AN A.S. PRATT PUBLICATION
FEBRUARY/MARCH 2019
VOL. 5 • NO. 2

PRATT'S PRIVACY & CYBERSECURITY LAW REPORT

LexisNexis®

Pratt's Privacy & Cybersecurity Law Report

VOLUME 5 **NUMBER 2** **FEBRUARY/MARCH 2019**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please contact:

Deneil C. Targowski at	908-673-3380
Email:	Deneil.C.Targowski@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at	(800) 833-9844
Outside the United States and Canada, please call	(518) 487-3385
Fax Number	(800) 828-8341
Customer Service Web site	http://www.lexisnexis.com/custserv/

For information on other Matthew Bender publications, please call

Your account manager or	(800) 223-1940
Outside the United States and Canada, please call	(937) 247-0293

ISBN: 978-1-6328-3362-4 (print)
ISBN: 978-1-6328-3363-1 (eBook)

ISSN: 2380-4785 (Print)
ISSN: 2380-4823 (Online)

Cite this publication as:
[author name], [*article title*], [vol. no.] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [page number] (LexisNexis A.S. Pratt);
Laura Clark Fey and Jeff Johnson, *Shielding Personal Information in eDiscovery*, [5] PRATT'S PRIVACY & CYBERSECURITY LAW REPORT [37] (LexisNexis A.S. Pratt)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

An A.S. Pratt™ Publication
Editorial

Editorial Offices
630 Central Ave., New Providence, NJ 07974 (908) 464-6800
201 Mission St., San Francisco, CA 94105-1831 (415) 908-3200
www.lexisnexis.com

MATTHEW BENDER

(2019–Pub. 4939)

Editor-in-Chief, Editor & Board of Editors

Pratt's Privacy & Cybersecurity Law Report is published nine times a year by Matthew Bender & Company, Inc. Periodicals Postage Paid at Washington, D.C., and at additional mailing offices. Copyright 2019 Reed Elsevier Properties SA, used under license by Matthew Bender & Company, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact LexisNexis Matthew Bender, 1275 Broadway, Albany, NY 12204 or e-mail Customer.Support@lexisnexis.com. Direct any editorial inquires and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Privacy & Cybersecurity Law Report,* LexisNexis Matthew Bender, 630 Central Ave., New Providence, NJ 07974.

The California Consumer Privacy Act

Dominique Shelton Leipzig, Sari Ratican, and Laura Mujenda*

The California Consumer Privacy Act that will go into effect on January 1, 2020, goes well beyond the EU's General Data Protection Regulation. It requires companies that handle data analytics that target California consumers' data to respond to eight specific consumer rights, observe restrictions on data monetization business models, and update their privacy notices to provide detailed disclosures about the data handling practices of California consumers' personal information. The authors of this article explain the Act.

Does your company handle data analytics to target California consumers? If so, it is imperative that you pay close attention to the California Consumer Privacy Act ("CCPA") that goes into effect on January 1, 2020. The CCPA goes well beyond the General Data Protection Regulation ("GDPR"); however, if you've achieved compliance with the GDPR, you are well on your way to achieving CCPA compliance.

Once in effect, the CCPA will require businesses processing the personal information ("PI") of 50,000 or more California consumers (defined as California residents) to comply with new regulations governing the processing of their PI. Businesses will have to respond to eight specific consumer rights, observe restrictions on data monetization business models, and update their privacy notices to provide detailed disclosures about the data handling practices of California consumers' PI.

BACKGROUND

The impetus for the CCPA was a growing concern for the volume of data collected about California consumers. In June 2018, the initiative qualified for the ballot with 629,000 signatures, nearly twice the signatures required. To facilitate amendments and respond to heavy criticism regarding workability, the ballot initiative was withdrawn from the November 2018 ballot in exchange for California Assembly Bill ("AB") 375 — the first iteration of the CCPA. On June 28, 2018, Governor Brown signed the AB 375 bill into law.

Shortly thereafter, California Senate Bill ("SB") 1121 was introduced to amend the CCPA in four ways:

[*] Dominique Shelton Leipzig (dsheltonleipzig@perkinscoie.com) is a partner at Perkins Coie LLP and co-chair of the firm's Ad Tech Privacy & Data Management group providing privacy and cyber-preparedness compliance counseling, and defending, counseling, and representing companies on privacy, global data security compliance, data breaches and investigations. Sari Ratican (sratican@perkinscoie.com) is senior counsel at the firm and a Certified Information Privacy Professional maintaining a global privacy and data protection practice. Laura Mujenda (lmujenda@perkinscoie.com) is a privacy and data security associate at the firm.

1. Eliminating the requirement that a consumer bringing a private right of action first notify the Attorney General;
2. Including a carve out for providers of health care governed by the California Confidentiality of Medical Information Act;[1]
3. Carving out any conflicts with the California Financial Information Privacy Act;[2] and
4. Limiting civil penalties assessed in an Attorney General action to not more than $2,500 per violation or $7,500 per each intentional violation.

On September 23, 2018, Governor Brown signed SB 1121 into law. Nevertheless, further amendments are likely forthcoming as the current amendments do not address all the concerns raised by industry and consumer groups, as well as the California Attorney General, Xavier Becerra.

CCPA BASICS

The CCPA gives California consumers[3] eight new privacy rights and imposes eight corresponding as well as three independent obligations on businesses processing California consumers' PI. Among other rights, it gives California consumers the right to request that a business provide the requesting consumer the categories and specific pieces of PI it collects about them, the categories of sources from which that information is collected, the business purposes for collecting or selling the information, and the categories of third parties with which the information is shared. Further, consumers have a right to request that a business that sells or discloses their PI for a business purpose, disclose the identity of third parties to which the information was sold or disclosed.

Under the CCPA, businesses must verify the requesting consumer's identity, promptly act on the consumer's request, and update its general privacy policy to include (amongst other items) a description of California consumers' rights, the purpose(s) of PI collection, and the categories of PI sold, collected or disclosed for a business purpose in the past 12 months. Businesses also have an obligation to provide the requested PI in a readily-usable and portable format and respect consumers' choice to opt out of the sale of their PI. The CCPA prohibits businesses from discriminating against consumers who exercise their rights under the CCPA. Finally, the CCPA compels businesses to train employees, create designated methods for consumers to assert their rights under the CCPA, and to execute written agreements with third party data processors to prohibit the selling, retaining, using, or disclosing the PI subject to the agreement.

[1] Cal. Civ. Code Section 1798.145(c)(1)(A)-(B).

[2] Cal. Civ. Code Section 1798.145(e).

[3] Cal. Civ. Code Section 1798.140(g) (defining "consumer" as a natural person who is a California resident); Cal. Code Regs. Tit. 18, Section 17014.

The CCPA expands the definition of PI beyond the GDPR and well beyond current US privacy law. It defines PI as "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*"[4] (emphasis added). The definition also includes personal identifiers, IP addresses, commercial information, records of personal property, products or services purchased, obtained or considered, or other purchasing or consuming histories or tendencies; internet or other electronic network activity information, professional or employment-related information; or any consumer profile.

In addition to the business obligations under the CCPA, businesses are provided with several general defenses and applicable exemptions to consumer requests and enforcement actions.

Eight Consumer Rights

The CCPA provides consumers with the eight exercisable rights regarding their PI being held by a business as follows:

1. *Abbreviated Disclosure Right Applicable to Businesses that Collect PI* – Provides a consumer the right to request that a business disclose the categories and specific pieces of PI collected about them.[5]
2. *Expanded Disclosure Right Applicable to Businesses that Collect PI* – Provides a consumer the right to request that a business disclose the categories and specific pieces of PI collected, sources from which the PI is collected, the business or commercial purpose (similar to legitimate interests under the GDPR) of collection, and to whom the collected PI is shared (i.e., third party sharing).[6] Consumers have the right to receive a specific notice of the business' PI collection practices[7] as well as notice of these rights within the business' general privacy policy.
3. *Right to Request Information from Businesses that Sell or Disclose PI for a Business Purpose* – Provides consumers the right to request that a business disclose for the previous 12 months: the categories of PI collected and sold; the categories of third parties to whom data is sold; and, the categories of PI disclosed about the consumer for a business purpose.[8] Consumers have the right to receive specific notice of the business' PI collection practices as well as notice of these rights within the business' general privacy policy.[9]

[4] Cal. Civ. Code Section 1798.140(o).

[5] Cal. Civ. Code Section 1798.100(a).

[6] Cal. Civ. Code Section 1798.110(a).

[7] *Id.*; Cal. Civ. Code Section 1798.110(c) Legislative Digest at p. 91; and 1798.130(a)(5)(B).

[8] Cal. Civ. Code Section 1798.115(a).

[9] Cal. Civ. Code Section 1798.115(c); and Cal. Civ. Code Section 1798.130(a)(5)(C).

4. *Right to Opt-Out of the Sale of Data* – Gives consumers or their authorized agent the ability to direct businesses to stop selling their PI to third parties.[10] Consumers have the right to receive notice of these rights within the business' general privacy policy that must contain a separate link to the "Do Not Sell My PI" web page.[11]
5. *Right to Opt-in for Children: Business Obligation Not to Sell Children's PI Without Affirmative Authorization* – Provides that a business must obtain the opt-in consent from the child's parent or guardian before selling the child's PI.[12]
6. *Deletion Rights* – Gives consumers the right to request that a business delete their PI after receipt of a verifiable request.[13] In support of this right, consumers have the right to receive notice of their right to deletion within the business' general privacy policy.[14]
7. *Rights to Access and Portability* – Provides consumers the right to access their PI after submitting a verifiable access request.[15]
8. *Not to be Discriminated Against for Exercising Any of the Consumer's Rights under the Title* – Gives consumers the right to not be discriminated against for exercising their rights under the CCPA. Examples of discrimination include: denying goods or services to the consumer,[16] charging different prices or rates for goods or services,[17] providing a different level or quality of goods or services to the consumer,[18] or suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services.[19]

Eight Corresponding Business Obligations

To support consumers' new rights, the CCPA has imposed the corresponding eight obligations. In order to appropriately respond to each request, businesses should first verify the requesting consumer's identity and the validity of the request. Only upon successful verification should businesses act upon the request-specific obligation(s).

1. *Obligation to Respond to Abbreviated Disclosure Request* – Once the requesting consumer's identity has been verified, the business must disclose and deliver the categories and specific pieces of the consumer's PI collected in the 12 months preceding the request free of charge within 45 days of receiving the verifiable

[10] Cal. Civ. Code Section 1798.120(a).

[11] Cal. Civ. Code Section 1798.135(a)(1)-(a)(2).

[12] Cal. Civ. Code Section 1798.120(c)-(d).

[13] Cal. Civ. Code Section 1798.105(a).

[14] Cal. Civ. Code Section 1798.105(b); Cal. Civ. Code Section 1798.130(a)(5)(A).

[15] Cal. Civ. Code Section 1798.100(d); Legislative Digest Section 2(i)(4).

[16] Cal. Civ. Code Section 1798.125(a)(1)(A).

[17] Cal. Civ. Code Section 1798.125(a)(1)(B).

[18] Cal. Civ. Code Section 1798.125(a)(1)(A)(C).

[19] Cal. Civ. Code Section 1798.125(a)(1)(A) (D).

request (unless an extension of an additional 45 days is obtained where necessary, and the consumer is given notice of the extension).[20] Lastly, a business has the obligation to provide the categories of PI collected in a general notice to consumers within their stated privacy policy.[21]

Here, the CCPA goes beyond GDPR Article 13 by requiring identification of specific pieces of information about the consumer and requires special notice to individual consumers outside of a privacy policy. And unlike GDPR Article 20 which entitles the data subject to "receive" the data, CCPA's *Abbreviated Disclosure Right* only calls for the company to "disclose and deliver the required information."

2. *Obligation to Respond to Expanded Disclosure Request* – Once the requesting consumer's identity has been verified,[22] the business must disclose and deliver the following information covering the 12 months preceding the request: the categories of PI collected,[23] the categories of sources from which PI is collected,[24] the business or commercial purpose for collecting or selling the PI[25] (similar to legitimate interests under the GDPR), the categories of third parties with whom the business shares PI,[26] and the specific pieces of PI the business collected about consumer.[27]

   The information must be provided free of charge within 45 days of receiving the verifiable request (unless an extension of an additional 45 days is obtained where necessary, and the consumer is given notice of the extension).[28] Disclosure must be made in writing and delivered[29] through the consumer's account with the business if the consumer maintains such an account, via postal mail or electronically at the consumer's option or in a readily-useable format that allows the consumer to transmit this information from one entity to another entity without hindrance.[30] A business must not require the consumer to create an account with the business to make a verifiable request.[31]Lastly, a business has the obligation to provide the categories of PI collected in a general notice to consumers within their stated privacy policy.[32]

[20] Cal. Civ. Code Section 1798.110(b); Cal. Civ. Code Section 1798.130(a)(2).
[21] Cal. Civ. Code Section 1798.100(b).
[22] Cal. Civ. Code Section 1798.110(b); Cal. Civ. Code Section 1798.130(a)(3)(A).
[23] Cal. Civ. Code Section 1798.110(c)(1).
[24] Cal. Civ. Code Section 1798.110(c)(2).
[25] Cal. Civ. Code Section 1798.110(c)(3).
[26] Cal. Civ. Code Section 1798.110(c)(4).
[27] Cal. Civ. Code Section 1798.110(a)(5).
[28] Cal. Civ. Code Section 1798.130(a)(2).
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] Cal. Civ. Code Section 1798.130(a)(2).

The notice of business purpose under CCPA is similar to GDPR's notice of legitimate interest. The CCPA requirement to disclose "the business or commercial purposes for collecting or selling PI" is similar to the GDPR requirement to disclose/notify data subject(s) if relying on legitimate interest to process PI.[33] The CCPA requirement to provide specific pieces of consumer PI collected "in a readily useable format that allows the consumer to transmit this information from one entity to another entity without hindrance[34] is similar to the GDPR Portability Right in Article 20. However, the GDPR is more restrictive as portability requests may only be made if the business' lawful basis for processing the PI is the data subject's consent[35] or contractual necessity.

3. *Obligation to Respond to Request for Information from Businesses that Sell or Disclose PI for a Business Purpose* – Once the requesting consumer's identity has been verified, the business must create two separate lists covering the preceding 12 months: (1) PI sold; and a separate list of (2) PI disclosed for a business purpose.[36] The information must be provided free of charge within 45 days of receiving the verifiable request (unless an extension of an additional 45 days is obtained where necessary, and the consumer is given notice of the extension).[37] In addition to responding to the requested disclosure, a business must implement two or more designated methods for consumers to submit requests for information, including at a minimum, a toll-free telephone number, and if the business maintains a website, a website address.[38] Lastly, a business that sells consumer PI or discloses it for a business purpose must disclose such within their online privacy policy.[39]

   This right goes beyond GDPR Article 13 and requires notice of specific categories of data sold or disclosed relatable to specific consumers.[40]

4. *Obligation to Respond to Request to Opt-Out of the Sale of Data* – Once the requesting consumer's (or consumer's authorized representative's[41]) identity has been verified, the business must stop selling the consumer's data unless the consumer subsequently provides express authorization for the sale of the consumer's PI.[42] A business must respect the consumer's decision to opt-out for at least 12 months before requesting that the consumer authorize the sale

[33] GDPR Art. 13(1)(d).

[34] Cal. Civ. Code Section 1798.130(a)(2).

[35] *Id.*, GDPR Art. 20(1)(a).

[36] Cal. Civ. Code Section 1798.130(a)(4)(B).

[37] Cal. Civ. Code Section 1798.130(a)(2).

[38] Cal. Civ. Code Section 1798.130(a)(1); Cal. Civ. Code Section 1798.140(i).

[39] Cal. Civ. Code Section 1798.115(c); Cal. Civ. Code Section 1798.130(a)(5)(C).

[40] *Id.*; GDPR Art. 13.

[41] Cal. Civ. Code Section 1798.120.

[42] Cal. Civ. Code Section 1798.120(c).

of the consumer's PI again.[43] An exception does exist for PI collected in connection with a consumer's exercise of an opt-out request if the PI is solely used for complying with the opt-out request.[44]

This consumer right goes beyond GDPR Article 18 which is limited to the four circumstances where a user is contesting accuracy, lawfulness, use beyond a legal claim, or contesting the legitimate interest reasoning.[45] Further, a business is required to create a separate "Do Not Sell My PI" web page with a clear and conspicuous link from their homepage that directs California consumers, or a person authorized by the consumer, to opt out of the sale of the consumer's PI.[46] This notice may also be provided through a separate home page dedicated to California consumers which discloses the California specific description of their privacy rights.[47]

5. *Obligation to Respond to Obtain Opt-In Consent for Children* – Businesses are obligated to obtain opt-in consent from a child's parent or guardian before selling the PI of a child under 13 years of age.[48]

   Under GDPR Article 8, parental (or guardian) opt-in consent is required for children under 16 years of age.[49]

6. *Obligation to Respond to Deletion Requests* – Once the consumer's deletion request has been verified, the business must delete the consumer's PI.[50] The CCPA recommends such deletion requests be fulfilled within 45 days.[51] Businesses also have an obligation to notify consumers of their deletion rights in a form that is reasonably accessible to consumers[52] via a general privacy notice or in a section specific to California Privacy Rights.[53] Additionally, businesses must implement two (2) or more designated methods for consumers to submit requests for information including, at a minimum, a toll-free telephone number and, if the business maintains a website, a website address.[54] A business is not required to comply with a consumer's deletion request if the PI is necessary for specific enumerated reasons including to complete a contractual transaction or provide a good or service requested by the consumer.[55]

[43] Cal. Civ. Code Section 1798.135(a)(5).
[44] Cal. Civ. Code Section 1798.135(a)(6).
[45] GDPR Art. 18.
[46] Cal. Civ. Code Section 1798.135(a)(1).
[47] Cal. Civ. Code Section 1798.135(b).
[48] Cal. Civ. Code Section 1798.120(d).
[49] GDPR Art. 8.
[50] Cal. Civ. Code Section 1798.105.
[51] Cal. Civ. Code Section 1798.130(a)(2).
[52] Cal. Civ. Code Section 1798.135(a).
[53] Cal. Civ. Code Section 1798.105(b); Cal. Civ. Code Section 1798.130(a)(5)(A).
[54] Cal. Civ. Code Section 1798.130(a)(1).
[55] Cal. Civ. Code Section 1798.105(b).

The CCPA's deletion right is broader than GDPR Article 17's provisions as the CCPA allows deletion requests to be made for any reason, whereas GDPR Article 17 only allows erasure requests in specific circumstances.[56]

7. *Obligations to Respond to Requests for Access and Portability* – Once the consumer's request has been verified, the business must disclose and deliver free of charge the required information via post or electronically in a portable format within 45 days of receiving the verifiable request.[57] The PI should be delivered in a readily-useable format so that the consumer may transfer their PI to another business without hindrance. A business is not required to provide PI to a consumer more than twice in a 12-month period.[58]

   This CCPA right is broader than the data portability right under GDPR Article 20 as data portability requests under the GDPR are limited to those in which the business' lawful basis for processing the PI is the data subject's consent or contractual necessity.[59]

8. *Obligation Not to Discriminate Against Consumers Exercising Their CCPA Rights* – Businesses are prohibited from discriminating against consumers exercising their CCPA rights in the following ways: denying goods or services to the consumer;[60] charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;[61] providing a different level or quality of goods or services to the consumer if they exercise their rights under CCPA,[62] A business is allowed to charge a higher price/rate or provide a different level/quality[63] if the higher price/rate or different level/quality is reasonably or directly related to the value provided to the consumer for their PI.[64] The CCPA also allows a business to offer financial incentives, including payments to consumers as compensation for the collection, sale, or deletion of PI, so long as they notify consumers of the financial incentives, clearly describe the material terms of the financial incentive program,[65] and obtain their opt-in consent.[66] It is recommended to place notice of financial incentives in a general privacy policy notice as a best practice. However, a business may not use financial incentive practices that

[56] GDPR Art. 17.

[57] Cal. Civ. Code Section 1798.130(a)(2).

[58] Cal. Civ. Code Section 1798.100(d).

[59] GDPR Art. 20.

[60] Cal. Civ. Code Section 1798.125 (a)(1)(A).

[61] Cal. Civ. Code Section 1798.125 (a)(1)(B).

[62] Cal. Civ. Code Section 1798.125 (a)(1)(A)(C).

[63] Cal. Civ. Code Section 1798.125 (a)(2).

[64] Cal. Civ. Code Section 1798.125 (b)(1).

[65] Cal. Civ. Code Section 1798.125 (b)(3).

[66] Cal. Civ. Code Section 1798.125 (b).

are unjust, unreasonable, coercive, or usurious[67] and a consumer can revoke their consent here at any time.[68]

Independent Business Obligations

Under the CCPA, businesses also have the following independent obligations:[69]

1. *Train Employees* – The CCPA requires businesses to train employees handling consumer inquiries on the requirements related to CCPA-provided consumer rights and business obligations.[70] Businesses are also obligated to ensure that employees know how to direct consumers to exercise their rights under the law.[71]
2. *Create Designated Methods for Consumers to Assert Their Rights* – Businesses must create two or more designated methods for consumers to submit requests for information, including a toll-free phone number and a website address if the business maintains a website.[72] "Designated methods for submitting requests" include a postal mailing address, email address, internet web page or portal, toll-free telephone number, or other applicable contact information, whereby consumers may submit a request or direction under the CCPA.[73]
3. *Execute Vendor Contracts Containing Specific Criteria* – Businesses who engage vendors to handle PI must execute written contracts with specific criteria with those vendors.[74] Among other requirements, the contract should prohibit vendors from selling, retaining, using or disclosing the PI outside of the direct business relationship with the business.[75] The contract must also include a certification from the vendor that he/she understands the restrictions and will comply with them.[76]

   GDPR Article 28's vendor obligations are more expansive than those required by the CCPA. Specifically, GDPR Article 28 requires businesses and vendors to enter into data processing agreements ("DPA") whereby vendors attest to:

   (i) only process personal data on the business' documented instructions;
   (ii) ensure that persons authorized to process data are subject to confidentiality obligations;
   (iii) take certain security measures;
   (iv) obtain consent for sub-vendors;

[67] Cal. Civ. Code Section 1798.125 (b)(4).
[68] Cal. Civ. Code Section 1798.125 (b)(3).
[69] Cal. Civ. Code Section 1798.130(a); Cal. Civ. Code Sections 1798.140(i) and w(2)(A).
[70] *Id.*
[71] *Id.*
[72] Cal. Civ. Code Section 1798.130(a).
[73] Cal. Civ. Code Section 1798.140(i).
[74] Cal. Civ. Code Section 1798.140(w)(2)(A).
[75] *Id.*
[76] *Id.*

(v) help respond to consumer verified requests;
(vi) help with data breach responses;
(vii) return or destroy all data at the end of services; and
(viii) provide information to demonstrate the business' compliance with the GDPR, including by allowing and contributing to audits.

General Business Defenses

The CCPA provides businesses with seven general defenses to the required obligations. Specifically, a business may assert that:

1. It is not a covered business under the CCPA;
2. It is not processing PI as defined under the CCPA;
3. It falls under one of the CCPA's applicable exemptions; and
4. The consumer request is not verifiable.

Additional general defenses include the fact that the data was collected for a single, one-time transaction and not sold or retained; the request would require the business to re-identify or otherwise link information that is not maintained in a manner that would be considered PI; and the action is by the vendor and the proper contractual language is contained in the vendor agreement.

Applicable Exemptions

In addition to the general defenses, the CCPA provides seven applicable exemptions for businesses including, but not limited to, the exemption applicable to protected medical or health information that is governed by the California Confidentiality of Medical Information Act,[77] Health Insurance Portability and Accountability Act[78] and the Health Information Technology for Economic and Clinical Health Act,[79] as well as information collected as part of a clinical trial subject to the Federal Policy for the Protection of Human Subjects.[80]

PENALTIES

The CCPA provides a private right of action for any consumer whose non-encrypted PI is subject to an unauthorized access, exfiltration, theft, or disclosure as a result of the business' failure to implement and maintain reasonable security procedures and practices.[81] Consumers may (1) recover damages not less than $100 and not greater

[77] Cal. Civ. Code Section 1798.145(c)(1)(A)-(B).

[78] *Id.*

[79] *Id.*

[80] Cal. Civ. Code Section 1798.145(c)(1)(C).

[81] Cal. Civ. Code Section 1798.150(a)(1).

than $750 per consumer per incident or actual damages, whichever is greater; (2) seek injunctive or declaratory relief; and/or (3) any other relief the court deems proper.[82]

Prior to initiating any action, a consumer must give the business 30 days' written notice identifying the specific CCPA provisions that have been or are being violated.[83] No action may be initiated if the business cures the noticed violations within 30 days of receiving notice, and gives the consumer an express written statement confirming that the violations have been cured and that no further violations will occur.[84] However, if the business violates the CCPA in breach of this express written statement, the consumer may initiate an action to enforce the statement and pursue statutory damages for each breach of the statement, as well as any other violation that postdates the statement.[85] This statement seems to contradict other sections of the CCPA, which limits a consumer's private right of action to violations related to security breaches.[86] Hopefully, further amendments to the bill will provide more clarity on this issue.

AREAS OF INFLUENCE

The Attorney General ("AG") cannot bring an enforcement action until six months after the publication of the final regulations or until July 1, 2020, whichever is sooner.[87] On August 22, 2018, the AG wrote a letter to California legislative leaders, raising a number of concerns about the CCPA.[88] SB-11221 addresses some but not all of these concerns.[89] First, SB-11221 addresses the AG's timing and resource concerns by allocating 80 percent of civil penalties and settlements collected under the law to the office and courts to offset costs.[90] Further, it mandates that the AG's enforcement actions are subject to civil penalties of not more than $2,500 for each violation or $7,500 for each intentional violation.[91]

Overall, the amendments in SB-1121 are purely technical. Further amendments are likely to be made when the legislature reconvenes in January 2019 as SB-1121 does not address all the concerns raised by the AG and consumer groups. Accordingly, businesses may want to get involved with the Better Business Bureau's lobbying efforts to influence legislative efforts.

[82] *Id.*

[83] Cal. Civ. Code Section 1798.150(b).

[84] *Id.*

[85] *Id.*

[86] Cal. Civ. Code Section 1798.150(c).

[87] Cal. Civ. Code Section 1798.185(a)(7)(c).

[88] Michael Lamb, California legislature publishes CaCPA amendments; vote scheduled for this week, IAPP Org. (Aug. 27, 2018), https://iapp.org/news/a/california-legislature-publishes-cacpa-amendments-vote-scheduled-for-this-week/?mkt.

[89] *Id.*

[90] 2017-2018 CA SB-1121(3).

[91] *Id.*

CONCLUSION

Before the CCPA goes into effect on January 1, 2020, businesses must prepare data inventories of all PI pertaining to California residents (including employees), households, and devices, as well as information sources, storage locations, usage, and recipients. Absent that discipline, CCPA compliance will not be possible. Further, more detailed requirements will be enacted during 2019 as additional revisions are debated and the AG begins implementation.