Bloomberg Law®

# California Consumer Privacy Act:

## A Work in Progress, With More Changes to Come

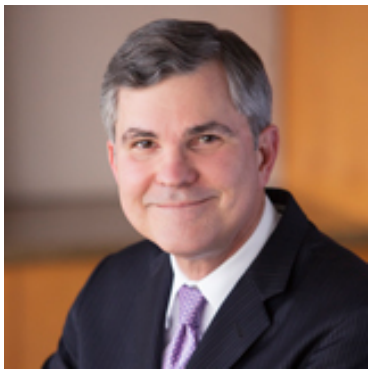
Contributed by

W. Reece Hirsch

Ellie F. Chapman

Kristin M. Hadgis

Morgan Lewis & Bockius LLP



*Reece Hirsch is a partner in Morgan Lewis's San Francisco office and co-head of its Privacy and Cybersecurity practice. He can be reached at reece.hirsch@morganlewis.com.*

*Ellie Chapman is an associate in Morgan Lewis's San Francisco office. She can be reached at ellie.chapman@morganlewis.com.*

*Kristin Hadgis is an associate in Morgan Lewis's Philadelphia office. She can be reached at kristin.hadgis@morganlewis.com.*

Bloomberg Law Privacy & Data Security

# California Consumer Privacy Act: A Work in Progress, With More Changes to Come

*Contributed by W. Reece Hirsch, Ellie F. Chapman, and Kristin M. Hadgis of Morgan Lewis & Bockius LLP.*

TABLE OF CONTENTS

Introduction ..... 1
SB 1121: The First Round of Amendments ..... 2
A. Exemptions for Medical Data ..... 2
B. Exemption for Nonpublic Personal Information Collected Pursuant to Gramm-Leach-Bliley ..... 2
C. Eliminates Notice to Attorney General Before Bringing a Private Right of Action for a Security Breach ..... 2
D. Reduction in Amount of Civil Fines ..... 3
E. Delayed Enforcement ..... 3
Open Issues ..... 3
A. Employees ..... 4
B. Commercial Customers ..... 4
C. "Specific Pieces of Information" ..... 4
D. "All or Nothing" Opt-Outs ..... 5
E. Data Use for Identity-Verification and Fraud-Detection Purposes ..... 5
F. Statutory Damages for Data Breach ..... 6
The DOJ's Public Forums ..... 6
CCPA's Progeny ..... 7

## Introduction

The January 1, 2020 effective date of the California Consumer Privacy Act (CCPA) is less than a year away and the many companies subject to the groundbreaking privacy law are understandably growing anxious. The new consumer privacy rights created by the CCPA are expansive, raising a host of operational issues for affected businesses. However, it remains difficult for businesses to commence CCPA implementation efforts because the law is still in flux, with likely legislative amendments, regulations, and guidance yet to come, and the Attorney General's office soliciting comments at public forums around the state. This article examines recent developments regarding the CCPA, and looks at some issues that will likely be a focus in the coming months now that the California Legislature is back in session.

## SB 1121: The First Round of Amendments

On September 23, 2018, California Governor Jerry Brown signed Senate Bill 1121 (SB 1121), amending the CCPA. The CCPA was enacted in June in an extremely expedited fashion, having been introduced within a week of its passage. As we previously reported, the outcome of this fire-drill process was a law that included many ambiguities and some outright errors needing correction. SB 1121 sought to do just that. Although SB 1121 does not address all of the ambiguities created by the original version of the CCPA, it clarifies some exemptions that were confusingly drafted, eliminates the requirement of notice to the Attorney General prior to asserting a private right of action, reduces the amount of civil fines recoverable, and, most importantly, effectively delays enforcement until July 1, 2020. The CCPA still remains very much a work in progress, but the enactment of SB 1121 is an important first step.

### A. Exemptions for Medical Data

As amended, the CCPA makes clear that it does not apply to protected health information ("PHI") collected by a covered entity or business associate governed by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") or the California Confidentiality of Medical Information Act ("CMIA"). Cal. Civ. Code § 1798.145(c)(1)(A). The amendments also expressly exempt "patient information" to the extent such information is maintained in the same manner as PHI or medical information subject to HIPAA or the CMIA. Cal. Civ. Code § 1798.145(c)(1)(B). While the CCPA had previously included an exemption for PHI maintained by a covered entity, SB 1121 makes clear that the exemption also applies to (1) HIPAA business associates and (2) entities that maintain medical information in accordance with HIPAA or the CMIA.

In addition, as amended, the CCPA carves out an exemption for information collected as part of a clinical trial. Cal. Civ. Code § 1798.145(c)(1)(C). Notably, as drafted, this exemption would not appear to apply to information collected pursuant to a clinical research study that is not part of a clinical trial, but that might still be subject to Federal Policy for the Protection of Human Subjects, also known as the Common Rule. The CCPA's new clinical trial exemption would benefit from some clarification and expansion.

### B. Exemption for Nonpublic Personal Information Collected Pursuant to Gramm-Leach-Bliley

As originally enacted, the CCPA included a confusing provision stating that it did not apply to "personal information collected, processed, sold or disclosed pursuant to the federal Gramm-Leach-Bliley Act ... if it is in conflict with that law." As amended, SB 1121 removes the "if it is in conflict" language, making clear that nonpublic personal information collected by financial institutions pursuant to the Gramm-Leach-Bliley Act ("GLBA") or the California Financial Information Privacy Act is not subject to the CCPA. Cal. Civ. Code § 1798.145(c).

### C. Eliminates Notice to Attorney General Before Bringing a Private Right of Action for a Security Breach

As originally drafted, the CCPA created a private right of action and statutory damages with respect to security breaches. More specifically, the CCPA required that a consumer bringing an action must notify the Attorney General's office within 30 days of filing. The Attorney General could then choose to prosecute the violation and notify the consumer of that decision. If the Attorney General chose not to proceed with its proposed prosecution after six months, then the consumer could proceed with the action. If the Attorney General took no action within 30 days of the filing notification, then the consumer could proceed with the action.

In response to the CCPA, Attorney General Xavier Becerra sent a strongly worded letter to lawmakers on August 22, 2018 raising "five primary concerns" with the CCPA, including "several unworkable obligations and serious operational challenges upon the Attorney General's Office." One of these concerns included the "unnecessary requirement that private plaintiffs give notice to the Attorney General before filing suit." Attorney General Becerra criticized this requirement as having "no purpose" because the courts, not the Attorney General, decide the merits of private lawsuits.

In an apparent acknowledgment of the Attorney General's concerns, SB 1121 eliminates the requirement that a consumer must first notify the Attorney General before bringing a lawsuit where that consumer's nonencrypted or nonredacted personal information was subject to a breach caused by the business's failure to "implement and maintain reasonable security procedures and practices." Cal. Civ. Code § 1798.50(a)(1). A consumer, however, is still required to provide the defendant business with 30 days' written notice identifying the alleged CCPA violation and providing an opportunity to cure, prior to bringing a civil action under the CCPA for individual or class-wide statutory damages. Cal. Civ. Code § 1798.50(b).

### D. Reduction in Amount of Civil Fines

Attorney General Becerra also took issue with the CCPA's civil penalty provision as "likely unconstitutional" because it purported to amend and modify the civil penalty provisions under the Unfair Competition Law. As revised, SB 1121 makes clear that the Attorney General may seek civil penalties of up to $2,500 for each violation of the CCPA, or $7,500 for each intentional violation. These provisions make plain the intent of the CCPA as originally enacted by eliminating a difficult-to-interpret cross-reference to another California law. SB 1121 also allows the Attorney General to seek injunctive relief. Cal. Civ. Code § 1198.155(b).

### E. Delayed Enforcement

As originally drafted, the CCPA became effective on January 1, 2020. SB 1121 expressly preserves this effective date for preemption purposes such that California localities cannot adopt laws conflicting with the CCPA. Cal. Civ. Code §§ 1798.180, 1798.199. Although the effective date remains unchanged, SB 1121 provides the Attorney General with an additional six months to (1) establish rules and procedures implementing the CCPA and (2) enforce the CCPA. These changes are likely in response to Attorney General Becerra's criticism that "the CCPA provided no resources for the AGO to carry out the rule-making – or even its implementation thereafter" within the original one-year timeframe.

Accordingly, as amended, the CCPA provides the Attorney General with an additional six months, to July 1, 2020, to adopt regulations implementing SB 1121 and precludes the Attorney General from bringing a CCPA enforcement action until six months after the publication of the final regulations or July 1, 2020, whichever is sooner. Cal. Civ. Code § 1798.185(a), (c). Assuming the Attorney General does not issue final regulations before January 1, 2020, businesses subject to the CCPA will have an additional six-month grace period to plan for compliance. Importantly, however, consumers could still bring a private right of action against a defendant business if a security breach occurs during this six-month grace period. Cal. Civ. Code § 1798.150.

## Open Issues

SB 1121 addresses some of the ambiguities created by the original version of the CCPA but fails to grapple with others. The following outstanding issues and ambiguities are likely to be subjects of

discussion moving forward, as highlighted in an August 6 letter to Senator Bill Dodd, one of the co-authors of the CCPA, from a consortium of California business groups that included the California Chamber of Commerce, the California Retailers Association, the California Bankers Association, the California Cable and Telecommunications Association, the California Hospital Association and the Internet Coalition (the "Business Coalition"). In addition, a consortium of advertising trade associations addressed a letter to the California Attorney General on January 31 urging modifications to provisions of the CCPA that may prove problematic for the industry. The letter was signed by the American Association of Advertising Agencies, the American Advertising Federation, the Association of National Advertisers, the Interactive Advertising Bureau, and the Network Advertising Initiative, raising concerns regarding issues such as the "specific pieces of information" and "all or nothing" opt-out matters discussed below.

### A. Employees

As originally drafted, the CCPA's definition of consumer encompasses all California residents, and without clarification could be read as including employees of a business subject to the CCPA. As argued by the Business Coalition, the inclusion of employees in the law's definition of "consumer" is arguably contrary to the law's intent as well as its text, which references "consumer data" numerous times, including in the bill's very title. As currently drafted, the definition of "consumer" is broadly defined to mean "a natural person who is a California resident, … however identified, including by any unique identifier." Cal. Civ. Code § 1798.140(g).

Such an interpretation of the CCPA may potentially result in unintended consequences. For example, as drafted, an employee accused of sexual harassment could request that complaints about him or her be expunged from company files, pursuant to the CCPA's right to delete (Cal. Civ. Code § 1798.105). Additionally, the inclusion of employees (past and current), job applicants, and other related individuals who do not have a pure "consumer" relationship with the business in the CCPA's definition of "consumer" may result in businesses needing to create separate processes for these individuals, which could result in additional and substantial operational costs.

### B. Commercial Customers

As originally drafted, the CCPA's definition of consumer could be read as including those involved in business-to-business interactions. The opportunity to delete or opt out of the disclosure of business data in a business-to-business transaction could potentially result in fraud. Moreover, it could become impossible to achieve compliance with third-party due diligence requirements under anti-corruption, anti-money laundering, export control, and Know Your Customer laws. Thus, the Chamber of Commerce and other industry groups argue that the inclusion of business customers in the CCPA's definition of "consumer" could have a chilling effect on commerce and economic opportunities for businesses based in California.

### C. "Specific Pieces of Information"

As originally drafted, the CCPA requires a business to identify "specific pieces of information" about a consumer in response to a request for access from that consumer, but the statute does not explain or define what it means by that phrase. Providing certain information, such as a consumer's Social Security number or driver's license number, in response to such a request could create unnecessary risks to both the security of the consumer's information and the business's ability to protect such information. For example, a business risks inadvertent disclosure in the event that an individual fraudulently poses as another consumer in requesting such information.

To the extent this requirement obliges a business to research and reassociate every data element in the definition of "personal information" with an identifiable individual, and/or maintain records in a form that directly identifies individuals in order to be able to respond to these requests, such a requirement may become unworkable and, further, arguably undermines the privacy intent of the statute.

### D. "All or Nothing" Opt-Outs

As enacted, the CCPA could be construed to require a business to apply a consumer's opting out of one type of sale of personal information, such as third-party cookies on a website, to another type of sale, such as a joint marketing email campaign. The Chamber of Commerce and other industry groups argue that this could potentially have unintended consequences that harm consumers. For example, if a consumer opts out of receiving online targeted ads resulting from the use of third-party cookies, unless the law is clarified, he or she might also inadvertently be deprived of special discounts and promotions for existing and new services that could save him or her money. From an operational perspective, it would seemingly also require fundamental changes to existing online self-regulatory, opt-out mechanisms. Indeed, a prior version of the ballot initiative that preceded the CCPA contained language designed to give consumers these expanded choices.

### E. Data Use for Identity-Verification and Fraud-Detection Purposes

The CCPA's opt-out and other consumer privacy rights do not provide an exception for the use of consumer data to prevent fraud or other criminal activity. The Chamber of Commerce and other industry groups argue that such an exception is needed to preserve the effectiveness of important efforts that rely on data supplied by businesses to prevent criminal activities, such as anti-fraud, sanctions, and money-laundering screening, and identity verification functions and services. If criminals are permitted to "opt out," that may have negative side effects downstream because those individuals will no longer appear in systems provided by vendors that are subject to the CCPA to warn of possible criminal activity. Such an expansive interpretation of the CCPA's opt-out right could impair anti-terrorism efforts (ensuring that people on terrorist watch lists do not have access to financing), anti-money laundering efforts and anti-fraud programs, locating persons of interest in criminal investigations, verification of identities, and law enforcement officer safety issues, such as the identification of the occupants of an address.

In addition, once a consumer has "opted out," a criminal may have an easier time fraudulently using the consumer's identity to obtain goods and services, as merchants will no longer be able to use identity-verification tools to confirm that the purchaser is whom he or she claims to be.

Moreover, without a fraud-prevention exception, the CCPA may have the unintended impact of undermining government safety-net programs that rely on data supplied by businesses, with the potential result of harming California's most vulnerable populations. Many California government entities utilize data supplied by private companies in fulfilling their missions. If an individual's personal data is unavailable for such use, the effectiveness of the associated government program may suffer. State and local government programs that may be impacted by unintended consequences due to the current language of the CCPA include Medi-Cal, the Department of Health Care Services, the Department of Social Services, Employment Development Department Program Integrity Divisions, state and county Tax Fraud Prevention and Detection programs, programs ensuring payment of child support, and foster youth programs.

### F. Statutory Damages for Data Breach

The CCPA creates a private right of action and statutory damages with respect to security breaches. Interestingly, the CCPA employs a different, and narrower, definition of "personal information" with respect to breaches than the definition applicable to the law's consumer privacy rights. The definition is drawn from California's "reasonable security law," Cal. Civ. Code § 1798.81.5. The private right of action is also triggered by an unauthorized access and exfiltration, theft or disclosure of personal information 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," language that parallels the reasonable security law. Cal. Civ. Code § 1798.150(a)(1).

As currently drafted, it appears that the CCPA's exemptions, such as those for businesses regulated under HIPAA and GLBA, do not apply to the private right of action for breaches. However, the fact that the provision appears to require a violation of "the duty" set forth in the reasonable security law begs the question: do the exceptions to that law apply to the CCPA's private right of action? The reasonable security law includes exceptions for entities regulated under HIPAA, CMIA and the California Financial Information Privacy Act, as well as other federal laws offering a greater level of protection for personal information. Cal. Civ. Code § 1798.81.5(e). This is an open issue that is of particular interest to health care and financial services companies.

## The DOJ's Public Forums

The California Department of Justice ("DOJ") conducted six public forums across California to solicit comments on the CCPA between January 8 and February 13. The first such forum, held in San Francisco on January 8, was slightly anticlimactic for the approximately 150 people who attended. The DOJ offered no commentary or insights regarding its views on, or approach to, the CCPA. The forum, which was scheduled for three hours, concluded after about an hour and 15 minutes, with fewer than 15 people offering comments. The DOJ, did, however, identify these seven areas of focus for CCPA rule-making:

1. the categories of personal information that will be subject to the CCPA;
2. the definition of "unique identifiers";
3. exceptions to the CCPA;
4. submitting and complying with consumers' requests;
5. developing a uniform opt-out logo or button;
6. what notices and information businesses must provide to consumers; and
7. how businesses will need to verify consumers' requests.

Attendees at the forum raised many of the open issues identified above in this article. Several presenters urged that the CCPA's requirements be more closely aligned with existing privacy regimes, particularly the European Union's General Data Protection Regulation (GDPR), by adding some form of GDPR safe harbor.

Consumer privacy advocacy organizations also voiced their concerns at the forum. The CCPA's nondiscrimination provisions permit a business to charge those consumers who exercise their rights different rates or to provide different levels of service as long as the price or difference is directly related to the "value provided to the consumer by the consumer data." Cal. Civ. Code § 1798.135(a)(2). One commenter noted that such differing rates could impose a disproportionate burden on low-income consumers, particularly if they seek to opt out of the sale of their personal information across multiple platforms.

## CCPA's Progeny

Many innovative California privacy and security laws, such as the state's security breach notification statute, have inspired a groundswell of similar laws in state legislatures across the country. It remains to be seen whether the CCPA will set a precedent that is followed by other states, but several bills already have been introduced that seem to be influenced to one degree or another by the California law. New Jersey Senate Bill 2834, introduced on July 23, 2018, requires commercial websites and online services to notify customers of collection and disclosure of personally identifiable information and allows customers to opt out. New York Senate Bill 224, introduced on January 9, 2019, also known as the "right to know act of 2019," would require a business to make available, free of charge, access to, or copies of, all of the customer's personal information retained by the business.

The most expansive of the new bills, and the one that most closely parallels the CCPA, is New Mexico Senate Bill 176, which includes a right of access and right to delete personal information, a right to opt out of the sale of personal information, and a private right of action for security breaches, and a similar effective date of July 1, 2020 for most provisions. If the New Mexico, New York and New Jersey measures gain traction in their legislatures and other states follow suit, the US privacy regulatory landscape could quickly become much more complex and challenging for businesses, driving interest in a comprehensive federal privacy law.

The CCPA remains very much a work in progress, and many issues remain to be resolved. Nevertheless, with January 1, 2020, the CCPA's earliest possible enforcement date, fast approaching, businesses must continue to watch the CCPA's progress closely and take the steps that can be taken at this time to prepare for the law's array of groundbreaking new consumer privacy rights.

_____

*Reece Hirsch (reece.hirsch@morganlewis.com) is a partner in Morgan Lewis's San Francisco office and co-head of its Privacy and Cybersecurity practice. Ellie Chapman (ellie.chapman@morganlewis.com) is an associate in the firm's San Francisco office, and Kristin Hadgis (kristin.hadgis@morganlewis.com) is an associate in its Philadelphia office.*

Bloomberg Law®

To learn more about Bloomberg Law®,
contact your representative at 888.560.2529
or visit www.bna.com/bloomberglaw/