progress on these laws should be monitored closely over the next few months.

Status of a Federal Privacy Law
And, of course, no update would be complete without monitoring federal privacy legislation. Congresswoman Suzan DelBene (WA) introduced the Information Transparency and Personal Data Control Act on March 10, 2021, which would create a national data privacy standard for the protection of personal information, including information related to financial, health, genetic, biometric, geolocation, sexual orientation, citizenship and immigration status, social security numbers, and religious beliefs, as well as information about minors.

Given the potential patchwork of state laws mentioned above, many businesses would welcome a uniform standard, but the timing on when a comprehensive federal law will actually be enacted remains unclear. For now businesses must closely monitor the various state laws being passed and determine what laws they may need to comply with.

Recent Court Decisions Regarding Privacy

Data privacy litigation remains active, and recent court decisions have provided some clarity and guidance regarding the scope of certain privacy laws.

Scope of CCPA's Private Right of Action
Certain recent court rulings have limited the scope of the CCPA's private right of action. For example, in *Gardiner v. Walmart Inc. et al*, No. 4:20-cv04618 (N.D. Cal.),[4] defendants secured a ruling rendering a narrow interpretation of the CCPA. In Gardiner, a Walmart customer sued the retail company under the CCPA for failing to implement and maintain reasonable and appropriate security procedures and practices to protect information he gave to Walmart to create an account on the company's website. Gardiner claimed that his personal information had been subject to unauthorized exfiltration on Walmart's website and sold on the dark web, exposing him to purportedly ongoing risk of financial fraud and identity theft. On March 5, 2021, the District Court for the Northern District of California dismissed Gardiner's claim for damages under the CCPA on two grounds. First, the court could not determine whether the alleged breach occurred before or after the effective date of the CCPA because the complaint did not specifically allege a date when the purported breach occurred. Second, the court held that in order to state a viable CCPA claim, a plaintiff must allege specific, unauthorized disclosure of "personal information." This could indicate that courts will strictly interpret the CCPA to apply only where the specific categories of personal information listed in the law are actually exposed in a data breach. However, it is important to note that the court granted the Plaintiff leave to amend, allowing the Plaintiff to potentially cure the complaint's shortcomings and perhaps get a second shot at litigating his claims.

In *McCoy v. Alphabet, Inc. et al.*, No. 5:20-cv-05427 (N.D. Cal.),[5] the court held that there is no general private right of action under CCPA. Plaintiff Robert McCoy had filed a class action complaint against defendants Alphabet Inc. and Google LLC for monitoring and collecting the sensitive personal data of Android Smartphone users when they interact with non-Google applications on their smartphones, without first obtaining users' consent. In its February 2, 2021 order denying in part and granting in part the Defendants' motion to dismiss, the court emphasized that the Plaintiff had not pled a data security incident and had conceded during arguments that the CCPA claims should be dismissed because no data breach occurred. The order states that the CCPA, "confers a private right of action for violations of section [Cal. Civ. Code § 1798.150](a), which is related to personal information security breaches. Further, it explicitly states that '[n]othing in this title shall be interpreted to serve as the basis for a private right of action under any other law.' Cal. Civ. Code § 1798.150(c)." Whether this reasoning is adopted in other cases remains to be seen.

Standing in Data Privacy Cases
At the Circuit Court level there is currently ongoing dialogue regarding whether data breach victims can establish a right to sue merely by showing that they are at increased risk of identity theft.

[4] See: https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3423&context=historical
[5] See: https://www.severson.com/wp-content/uploads/2021/02/McCoy-v.-Alphabet-Inc.-et-al-Order-on-Motion-to-Dismiss.pdf

The Second Circuit Court of Appeals recently issued a decision in *McMorris v. Carlos Lopez & Assocs.*, 2021 U.S. App. LEXIS 12328 (2d Cir. Apr. 27, 2021) clarifying that the risk of identity theft after a data breach may be grounds to sue. The latter notwithstanding, the court affirmed the dismissal of a proposed class action against a veteran's health services company over an accidentally sent email that contained workers' social security numbers. In the summer of 2018, Defendant's employee accidentally sent an email to 65 others at the company. Attached to the email was a spreadsheet containing sensitive personally identifiable information of approximately 130 current and former employees. Three plaintiffs whose information had been disclosed filed suit. They asserted claims for negligence, negligence per se, consumer protection, and other state law claims on behalf of California, Florida, Texas, Maine, New Jersey, and New York classes. Upon the Defendant's motion the District Court dismissed the case for lack of subject matter jurisdiction. An appeal to the Second Circuit followed.

On appeal, the Second Circuit noted that it has been "suggested" that there is a circuit split on standing in the data breach context concerning whether a plaintiff may establish standing based on a risk of future identity theft or fraud stemming from the unauthorized disclosure of that plaintiff's data. However, the court found that "requiring plaintiffs to allege that they have already suffered identity theft or fraud as the result of a data breach would seem to run afoul of the Supreme Court's recognition that '[a]n allegation of future injury may suffice' to establish Article III standing 'if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur.'" The Second Circuit then went on to hold that in the abstract, "plaintiffs may establish standing based on an increased risk of identity theft or fraud following the unauthorized disclosure of their data."

The Second Circuit's decision contrasts somewhat with the Eleventh Circuit's recent opinion in *Tsao v. Captiva MVP Restaurant Partners*, LLC, 986 F.3d 1332, 1339 (11th Cir. 2021)[6] holding that a plaintiff alleging a threat of future identity theft or other harm lacks Article III standing unless the hypothetical harm alleged is either certainly impending or there is a substantial risk of such harm taking place. (Emphasis added.) The Tsao case arose out of a security breach at PDQ, a group of American restaurants owned by Captiva MVP Restaurant Partners. Within two weeks, PDQ posted a notice notifying its customers that its systems had been a victim of a cyber-attack. Tsao filed suit to recover damages stemming from the breach. The dispute in the class-action lawsuit was based on two questions. First, whether Tsao and the class of patrons of the restaurant had standing to sue because they were exposed to the future risk of identity theft, despite not suffering any misuse of their information. Second, whether Tsao's efforts to mitigate the risk of future identity theft presented a concrete injury sufficient to establish standing. The Eleventh Circuit answered no to both issues.

[6] See: https://law.justia.com/cases/federal/appellate-courts/ca11/18-14959/18-14959-2021-02-04.html

Conclusion

In sum, we're off to a fast and furious start to 2021, but more is coming. This ever-changing area of the law requires businesses to take proactive measures now to prepare themselves for the compliance obligations coming their way. Stay tuned for further developments. If your company needs assistance with any privacy issues, Coblentz Cybersecurity and Data Privacy attorneys can help. Please contact Scott Hall at shall@coblentzlaw.com for further information or assistance.

Authors

Scott C. Hall

Head of Cybersecurity & Data Privacy Group
Partner
San Francisco

Contact
415.772.5798
shall@coblentzlaw.com

Mari S. Clifford

Associate
San Francisco

Contact
415.268.0504
mclifford@coblentzlaw.com

Coblentz Patch Duffy & Bass LLP
One Montgomery Street, Suite 3000
San Francisco, CA 94104

coblentzlaw.com