CALIFORNIA VOTERS APPROVE (ANOTHER) OVERHAUL OF CALIFORNIA CONSUMER PRIVACY LAWS: MEET THE CALIFORNIA PRIVACY RIGHTS ACT

Date: 14 January 2021

U.S. Data Protection, Privacy, and Security Alert

By: Tara C. Clancy, Paul W. Sweeney, Jr., Gregory T. Lewis

For the second time in two years, California is preparing to revolutionize its consumer privacy law framework. California voters overwhelmingly voted in favor of Proposition 24, the California Privacy Rights Act (CPRA), in the 3 November 2020 general election, approving the measure by a double-digit percentage margin—over two million votes. The CPRA's inclusion on the ballot came due to efforts from Californians for Consumer Privacy, the same organization whose consumer privacy ballot initiative in 2018 prompted the California legislature to enact the California Consumer Privacy Act (CCPA). Californians for Consumer Privacy asserted that an "assault by giant corporations" on the CCPA during the legislative process weakened the law's final, codified version, however, and therefore prompted the organization's efforts to put the issue of adopting a new consumer privacy regime in California before California voters once more.

The key provisions of the CPRA, which will not go into effect until 1 January 2023, simultaneously constitute both a strengthening and a weakening of the current regime under the CCPA. As we explained in our earlier alert on the CPRA, some provisions of the CPRA expand the CCPA's reach, enhancing the consumer privacy protections set forth in the CCPA both by clarifying rights currently existing under the CCPA and by imposing additional obligations on businesses subject to the CPRA's provisions. However, the CPRA does narrow the scope of businesses subject to the law.

Businesses have time, given the effective date of the CPRA, to determine what modifications must be made to their existing CCPA compliance efforts. The full 53-page text of the CPRA can be found here,[1] but this alert will discuss several of the highlights from the CPRA.[2] This alert also will clarify whether these key components of the CPRA constitute modifications of what currently exists in the CCPA or are entirely new proposals.

The CPRA will (eventually) replace the CCPA

The CPRA will subsume the CCPA but will not do so immediately. Most provisions of the CPRA, if adopted, will become operative on 1 January 2023.[3] The CPRA would also apply only to information collected on or after 1 January 2022, with the exception to the right of access.[4] The governing privacy regime prior to these dates will remain the CCPA.[5] The CPRA's enactment would have some immediate effects, however. First, the CPRA would extend the CCPA's exemptions for employee and business-to-business communications to 1 January 2023.[6] Second, the CPRA's provisions creating both the Consumer Privacy Fund and the California Privacy Protection Agency (CPPA) (further explained below) are already in force, as they became operative on the CPRA's effective

date—five days from the date when the California Secretary of State filed the statement of the vote for the election.[7]

New: The CPRA creates a category of "sensitive personal information"

The CPRA creates a new subcategory of personal information called "sensitive personal information"[8] and provides consumers with additional authority to limit the use and disclosure of this type of personal information.[9] Sensitive personal information includes, but is not limited to, government identification numbers (e.g., Social Security numbers, driver's license numbers, and passport numbers); debit card and credit card numbers in combination with required security or access codes, passwords, or credentials; a consumer's precise geolocation, religious beliefs, racial or ethnic origin, biometric information, sex life or sexual orientation information; and contents of a consumer's mail, email, or text messages unless that business is the intended recipient.[10]

New: The CPRA encompasses precise geolocation data

Precise geolocation data appears to be an area of particular concern under the CPRA. It is included within the definition of "sensitive personal information"[11] and is defined as "any data that is derived from a device and that is used or intended to be used to locate a consumer within a geographic area that is equal to or less than the area of a circle with a radius of one thousand, eight hundred and fifty (1,850) feet, except as prescribed by regulations."[12] The CPRA directs the California Attorney General to promulgate regulations to provide further definitions for this term, specifically to address situations where this distance is "not sufficient" to protect consumers in "sparsely populated areas" and situations "when the personal information is used for normal operational purposes, such as billing."[13]

New: The CPRA specifically targets cross-context behavioral advertising

Cross-contextual behavioral advertising is another specific focus of the CPRA. The CPRA defines "cross-context behavioral advertising" as "the targeting of advertising to a consumer based on the consumer's personal information obtained from the consumer's activity across businesses, distinctly-branded websites, applications, or services, other than the business, distinctly-branded website, application, or service with which the consumer intentionally interacts."[14] The CPRA explicitly excludes "cross-context behavioral advertising" from the definition of "advertising and marketing services" that constitute a business purpose for the collection and use of personal information.[15] This exclusion and the new definition of "sharing,"[16] which includes communicating "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," require businesses using "cross-context behavioral advertising" to provide consumers the opportunity to opt out of such use.[17]

New: The CPRA grants consumers the right to correct inaccurate information and access their personal information

The CPRA creates a right for a consumer to request a business to correct inaccurate personal information the business possesses about the consumer.[18] The CPRA directs any business that receives such a request to use "commercially reasonable efforts" to correct the inaccurate information.[19] The CPRA also grants the consumer with the "right to request the specific pieces of personal information the business has collected about that consumer," commonly known as "the right of access."[20] The CPRA instructs the California Attorney General to issue regulations that will further clarify and maximize this consumer right.[21]

New: The CPRA imposes enhanced protections regarding the personal information of consumers younger than 16 years old

The CPRA contains special protections for the information of individuals younger than 16 years old (under-16 consumers). Californians for Consumer Privacy highlights this issue as one of the critical reasons for why Californians should pass the CPRA. There are two main protections the CPRA implements with respect to under-16 consumers' information. First, the CPRA mandates that a business cannot sell or share the information of an under-16 consumer without first receiving affirmative consent from either the consumer (if the consumer is at least 13 years old) or from the consumer's parent or guardian (if the consumer is younger than 13 years old).[22] The CPRA also states that any business who "willfully disregards the consumer's age shall be deemed to have had actual knowledge of the consumer's age."[23] This provision is important for the second key protection the CPRA provides for under-16 consumers' information: substantial penalties. The CPRA increases the penalties imposed upon a business, service provider, contractor, or other person that commits violations of the CPRA with respect to an under-16 consumer's personal information when that business, service provider, contractor, or other person has actual knowledge that the consumer is under 16 years of age.[24] These penalties apply for both intentional and unintentional violations.[25] Businesses that violate the CPRA with respect to under-16 consumers' personal information can be subject to a US$7,500 fine per violation—the same penalty imposed for an intentional violation against a regular consumer and triple the amount of an unintentional violation against a regular consumer.[26]

New: The CPRA targets automated decision-making technology

The CPRA provides a blueprint for how future privacy rules will affect business's automated decision-making technology. The CPRA empowers the California Attorney General to promulgate regulations "governing access and opt-out rights with respect to businesses' use of automated decision-making technology."[27] The CPRA specifically targets two key areas for regulations to exist that address this issue. First, the CPRA contemplates regulations addressing "profiling."[28] The CPRA's text defines "profiling" as "any form of automated processing of personal information . . . to evaluate certain personal aspects relating to a natural person, and in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements."[29] It also calls for the California Attorney General to expand upon this definition through regulations.[30] Second, the CPRA also calls for regulations that "require[e] businesses' response to access requests to include meaningful information about the logic involved in s33uch decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer."[31]

New: The CPRA codifies the definition of consent

The CPRA explicitly defines what does and does not constitute as consumer "consent" for a business engaging in activities otherwise prohibited in the CPRA, including selling or sharing the consumer's personal information and opting the consumer into a financial incentive program. The CPRA states that "consent" "means any freely given, specific, informed[,] and unambiguous indication of the consumer's wishes by which he or she, or his or her legal guardian, by a person who has power of attorney or is acting as a conservator for the consumer, such as by a statement or by a clear affirmative action, signifies agreement to the processing of personal information relating to him or her for a narrowly defined particular purpose."[32] According to the CPRA, consent does not include (1) "[a]cceptance of a general or broad terms of use or similar document that contains descriptions of personal

information processing along with other, unrelated information"; (2) "[h]overing over, muting, pausing, or closing a given piece of content"; or (3) "agreement obtained through use of dark patterns."[33]

New: The CPRA allows law enforcement to request a 90-day hold for deletion

The CPRA permits law enforcement agencies to direct a business not to delete a consumer's personal information for 90 days.[34] If a business receives such a request from a law enforcement agency, it must not delete the information, even if it also receives a request to delete the personal information from the consumer.[35] Upon receiving a request to delete from the consumer, however, the business may use the information only to retain it for law enforcement.[36] The CPRA also permits a law enforcement agency to submit additional 90-day requests not to delete if the agency shows good cause and does so "only to the extent necessary for investigatory purposes."[37]

New: The CPRA requires any future amendments and regulations to maximize "consumer privacy"

The CPRA limits the extent to which subsequent legislation and executive rulemaking can dilute its provisions. Consumer privacy advocates criticized the adoption of many amendments to the CCPA that they alleged weakened the protections set forth in the original version of the CCPA.[38] For this reason, the CPRA explicitly states that any amendments to its text must be "consistent with and further the purpose of this Act."[39] The CPRA similarly directs the California Attorney General in several portions of its text to promulgate regulations "with the goal of maximizing consumer privacy."[40]

New: The CPRA creates a new administrative agency

The CPRA establishes a new administrative agency, the CPPA, "to implement and enforce" the CCPA and the CPRA (when it becomes operative and thereby replaces the CCPA).[41] The CPPA would become the first agency in the United States devoted exclusively to consumer-data privacy issues. The CPPA will consist of a five-member board appointed by high-ranking members of California's executive and legislative branches: The California Governor will appoint the chair of the board and one member, the California Attorney General will appoint one member, the California Senate Rules Committee will appoint one member, and the Speaker of the California State Assembly will appoint one member.[42] Each member of the board can serve for a maximum of eight consecutive years, and each member serves at the pleasure of their respective appointing authority.[43] The CPRA imposes several restrictions on board members following their tenure with the board.[44] Most significantly, the CPRA outlines the responsibilities with which it tasks the CPPA.[45] As one example, the CPRA instructs the CPPA to assume responsibility from the California Attorney General for promulgating, revising, and implementing regulations interpreting the CCPA and CPRA by the later of 1 July 2021 or six months after the CPPA indicates it is ready to begin rulemaking.[46] The CPRA also instills the CPPA with the authority to conduct its own hearings, subpoena witnesses and compel their testimony, take evidence, and impose fines upon any violators.[47] Before the CPPA can conduct a hearing to determine whether any violations occurred, however, the CPRA requires it (1) to provide the alleged violator with 30 days' notice that a private "proceeding held for the purpose of considering probable cause" will occur, (2) include in this notice the summary of the evidence and statements informing the purported violator of their rights both to appear in person and be represented by counsel, and (3) find probable cause of the violation at this proceeding.[48]

Modification: The CPRA covers both the sale *and* sharing of personal information

The CCPA defines a “sale” broadly: It includes “selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information to another business or a third party.”[49] For these activities to constitute a sale, however, the action must be done “for monetary or valuable consideration.”[50] The CPRA, by contrast, imposes obligations not just on businesses that “sell” personal information[51] but also upon those that “share” information “to a third party for cross-context behavioral advertising, whether or not for monetary or other valuable consideration.”[52]

Modification: The CPRA revises which businesses are subject to its provisions

Although the CPRA expands the types of businesses whose activities would be governed by the CPRA from the CCPA, the CPRA narrows the scope of businesses subject to its provisions as compared to the CCPA. An entity is subject to the CCPA if it had annual gross revenues exceeding US$25 million; bought, sold, or shared for commercial purposes the personal information of 50,000 or more consumers, households, or devices; or derived 50 percent or more of its annual revenues from selling consumers' personal information.[53] An entity could also be subject if it controlled, or was controlled by, a business that met the statute's requirements and shared common branding with that business (the “control+branding test”).[54] The CPRA maintains most of these requirements, with a few adjustments. First, the CPRA clarifies the entity must have satisfied the US$25 million annual gross revenue threshold in the previous calendar year to be a subject business.[55] Second, it changes the “50,000 consumers, households, or devices” threshold to 100,000 or more consumers or households.[56] Third, the business can qualify if it derives 50 percent or more of its revenue from selling or sharing consumers' personal information.[57] Fourth, an entity not otherwise required to be subject to the CPRA must satisfy the control+branding test and have personal information shared with it by the CPRA-subject business in order for the entity to become subject to the CPRA.[58] Fifth, the CPRA expands on the definition of “common branding” to mean not just “a shared name, servicemark, or trademark,” but “a shared name, servicemark, or trademark, such that the average consumer would understand that two or more entities are commonly owned.”[59] Sixth, the CPRA applies to a joint venture or partnership composed of “businesses in which each business has at least a 40 percent interest.”[60] There is no requirement for common branding in this scenario: “[T]he joint venture or partnership and each business that composes the joint venture or partnership shall separately be considered a single business,” and there are limitations to the sharing of personal information in this arrangement.[61] Seventh, the CPRA includes the ability for businesses that do not meet the threshold requirements of a “business” to certify voluntarily that they are compliant with the CPRA.[62]

Modification: The CPRA expands the definition of “publicly available” information

The CPRA applies a broader standard than the CCPA regarding what information is “publicly available” and therefore does not constitute personal information. The CPRA clarifies that publicly available information includes not only information that is “lawfully made available from federal, state, or local government records,” but it also includes information “that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media” and “information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience.”[63] Therefore, the CPRA states that personal information does not include publicly available information or “lawfully obtained, truthful information that is a matter of public concern.”[64]

Modification: The CPRA expands businesses' obligations regarding notices of collection

The CPRA requires a business to provide greater disclosures in their notices of collection than what currently exists in the CCPA. The CCPA requires a business to inform consumers about the categories of personal information it would be collecting and the purposes for which it would use the personal information.[65] It also prohibits a business from collecting additional categories of information or using collected personal information without providing new notice to the consumer.[66] As under the CCPA, the CPRA requires the business to provide notices of collection both to their consumers and to consumers who are otherwise exempt from the statute's provisions because they are engaged in employment-related relationships with the business: employees, job applicants, owners, directors, officers, medical staff members, and independent contractors.[67] The CPRA, however, expands on the CCPA's requirements in two respects. First, the CPRA requires the business to disclose to the consumer whether the business sells or shares the individual's personal information and the length of time it intends to retain each category of personal information or the criteria it will use to determine how long it will retain the information.[68] Second, the CPRA instructs a business to apply these requirements both to personal information and to sensitive personal information specifically.[69] The CPRA does narrow a business's obligations with the notice of collection in one respect: the requirement for a business to give new notice to a consumer to use the personal information or sensitive personal information it has collected for additional purposes now applies only in situations when the additional purposes "are incompatible with the disclosed purposes for which the personal information was collected."[70]

Modification: The CPRA imposes stricter requirements for contracts with contractors and service providers

The CPRA expands on the requirements set forth in the CCPA regarding required provisions that should be included in contracts with service providers. The CCPA required only a provision that prohibited retaining, using, or disclosing a consumer's personal information other than for the specific purposes of performing the services or as otherwise permitted under the CCPA.[71] The CPRA, by contrast, requires contracts with service providers to prohibit (1) the selling or sharing of personal information; (2) retaining, using, or disclosing the information outside the purposes specified in the contract or as otherwise permitted under the CPRA; (3) retaining, using, or disclosing outside the direct business relationship with the business; and (4) combining data it receives from the business from information it collects from another person, including the consumer.[72] Additionally, these contracts must specify that (1) the personal information sold or disclosed to the service provider is "only for limited and specified purposes[,]" (2) the service provider is subject to the CPRA and must provide the privacy protections specified therein, (3) the business retains the rights to take "reasonable and appropriate steps" to ensure the service provider uses the transferred or disclosed personal information in accordance with the CPRA, (4) the service provider must notify the business if it cannot meet its obligations under the CPRA, and (5) the business possesses the right, should the service provider be unable to fulfill its obligations under the CPRA, to "take reasonable and appropriate steps to stop and remediate unauthorized use of personal information."[73] Furthermore, unlike with the CCPA, the CPRA also applies these requirements to any contracts the business enters into with contractors.[74]

K&L Gates will continue to monitor these developments and provide additional updates regarding proposed regulations and other legislative amendments affecting the CPRA. The firm has a robust privacy, data protection,

and information management practice that handles privacy issues globally—from the GDPR to the CCPA—on a comprehensive, integrated basis. The firm also frequently publishes articles on privacy law issues, including issues arising under the current CCPA regime. Click here more information on the firm's capabilities in this area of the law.

FOOTNOTES

[1] All section references, unless otherwise stated, refer to the corresponding sections in the Ballot Initiative located in the hyperlinked text.

[2] As was the case with the CCPA, businesses will have to await the California Attorney General's Office establishing regulations, which will provide details implementing the provisions of the CPRA.

[3] *See* Section 31(a).

[4] *See id.*

[5] *See* Section 31(c).

[6] *See* Section 3.A.8; *see also* Section 15 (adding Civ. Code §§ 1798.145(m)(4) (employees) and 1798.145(n)(4) (business-to-business communications)).

[7] *See* Section 31(a)–(b).

[8] *See* Section 14 (adding Civ. Code § 1798.140(v)(1)(L)).

[9] *See*, e.g., Section 10 (adding Civ. Code § 1798.121); Section 13 (adding Civ. Code § 1798.135).

[10] *See* Section 14 (adding Civ. Code § 1798.140(ae)).

[11] *Id.*

[12] Section 14 (adding Civ. Code § 1798.140(w)).

[13] Section 21 (adding Civ. Code § 1798.185(a)(13)).

[14] Section 14 (adding Civ. Code § 1798.140(k)).

[15] *Id.* (adding Civ. Code § 1798.140(e)(6)).

[16] The complete definition of “share” is “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.” *Id.* (adding Civ. Code § 1798.140(ah)(1)).

[17] Section 21 (adding Civ. Code § 1798.185(a)(19)(A)).

[18] Section 6 (adding Civ. Code § 1798.106).

[19] *Id.* (adding Civ. Code § 1798.106(c)).

[20] Section 7 (amending Civ. Code § 1798.110(c)(5)).

[21] Section 21 (adding Civ. Code § 1798.185(a)(14)).

[22] Section 9 (adding Civ. Code § 1798.120(c)).

[23] *Id.*

[24] See Section 17 (amending Civ. Code § 1798.155(a)).

[25] *Id.*

[26] *Id.*

[27] Section 21 (adding Civ. Code § 1798.185(a)(16)).

[28] *Id.*

[29] Section 14 (adding Civ. Code § 1798.140(z)).

[30] *Id.*

[31] Section 21 (adding Civ. Code § 1798.185(a)(16)).

[32] Section 14 (adding Civ. Code § 1798.140(h)).

[33] *Id.* (adding Civ. Code § 1798.140(h)). The CPRA defines a "dark pattern" as "a user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice" and clarifies that it should be "further defined by regulation." *Id.* (adding Civ. Code § 1798.140(l)).

[34] See Section 15 (amending Civ. Code § 1798.145(a)(2)).

[35] *Id.*

[36] *Id.*

[37] *Id.*

[38] *See, e.g.,* Section 2.D.

[39] Section 25(a).

[40] Section 21 (adding Civ. Code § 1798.185(a)(11)–(12)).

[41] Section 24 (adding Civ. Code § 1798.199.10(a)).

[42] *Id.*

[43] *Id.* (adding Civ. Code § 1798.199.20).

[44] *Id.* (adding Civ. Code § 1798.199.15(f)–(g)).

[45] *See generally id.* (adding, among other provisions, Civ. Code § 1798.199.40).

[46] *See id.* (adding Civ. Code § 1798.199.40(b)).

[47] *See* Section 21 (adding Civ. Code §§ 1798.199.55, 1798.199.65).

[48] *See* Section 24 (adding Civ. Code § 1798.199.50).

[49] Civ. Code § 1798.185(t).

[50] *Id.*

[51] *See* Section 14 (adding Civ. Code § 1798.140(ad)).

[52] *See id.* (adding Civ. Code § 1798.140(ah)).

[53] Civ. Code § 1798.140(c)(1). 54 Id. § 1798.140(c)(2).

[55] *See* Section 14 (amending Civ. Code § 1798.140(d)(1)(A)).

[56] *See id.* (amending Civ. Code § 1798.140(d)(1)(B)).

[57] *See id.* (amending Civ. Code § 1798.140(d)(1)(C)).

[58] *See id.* (amending Civ. Code § 1798.140(d)(2)).

[59] *Id.*

[60] *See id.* (adding Civ. Code § 1798.140(d)(3)).

[61] *Id.*

[62] *See id.* (adding Civ. Code § 1798.140(d)(4)).

[63] *See id.* (amending Civ. Code § 1798.140(v)(2)).

[64] *Id.*

[65] Civ. Code § 1798.100(b).

[66] *Id.*

[67] *Compare* Civ. Code § 1798.145(g)(3) with Section 15 (adding Civ. Code § 1798.145(m)(3)).

[68] *See* Section 4 (adding Civ. Code § 1798.100(a)(3)).

[69] *See id.* (adding Civ. Code § 1798.100(a)(2)).

[70] *See* id. (adding Civ. Code § 1798.100(a)(3))

[71] *See* Civ. Code § 1798.140(v).

[72] *See* Section 14 (adding Civ. Code § 1798.140(ag)(1)).

[73] *See* Section 4 (adding Civ. Code § 1798.100(d)).

[74] *See* Sections 4 (adding Civ. Code § 1798.100(d)) and 14 (adding Civ. Code § 1798.140(j)(1)).

KEY CONTACTS

TARA C. CLANCY
PARTNER

BOSTON
+1.617.261.3121
TARA.CLANCY@KLGATES.COM

GREGORY T. LEWIS
ASSOCIATE

AUSTIN
+1.512.482.6809
GREG.LEWIS@KLGATES.COM

PAUL W. SWEENEY, JR.
PARTNER

LOS ANGELES
+1.310.552.5055
PAUL.SWEENEY@KLGATES.COM