Volume 4 Number 1 2021 ISSN 2398-1679

Journal of Data Protection & Privacy

Henry Stewart Publications
Ruskin House, 40-41 Museum Street,
London, WC1A 1LT, UK
Tel: +44 (0)20 404 3040
Website: www.henrystewartpublications.com

Henry Stewart Publications
North American Business Office
The Bleachery
143 West Street
New Milford, CT 06776, USA
Tel: +1 860 350 0041; Fax: +1 860 350 0039
e-mail: hsp@subscriptionoffice.com

ISSN 2398-1679

Printed in the United Kingdom by Charlesworth Press, Wakefield, UK

Contents

Papers

The California Privacy Rights Act of 2020: A broad and complex data processing regulation that applies to businesses worldwide

Received: 8th December, 2020

Lothar Determann
Partner, Baker McKenzie, USA

Lothar Determann teaches computer, internet, data privacy and commercial law at Freie Universität Berlin, the University of California, Berkeley, School of Law, and Hastings College of the Law, and he practices law as a partner at Baker McKenzie, where he has been counselling companies since 1998 on privacy law compliance and taking products and business models international. He has authored numerous articles, treatise contributions and books, including *Determann's Field Guide to Data Privacy Law* and *California Privacy Law: Practical Guide and Commentary*.

2 Embarcadero Center, Suite 1100, San Francisco, CA 94111, USA
Tel: +1 (650) 856-5533; E-mail: Lothar.Determann@bakermckenzie.com

Jonathan Tam
Senior Associate, Baker McKenzie, USA

Jonathan Tam is a senior associate at Baker McKenzie focusing on global privacy, technology transactions and cybersecurity. He started in Baker McKenzie's Toronto office in 2012 and transferred to the firm's San Francisco office in 2018. He is a co-chair of the IAPP's Silicon Valley KnowledgeNet chapter and a member of the Executive Committee of the San Francisco Bar Association's Privacy and Cybersecurity Section.

2 Embarcadero Center, Suite 1100, San Francisco, CA 94111, USA
Tel: +1 (415) 984-3883; E-mail: Jonathan.Tam@bakermckenzie.com

Abstract The California Privacy Rights Act of 2020 (CPRA) introduces sweeping changes to the California Consumer Privacy Act of 2018 (CCPA), most of which will become operative as of 1st January, 2023, with a 'look back' to 1st January, 2022. Key revisions include a new definition of 'sensitive personal information' and detailed obligations regarding the processing of sensitive personal information for non-essential purposes; a new and counterintuitive definition of 'sharing' personal information and related restrictions aimed at the digital advertising industry; new data subject rights to correct inaccurate information and opt out of the use of automated decision-making technology; new requirements to include data protection and processing terms in contracts with data recipients and vendors; new requirements regarding what privacy notices must include and how they must be furnished to data subjects; and the establishment of a new privacy authority, the California Privacy Protection Agency. Although some requirements are similar to those in other jurisdictions, some are unique in their scope and even more onerous and detailed than those of the European Union General Data Protection Regulation. For example, CCPA also applies to 'household data' and will require companies to include

California-specific language in their vendor contracts and privacy notices. This paper summarises some of the key revisions that CPRA makes to CCPA and offers practical recommendations on how companies subject to the law must comply. Companies that do business in California must comply not only with the revised CCPA but also detailed laws specific to particular sectors, industries, harms and activities.

KEYWORDS: California Consumer Privacy Act (CCPA), California Privacy Rights Act (CPRA), California Privacy Protection Agency (CPPA), cross-context behavioural advertising, right to know, right to access, right to deletion, right to correct inaccurate personal information, right to opt out of selling, right to opt out of sharing, right to restrict use and disclosure of sensitive personal information, right to opt out of automated decision-making technology, right to no retaliation

INTRODUCTION

At the general US election on 3rd November, 2020, Californians voted in favour of a proposition to enact the California Privacy Rights Act of 2020 (CPRA), which amends and reenacts the California Consumer Privacy Act of 2018 (CCPA), and establishes a new privacy authority, the California Privacy Protection Agency. CCPA and CPRA share similar origins: the privacy campaigners who proposed the 2018 ballot initiative that inspired CCPA were part of the same group who launched the 2020 ballot initiative that led to the enactment of CPRA.[1] Prior to CCPA, the United States had only enacted industry-, harm- or activity-specific privacy laws at the federal and state level. These laws were generally intended to be balanced and narrowly crafted to avoid adverse impacts on innovation, business and the freedom of information,[2] and apply to a broad range of situations and sectors, such as healthcare, financial services, children's data, website privacy policies, data security breaches, fitness trackers, automated license plate readers and supermarket club cards.[3]

CCPA and CPRA add omnibus regulations regarding the processing of personal information that are more comprehensive and rigid than even the European Union General Data Protection Regulation (GDPR) in various ways,[4] without repealing or preempting any of the now superfluous, duplicative or conflicting specific privacy laws in California. Thus, businesses in California face the worst of both worlds: onerous omnibus data processing regulations layered over a plethora of specific privacy laws.

Most CPRA provisions become operative on 1st January, 2023, although some 'look back' to 1st January, 2022, as the beginning of the period during which they apply. For example, as of 1st January, 2023, businesses must disclose certain information about what they were doing with California residents' personal information since 1st January, 2022. But, some provisions arguably become operative sooner than 1st January, 2023. For instance, as of 16th December, 2020 (the date CPRA becomes effective), businesses arguably have to provide job applicants, employees and other workers with an expanded privacy notice that includes certain details not originally required under CCPA, including the categories of sensitive personal information it collects and how long it retains personal information. The California Privacy Protection Agency will be responsible for drafting and adopting regulations by 1st July, 2022, specifying how certain requirements under the revised CCPA apply.

Most large- and medium-sized companies that do business in California will be impacted. Compliance with the European Union GDPR or other jurisdictions' privacy or data protection laws is not sufficient to meet requirements under the revised CCPA, which are prescriptive and

require companies to use counterintuitive terminology on website links and in privacy notices. For example, the revised CCPA defines 'sharing personal information' to mean disclosing personal information for cross-context behavioural advertising purposes and imposes onerous technical requirements on businesses that share California residents' personal information with other parties. The term 'sharing personal information' by itself does not imply that the disclosures are limited to cross-context behavioural advertising situations, making it important for businesses to examine CPRA and consider taking compliance steps that specifically address California privacy laws, separate from the compliance measures they might use to address other privacy laws.

This paper summarises some of the key revisions that CPRA makes to Title 1.81.5 of the California Civil Code, which codifies CCPA. The paper refers to Title 1.81.5 as effective on 1st January, 2020, as CCPA, and the version as amended or reenacted by CPRA as 'the revised CCPA'. Part 1 outlines who and what personal information the revised CCPA protects. Part 2 summarises who must comply with the revised CCPA. Part 3 describes some of the key changes and additions that CPRA makes to CCPA, with some recommendations that entities subject to the law can take to comply. Part 4 explains what sanctions and remedies are available under the revised CCPA. Any entity that does business in California should take stock of their personal information processing activities and determine how the revised CCPA impacts their privacy compliance programme, while keeping in mind that CCPA is just one of dozens of privacy laws in the state.

PART 1: WHO AND WHAT DATA IS PROTECTED?

CPRA does not significantly change the broad range of applicability of CCPA. The revised CCPA continues to protect the personal information of 'consumers', which the law defines to mean California residents,[5] and, in some cases, their 'households', which is now defined to mean 'a group, however identified, of consumers who cohabitate with one another at the same residential address and share use of common device(s) or service(s)'.[6] As the law defines 'consumer' to mean any 'natural person who is a California resident', the revised CCPA protects California residents not only in their role as consumers but also in their role as employees,[7] business contacts, patients, tenants, students and when engaging in other activities. The term 'resident' includes every individual who is in California for other than a temporary or transitory purpose, and every individual who is domiciled in California who is outside the state for a temporary or transitory purpose, subject to a number of clarifications and specifications set forth in Section 17014 of Title 18 of the California Code of Regulations.

CPRA defines 'personal information' broadly to mean 'information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household'.[8] Data can be protected even if it does not relate to a single individual (as 'households' are covered) and even if it does not contain a name. For example, annual water or energy consumption of a household, a particular employee's job description, an internet protocol (IP) address, web browsing history and 'purchasing tendencies' will be regulated as personal information if related to a particular California resident or household, even if no names are associated.

Excluded from the definition of 'personal information' are the following:

- 'Aggregate' information, which essentially means statistical information that relates to a group or category of California residents and which cannot be linked

to any particular California resident or household.[9] An example might be '30% of survey respondents like strawberry ice cream'.

- 'Deidentified' information, which essentially means information that cannot be associated with a particular California resident and which is subject to certain technical and organisational safeguards. A business that possesses deidentified information must publicly commit to maintaining the information in deidentified form.[10] An example of deidentified information might be 'one of the 100 survey respondents answered that strawberry ice cream is unhealthy', if no one kept records of the individual survey responses that could be used to identify the particular respondent.
- 'Publicly available' information, a term that CPRA expanded to mean (1) information that is lawfully made available from federal, state or local government records; (2) information that a business has a reasonable basis to believe is lawfully made available to the general public by the California resident or from widely distributed media or by the California resident; or (3) information made available by a person to whom the California resident has disclosed the information if the California resident has not restricted the information to a specific audience. CPRA added categories (2) and (3) and removed a qualification to (1) that the information be used only for a purpose compatible with the purpose for which the government record was made available.
- Lawfully obtained, truthful information that is a matter of public concern. CPRA does not define the term 'public concern', but this may potentially encompass information about public figures and information that concerns the life, health or security of others.

One CCPA section uses a different, narrower definition for the term 'personal information'. With respect to statutory damages for security breaches, CCPA refers to 'nonencrypted and nonredacted personal information, as defined in . . . Section 1798.81.5', which defines the term 'personal information' narrowly to include certain prescribed categories of personal information, such as an individual's first name or first initial and last name in combination with their social security number, medical information, payment card number with credentials, or biometric data.[11]

CCPA includes various exemptions at Cal. Civ. Code § 1798.145. CPRA adds some new exemptions, modifies some existing ones and arguably deletes a number of health-related exemptions. Examples of new and modified exemptions include the following:

- Emergency exemption: Businesses may cooperate with a government agency request for emergency access to a Californian's personal information if a natural person is at risk of death or serious physical injury, provided that certain conditions are met, including that the agency agrees to petition a court for an appropriate order within three days and to destroy the information if that order is not granted.[12]
- Household data exemptions: Businesses do not have to comply with certain obligations under the revised CCPA with respect to household data, such as to delete personal information, correct inaccurate information, or disclose how personal information is processed, sold and shared, on request.[13]
- Delayed operative date regarding human resources data and data concerning individual representatives of organisations: CCPA already delayed some compliance obligations with respect to human resources data and data concerning individual representatives of organisations to 1st January, 2021. CPRA grants businesses a further extension to 1st

January, 2023. In summary, businesses currently only have to provide 'notices at collection' to employees, workers and their emergency contacts and beneficiaries, and only have to comply with CCPA's data selling restrictions with respect to the personal information of individual representatives of organisations. All other CCPA obligations except those relating to statutory damages for privacy breaches currently do not apply to these categories of individuals in California. These exemptions were originally set to expire on 1st January, 2021, were extended to 1st January, 2022, by Assembly Bill 1281, and have now further been extended to 1st January, 2023, under CPRA.[14]

- Qualifying biomedical research studies exemption: CCPA currently does not apply to clinical trial data if certain requirements are met. CPRA expands this exemption by providing that the revised CCPA will not apply to personal information collected as part of a biomedical research study if certain requirements are met, such as that the study is conducted in accordance with certain prescribed medical research rules, and that participants' informed consent was obtained before their information is sold or shared.[15]
- Exemption regarding consumer reports and commercial credit reports: CCPA currently contains a narrow exemption regarding the sale of personal information to or from a consumer reporting agency that uses the personal information to generate a consumer report in accordance with the limitations of the Fair Credit Reporting Act (FCRA), a federal law that regulates how information may be collected, used and disclosed in the context of applications for credit, employment or insurance. The revised CCPA expands this exemption to other data processing activities and other entities that are regulated under FCRA. In addition, CPRA adds an exemption that limits the rights of owners and managers of businesses to ask commercial credit reporting agencies to delete or stop selling or sharing their contact information, as long as the credit reporting agency only uses the personal information for certain prescribed purposes.[16]
- Regulated financial activities exemption: CCPA currently exempts personal information processed pursuant to the Gramm-Leach-Bliley Act and California Financial Information Privacy Act, privacy laws that generally apply to financial institutions in relation to products or services that are used primarily for personal, family or household purposes. CPRA adds to this exemption personal information processed subject to the Federal Farm Credit Act of 1971, which relates to the financing of farms and other entities on which farming operations are dependent.[17]
- Exemptions related to processing personal information to produce a physical item: The revised CCPA provides that the rights of deletion and to opt out of sales of personal information do not apply to a business's use, disclosure or sale of particular pieces of a California resident's personal information if the California resident consented to the business's use, disclosure or sale of that information to produce a physical item, as long as certain requirements are met such as that the business incurred significant expense in reliance on the California resident's consent. The law gives the example of a school yearbook — other examples might include billboard advertisements and physical magazines.[18]
- Vehicle repairs and recalls exemption: CPRA adds an exemption that limits California residents' rights to opt out of the selling and sharing of their personal information vis-à-vis new motor vehicle dealers and vehicle manufacturers in the context of effectuating a vehicle repair covered by a vehicle warranty or a recall.[19]

- Exemptions related to the education industry: CPRA adds a couple of exemptions related to the education industry. First, the revised CCPA limits a California resident's right of deletion with respect to their grades and test scores that a business holds on behalf of a local educational agency at which the student is currently enrolled. Second, CPRA adds an exemption that limits California residents' rights to access their personal information in the context of education assessments where doing so would jeopardise the validity and reliability of that assessment.[20]
- Limitations of liability: A business that discloses California residents' personal information to a service provider, contractor or third party will not be held liable for their violation of the revised CCPA if the discloser entered into a written contract requiring the recipient to provide the same level of protection of the data subjects' rights under the statute as provided by the business, subject to certain exceptions.[21]

CPRA may have voided a number of health data-related exemptions that were passed into law in September 2020 under Assembly Bill 713. This bill was intended to clarify the interplay among CCPA and certain health-related laws and rules, including the federal Health Insurance Portability and Accountability Act (HIPAA) and its regulations. Assembly Bill 713 created exemptions relating to HIPAA business associates (ie entities that process protected health information on behalf of entities covered under HIPAA), personal information processed in regulated research studies, and patient information that was deidentified according to HIPAA's deidentification requirements. CPRA, however, states that it 'shall prevail over any conflicting legislation enacted after January 1, 2020' and that any conflicting legislation 'shall be null and void . . . regardless of the code in which it appears'.[22] The exemptions created by Assembly Bill 713 may now be invalid, as they are not found in, and therefore may be conflicting with, CPRA.

CPRA also modifies some of the exemptions that businesses may rely on when responding to data subject requests. We discuss some of these amendments in greater detail in Part 3.

PART 2: WHO MUST COMPLY?

An entity anywhere around the world has to comply with the revised CCPA if it does business in California, operates for profit, determines the purposes and means of personal information processing and exceeds one of the following three thresholds: (1) as of 1st January of any given year, it had annual gross revenues of $25mn in the preceding calendar year (as periodically adjusted by the California Attorney General to reflect Consumer Price Index increases); (2) it buys, sells or shares the personal information of 100,000 or more California residents or households; or (3) it derives 50 per cent or more of its annual revenues from selling or sharing California residents' personal information.[23] An entity that meets these requirements constitutes a 'business' subject to the statute. Currently under CCPA, threshold (2) is also met if a business receives, for its commercial purposes, personal information of 50,000 or more California residents, households or devices. CPRA's deletion of 'devices' and references to 'commercial purposes', and increase of the threshold number from 50,000 to 100,000 or more, may remove some smaller businesses from the scope of the revised CCPA.

An entity is also subject to the revised CCPA if: (1) it owns or is owned by an entity that qualifies as a 'business' based on the requirements described previously; (2) it shares common branding (ie a shared name, servicemark or trademark) with that business such that the average California resident would understand that

the entities are commonly owned; and (3) it and the business share consumers' personal information. In light of the counterintuitively narrow definition of 'sharing', fewer foreign businesses will be subjected to the revised CCPA merely because of their affiliation to a subsidiary or parent company, which some groups will find advantageous. Others, however, may lament that they can no longer rely on qualifying as one business and share personal information more freely under CCPA, given that 'selling' requires a 'third party'.[24]

The bulk of affirmative obligations under the revised CCPA apply to 'businesses', as controllers are subject to most GDPR duties, but some of the requirements under the revised statute also apply to the following categories of entities:

- A 'service provider', which is a term found in the original CCPA and which refers to an entity that receives personal information from or on behalf of the business and processes it for a business purpose pursuant to a written contract that includes certain prescribed provisions.[25]
- A 'contractor', which is a new term added by CPRA, and which refers to an entity to whom a business makes available personal information for a business purpose pursuant to a written contract that includes certain prescribed provisions.[26] The additional term 'contractor' seems intended to broaden the scope of requirements that apply to entities that either directly receive personal information from a business or to whom personal information is indirectly made available. The requirements that apply to contractors and service providers are practically identical under the revised CCPA.
- A 'third party', which is a term found in the original CCPA and refers essentially to a different entity that receives personal information from a business, based on the way in which the term is employed in the legislation. Specifically, CPRA amends the definition of 'third party' to mean 'a person who is not any of the following: (1) The business with whom the consumer [ie California resident] intentionally interacts and that collects personal information from the consumer as part of the consumer's current interaction with the business under [CCPA]; (2) A service provider to the business; or (3) A contractor'.[27]

PART 3: HOW TO COMPLY?

CPRA makes numerous changes and additions to the requirements under CCPA. The following is a description of some of the key compliance obligations that apply under the amended statute, grouped together thematically, followed by a high-level checklist that businesses may find helpful.

A. Key concepts

CPRA adds many new defined terms to CCPA, two of which are particularly relevant as background:

- 'Sensitive personal information' means certain prescribed categories of personal information about California residents, such as their social security, driver's license or passport numbers; financial account or payment card number in combination with relevant credentials; precise geolocation; racial or ethnic origin; religious or philosophical beliefs; the contents of their mail, e-mail and text messages, unless the business is the intended recipient of the communication; health, genetic and biometric data; and sexual orientation or sex life.[28] Note that the revised CCPA's definition of 'sensitive personal information' differs from GDPR's definition of 'special categories of personal data'.[29]
- 'Sharing' means disclosing a California resident's personal information by a business to a third party for cross-context behavioural advertising, whether or not for monetary or other valuable consideration.[30]

CPRA retains the term 'selling' from the original CCPA, which is defined to mean disclosing a California resident's personal information by a business to a third party for monetary or other valuable consideration.[31] The new term 'sharing' makes clear that ad tech providers cannot easily assume the role of a service provider or contractor when assisting with cross-context behavioural advertising.[32]

B. Data subject rights

CCPA currently gives California residents certain data subject rights — ie rights to request that a business provide them with certain information or to take certain actions or refrain from taking certain actions with respect to their personal information, subject to certain exceptions. Broadly speaking, the revised CCPA gives California residents affirmative rights that are similar to the rights that GDPR gives data subjects in the European Economic Area (EEA), although there are differences in their respective scope and the exceptions that businesses may rely on to deny data subject requests. The following is a summary of key additions and changes that CPRA makes to CCPA:

- The 'right to know and access' is currently found in CCPA and entitles a California resident to (i) obtain certain details about what personal information the business has about the individual and how the business processes it and (ii) receive copies of the personal information in a format that allows the individual to transmit the information to another entity without hindrance. CPRA essentially preserves the scope of the right but will also require a business to provide details about the purposes for which it shares California residents' personal information and to whom. By default, the right only applies to the personal information that the business collected during the 12-month period preceding the business's receipt of the data subject's verifiable request. But California residents will be able to exercise the right to know with respect to a period of any length (as long as the period begins no earlier than 1st January, 2022), unless doing so 'proves impossible or would involve a disproportionate effort', once the California Privacy Protection Agency adopts regulations regarding what 'impossible' or 'disproportionate effort' mean.[33]
- The 'right to deletion' is currently found in CCPA and entitles a California resident to direct a business to delete any personal information about the individual that the business collected from them. CPRA amends some of the exceptions that businesses may rely on to deny a request to delete. For example, the revised CCPA includes an exception that allows businesses to retain personal information 'to ensure security and integrity to the extent the use of the [California resident's] personal information is reasonably necessary and proportionate for those purposes'. CPRA defines the new term 'security and integrity' to mean the ability, among other things, to resist malicious, deceptive, fraudulent or illegal actions and help prosecute those responsible for such actions. A business that receives a request to delete personal information will have to notify its service providers and contractors to delete the information from their records, and these service providers and contractors are required, in turn, to notify the service providers, contractors and third parties to whom they disclosed the personal information to do the same. These obligations are subject to exceptions where discharging them would prove impossible and involve disproportionate effort.[34]
- The 'right to correct inaccurate personal information' is a new right under the revised CCPA. A business that receives a request to correct will be required to use commercially reasonable efforts to correct the inaccurate personal information. The

California Privacy Protection Agency's regulations will establish additional rules related to responding to such requests, including how concerns regarding the accuracy of the information may be resolved.[35]

- The 'right to opt out of sale or sharing' is currently found in CCPA regarding a business's sales of a California resident's personal information, and CPRA expands the right so that it also applies to a business's sharing of a California resident's personal information. Businesses that wish to sell or share the personal information of a California resident who is between 13 and 15 years of age, however, must obtain the individual's affirmative authorisation (ie opt-in consent), and businesses that wish to sell or share the personal information of a California resident who is 12 years or under require the affirmative authorisation of the individual's parent or guardian. Businesses that sell and share personal information must enable California residents to opt out of such disclosures either by posting an online link with the prescribed words 'Do Not Sell or Share My Personal Information' or acting on opt-out preference signals transmitted by the data subject via a platform, technology or other mechanism to be defined by regulation. CPRA adds a provision requiring a court or the California Privacy Protection Agency to disregard anti-avoidance steps that a business took to purposely avoid the definition of sell or share.[36] Currently, businesses that sell personal information about California residents with whom they have no direct relationship must also register with the California Attorney General's Office;[37] CPRA does not impact this requirement.
- The 'right to limit use and disclosure of sensitive personal information' is a new right under the revised CCPA which entitles a California resident to direct a business to limit its use of their sensitive information to: (1) uses necessary to perform the services or provide the goods reasonably expected by an average California resident who requests such goods or services; (2) certain operational purposes such as to 'help ensure security and integrity' if certain requirements are met, and 'to improve, upgrade, or enhance the service or device' that the business owns, manufactured or controls; and (3) as authorised by the California Privacy Protection Agency's regulations. Businesses that use sensitive personal information for any other purposes must enable California residents to exercise this right either by posting an online link with the prescribed words 'Limit the Use of My Sensitive Personal Information' or acting on opt-out preference signals transmitted by the data subject via a platform, technology or other mechanism to be defined by regulation. A business may combine its online opt-out links related to selling, sharing and processing sensitive personal information into a single link that enables opt-outs of all such activities.[38]
- 'Rights relating to a business's use of automated decision-making technology' are new rights contemplated by the revised CCPA. The California Privacy Protection Agency's regulations are to govern 'access and opt-out rights with respect to businesses' use of automated decision-making technology, including 'profiling' and requiring businesses' response to access requests to include meaningful information about the logic involved in such decision-making processes, as well as a description of the likely outcome of the process with respect to the consumer'. CPRA defines 'profiling' to include any form of automated processing of personal information to evaluate a natural person's personal aspects, including to analyse or predict their performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.[39]

- The 'right of no retaliation following exercise of CCPA rights' is currently found in CCPA and essentially prohibits a business from denying goods or services to a California resident or charging them different prices because they exercised their CCPA rights, unless they run a compliant financial incentive programme. A financial incentive programme is one in which the business offers a financial incentive to California residents as compensation for the collection, sale or retention (and now sharing) of their personal information. The financial incentive has to be reasonably related to the value to the business of the California resident's personal information and a business must obtain the California resident's prior opt-in consent before entering them into the financial incentive programme. CPRA also clarifies that the right of no retaliation means that businesses may not retaliate against employees, job applicants or independent contractors for exercising their CCPA rights, and that the above requirements apply to loyalty, rewards, premium features, discounts and club card programmes.[40]
- Timeline. CPRA preserves the 45-day timeline (with the ability to extend by another 45 days where necessary) for responding to verifiable requests to know, access and delete, and applies this timeline to requests to correct inaccurate personal information.[41] The Office of the California Attorney General's CCPA regulations currently require businesses to respond to requests to opt out of sales as soon as feasibly possible but no later than 15 business days from the date the business receives the request.[42] It remains to be seen whether the California Privacy Protection Agency's regulations will also use this timeline with respect to responding to requests to opt out of sharing and limit the use or disclosure of sensitive personal information. CPRA continues to contemplate that California residents may designate an authorised representative to exercise their rights on their behalf. A business is required to train the individuals responsible for handling the data subject requests it receives of the business's requirements under the revised CCPA.[43]
- Exemptions. CPRA adds some exemptions that may impact a business' obligations in the context of responding to data subject rights. For example, the revised CCPA states that it must not be construed to require a business, service provider or contractor to: (1) reidentify or otherwise link information that, in the ordinary course of business, is not maintained in a manner that would be considered personal information; (2) retain any personal information about a California resident if they would not retain it in the ordinary course of business; or (3) maintain information in identifiable or linkable form or obtain any data or technology to be capable of linking or associating a verifiable consumer request with personal information.[44]
- 'Service providers and contractors' have to assist businesses in connection with responding to certain data subject requests[45] but generally do not have to respond to certain data subject right requests in their role as service providers or contractors.[46]

C. Privacy disclosures

CCPA currently requires businesses to issue up to four types of privacy notices to California residents and prescribes what must be included in each and how they must be furnished to California residents. CPRA expands the types of disclosures that these notices must include and adds requirements regarding how they must be provided to California residents.

- 'Notice at collection': Before or at the point at which a business collects personal information from a California resident, it

must provide a privacy notice explaining what types of personal information it collects and the purposes of collection. CPRA will require notices at collection to include additional details, such as regarding its selling and sharing of personal information, its processing of sensitive personal information and how long it retains personal information.[47] CPRA also includes new provisions establishing how a business may furnish a notice at collection to a California resident if the individual does not directly interact with the business.[48] Although most CPRA provisions will become operative from 1st January, 2023, a specific requirement appears to require businesses to issue CPRA-compliant notices at collection to their job applicants, employees and other workers already as of 16th December, 2020.[49]

- 'Privacy policy': CCPA currently requires businesses to publish a comprehensive privacy policy that describes its online and offline practices regarding the collection, use, disclosure and sale of personal information and the rights that California residents have regarding their personal information. CPRA will require privacy policies to include additional disclosures about California residents' new rights under the revised CCPA and details about how they share California residents' personal information for cross-contextual behavioural advertising.[50]
- 'Notice of right to opt out': CCPA currently requires a business that sells California residents' personal information to provide a notice informing California residents of their right to direct the business to stop selling their personal information. CPRA expands this requirement to also apply to businesses that share personal information and to cover their sharing of personal information.[51]
- 'Notice of financial incentive': A business that offers financial incentives to California residents to collect, retain or sell their personal information must provide a notice explaining the material terms of the financial incentive programme and how the business arrived at the value of the financial incentive.[52] CPRA does not expressly amend the required contents of a notice of financial incentive.

D. Data transfer and processing terms

CPRA introduces terms that businesses must[53] or should[54] include in their contracts with business partners and vendors. A business should update its contracts so as to position as many of its vendors as 'service providers' or 'contractors', as defined under the revised CCPA, as possible. Otherwise, the business has to prepare for the likely scenario that Californians can effectively prohibit the business from using its vendors but remain entitled to the same service due to the revised CCPA's anti-discrimination provisions. Giving effect to such requests would likely be extremely burdensome or cost-prohibitive in many instances, such as where the business relies on cloud storage vendors, Software-as-a-Service providers, payroll service vendors and outsourcing service providers for essential business functions. Therefore, businesses are greatly incentivised, if not compelled, to include certain prescribed provisions in vendor agreements.

E. Proportionality and purpose limitation

CPRA generally requires that a business's collection, use, retention and sharing of a consumer's personal information be reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed, or for another disclosed purpose compatible with the context in which it was collected.[55] The revised CCPA also generally prohibits a business from collecting categories of personal information not listed in its notice at collection or using personal information for purposes that are incompatible with the

purposes set forth in the notice at collection, without providing the individual with a new notice at collection. CPRA also prohibits businesses from retaining consumers' personal information for each disclosed purpose for which the personal information was collected for longer than is reasonably necessary for that disclosed purpose.[56]

F. Data security breaches

CCPA currently entitles a California resident to recover statutory damages of between $100 and $750 or actual damages, if greater, from a business whose failure to implement reasonable and appropriate security procedures and practices caused the unauthorised access and exfiltration, theft or disclosure of certain prescribed categories of personal information about the California resident in a non-encrypted and non-redacted format.[57] These prescribed categories of personal information include, for instance, their first name or first initial and last name in combination with their social security number, medical information, payment card number with credentials, or biometric data. CPRA adds to this list of prescribed categories of personal information a California resident's e-mail address in combination with a password or security question and answer that would permit access to the account, a category that was already covered in California's data security breach notification law since 2016[58] and may have been inadvertently missed in CCPA. The revised CCPA expressly requires businesses to implement reasonable security procedures and practices, duplicating existing requirements[59] and contemplates further security-related regulations.[60]

G. Requirements on businesses whose processing presents significant risk

CPRA contemplates that special requirements shall apply to businesses whose processing of California residents' personal information presents significant risk to their privacy or security. In particular, CPRA tasks the California Privacy Protection Agency with issuing regulations that require such businesses to (1) perform a thorough and independent cybersecurity audit on an annual basis and (2) submit a risk assessment with respect to their processing of personal information to the California Privacy Protection Agency on a regular basis. CPRA contemplates that the assessment must take into account whether the processing involves sensitive personal information and identify and weigh the risks and benefits resulting from the processing.[61]

H. Record-keeping

The Office of the California Attorney General's CCPA regulations currently require businesses to maintain records of how they responded to CCPA requests for at least 24 months.[62] CPRA adds a provision to the statute permitting businesses to maintain a confidential record of deletion requests solely for the purpose of preventing the personal information from being sold, for compliance with laws, or for other purposes that the revised CCPA permits.[63] In addition, the California Privacy Protection Agency is responsible for issuing regulations 'specifying record keeping requirements for businesses to ensure compliance with' the amended CCPA.[64]

I. Compliance checklist

The following are steps that entities doing business in California should consider taking to prepare for the implementation of CPRA:

1. Take stock of current and anticipated processing activities, such as through a data inventorying or data mapping exercise.
2. Consider making strategic changes to business activities to reduce compliance obligations. Because the revised CCPA

restricts selling and sharing personal information, and using and disclosing sensitive personal information, entities may benefit from concerted efforts to avoid engaging in these activities. Also, businesses should consider relocating or deploying cutting-edge technology development to jurisdictions other than California or the European Economic Area where the amended CCPA and GDPR present insurmountable obstacles for the acquisition or sale of datasets for machine learning or autonomous driving technology development, block chains, analytics and precision medicine.[65]

3. Revise data sharing and processing agreements, including intercompany agreements.
4. Update data subject request protocols and procedures, including with respect to the rights: (1) to know and access; (2) to deletion; (3) to correct inaccurate personal information; (4) to opt out of sale; (5) to opt out of sharing; (6) to limit processing of sensitive personal information; (7) to use of automated decision-making technology; and (8) to no retaliation following exercise of CCPA rights.
5. Review financial incentives offered in exchange for the collection, selling, sharing and retention of personal information, such as in relation to loyalty, rewards, premium features, discounts or club card programmes.
6. Prepare for data minimisation, proportionality and purpose limitation requirements.
7. Update notices, including (1) notices at collection; (2) privacy policy; (3) notices of rights to opt out of selling, sharing and certain processing of sensitive personal information; and (4) notices of financial incentives.
8. Prepare for requirements regarding automated decision-making technology.
9. Upgrade and document security measures.
10. Keep up to date. The California Privacy Protection Agency is required to adopt regulations implementing CPRA by 1st July, 2022, and is tasked with providing guidance to California residents and businesses regarding the substance of the revised CCPA.

PART 4: SANCTIONS AND REMEDIES

Civil and administrative enforcement of the CPRA's additions and amendments to CCPA may only commence on or after 1st July, 2023.[66] CPRA establishes the California Privacy Protection Agency as the public agency responsible for implementing and enforcing the revised CCPA. The agency will be able to audit businesses' compliance of its own initiative or respond to third-party complaints of any person and will have a variety of powers to investigate possible violations of the revised CCPA, including to subpoena witnesses and compel the production of material books and records.[67] The agency must give parties a 30-day notice of violation before initiating an administrative hearing and must conduct an administrative hearing in accordance with the Administrative Procedure Act before determining whether a violation occurred.[68] The agency will have the authority to issue a cease-and-desist orders and order entities to pay an administrative fine of up to $2,500 for each violation or up to $7,500 for each intentional violation and each violation involving the personal information of minors.[69] The revised CCPA establishes a five-year limitation period for administrative actions.[70] Penalties paid by businesses are to be deposited in a Consumer Privacy Fund earmarked to offset government enforcement costs and support privacy education and activism.

CCPA currently establishes a private right of action for California residents affected by a security breach, as described in Part 3(F) earlier but does not create any other private rights of action, and expressly 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'.[71] This has not prevented private plaintiffs from instituting proceedings seeking remedies for CCPA violations,[72] and it remains to be seen whether courts accept such claims. CPRA maintains the private right of action relating to security breaches originally found in CCPA but does not expressly establish new private rights of action.

AUTHORS' NOTE

The authors practice law at Baker McKenzie's San Francisco office. This paper reflects the authors' opinions, not their firm's or clients'.

References and Notes

1. 'California privacy rights ballot initiative: businesses, watch this space', *The Recorder*, 22nd May, 2020, available at: https://www.law.com/therecorder/2020/05/22/california-privacy-rights-ballot-initiative-businesses-watch-this-space/ (accessed 9th January, 2021). For a summary of CCPA prior to amendments made by CPRA, see, eg, Determann, L. 'New California Law against data sharing – the California Consumer Privacy Act of 2018, broad data and business regulation', *Computer und Recht international,* 2018, p. 117, available at: https://www.degruyter.com/view/journals/cri/19/4/article-p117.xml?language=de, (accessed 9th January, 2021) and Determann, L. (2018) 'New California Law against data sharing', *The Computer & Internet Lawyer*,Vol. 353, No. 10, October 2018.
2. Schwartz, P. (2009) 'Preemption and privacy', *Yale Law Journal*,Vol. 118, pp. 916–922; Determann, L. (2020) 'Determann's Field Guide to Data Privacy Law', Fourth ed., International Corporate Compliance, Edward Elgar Publishing Limited, The Lypiatts, 15 Lansdown Road, Cheltenham, Glos GL50 2JA, UK.
3. Determann, L. (2020) 'California Privacy Law – Practical Guide and Commentary, U.S. Federal and California Law,' Fourth ed., International Association of Privacy Professionals, Chapter 2 (A-Z), Pease International Tradeport, 75 Rochester Ave., Suite 4, Portsmouth, NH 03801, USA.
4. For example, the term 'personal information' includes not only data pertaining to individuals but also 'households', and the data access right is subject to limited exceptions.
5. Revised Cal. Civ. Code § 1798.140(i).
6. *Ibid*., § 1798.140(q).
7. Determann, L. and Gupta, C. (2018) 'Impact of the California Consumer Privacy Act on employers', *Bloomberg BNA Privacy Watch*, 27th July, 2018, available at: https://news.bloomberglaw.com/privacy-and-data-security/insight-impact-of-the-california-consumer-privacy-act-on-employers (accessed 30th December, 2020).
8. Revised Cal. Civ. Code § 1798.140(v).
9. *Ibid*., § 1798.140(b).
10. *Ibid*., § 1798.140(m).
11. *Ibid*., § 1798.150.
12. *Ibid*., § 1798.145(a)(4).
13. *Ibid*., § 1798.145(p).
14. *Ibid*., § 1798.145(m) and (n).
15. *Ibid*., § 1798.145(c)(1)(C).
16. *Ibid*., § 1798.145(d) and (o).
17. *Ibid*., § 1798.145(e).
18. *Ibid*., § 1798.145(r).
19. *Ibid*., § 1798.145(g).
20. *Ibid*., § 1798.145(q).
21. Revised Cal. Civ. Code § 1798.145(i).
22. CPRA, Section 25(d).
23. Revised Cal. Civ. Code § 1798.140(d).
24. Determann, L. 'California Privacy Law – Practical Guide and Commentary, U.S. Federal and California Law', at 2.18, but see de la Torre, L. (2020) 'What is a business under CPRA?' *Medium*, 19th November, 2020, available at: https://medium.com/golden-data/what-is-a-business-under-cpra-41794347370b (accessed 30th December, 2020).
25. Revised Cal. Civ. Code § 1798.140(ag).
26. *Ibid*., § 1798.140(j).
27. *Ibid*., § 1798.140(ai).
28. *Ibid*., § 1798.140(ae).
29. EU General Data Protection Regulation, 2016/679, Article 9(1).
30. Revised Cal. Civ. Code § 1798.140(ah).
31. *Ibid*., § 1798.140(ad).
32. Freund, L. (2020) 'Agencies, brands and publishers beware: a service provider approach to CCPA is risky', AdExchanger, 21st October, 2020, available at: https://www.adexchanger.com/data-driven-thinking/agencies-brands-and-publishers-beware-a-service-provider-approach-to-ccpa-is-risky/ (accessed 30th December, 2020).
33. Revised Cal. Civ. Code §§ 1798.110, 1798.115 and 1798.130.
34. *Ibid*., §§ 1798.105 and 1798.130.
35. *Ibid*., §§ 1798.106 and 1798.130.
36. *Ibid*., §§ 1798.120, 1798.130, 1798.135 and 1798.190.
37. Determann, L. (2020) 'California data broker registrations: who made the list on Jan. 31?', *IAPP Privacy Advisor*, 11th February, 2020, available at: https://iapp.org/news/a/california-data-broker-registrations-who-made-the-list-on-jan-31/ (accessed 30th December, 2020).
38. Revised Cal. Civ. Code §§ 1798.121 and 1798.135.
39. *Ibid*., §§ 1798.140(z) and 1798.185(a)(16).
40. *Ibid*., § 1798.125.
41. *Ibid*., § 1798.130(a)(2).
42. California Consumer Privacy Act Regulations ('CCPA Regulations'), § 999.315(e).

43. Revised Cal. Civ. Code §§ 1798.130(a)(6) and 1798.135(c)(3).
44. *Ibid*., § 1798.145(j).
45. See, eg, revised Cal. Civ. Code §§ 1798.105(c)(3) and 1798.130(a)(3).
46. See, eg, revised Cal. Civ. Code §§ 1798.105(c)(3), 1798.121(c), 1798.130(a)(3)(A).
47. Revised Cal. Civ. Code § 1798.100(a).
48. *Ibid*., § 1798.100(b).
49. Section 31 of the CPRA provides that the revised Cal. Civ. Code § 1798.145(m) shall become operative on the effective date of the CPRA, which is 16st December, 2020. One interpretation of Cal. Civ. Code § 1798.145(m) is that it requires businesses to provide notices at collection to their workers and other individuals in accordance with the expanded requirements under the revised CCPA.
50. Revised Cal. Civ. Code § 1798.130(a)(5).
51. *Ibid*., § 1798.135(a).
52. Revised Cal. Civ. Code § 1798.125(b)(2) and CCPA Regulations, § 999.307.
53. Revised Cal. Civ. Code § 1798.100(d).
54. *Ibid*., § 1798.140(j) and (ag).
55. *Ibid*., § 1798.100(c).
56. *Ibid*., § 1798.100(a).
57. *Ibid*., § 1798.150; Determann, L. (2018) 'INSIGHT: Be Wary of Liability for Statutory Damages under California Consumer Privacy Act', Bloomberg Law Privacy & Data Security Law News, 6th July 2018, available at: https://news.bloomberglaw.com/privacy-and-data-security/insight-be-wary-of-liability-for-statutory-damages-under-california-consumer-privacy-act (accessed 9th January, 2021).
58. Cal. Civ. Code §1798.81.5(d).
59. *Ibid*., § 1798.81.5(b).
60. Revised Cal. Civ. Code § 1798.185(a)(15)
61. *Ibid*.
62. CCPA Regulations, § 999.317(b).
63. Revised Cal. Civ. Code § 1798.105(c)(2).
64. *Ibid*., § 1798.199.40(b).
65. See, eg, Determann, L. (2020) 'Healthy data protection', *Michigan Telecommunications and Technology Law Review*, Vol. 26, p. 229.
66. Revised Cal. Civ. Code § 1798.185(d).
67. *Ibid*., §§ 1798.199.45 and 1798.199.65.
68. *Ibid*., §§ 1798.199.50 and 1798.199.55.
69. *Ibid*., § 1798.199.55(a).
70. *Ibid*., § 1798.199.70.
71. Cal. Civ. Code § 1798.150(c).
72. Determann, L. and Michaud, T. (2020) 'CCPA litigation trends', *Bloomberg Law*, September 2020, available at: https://f.datasrvr.com/fr1/720/23011/CCPALitigationTrendsECO-66381.pdf (accessed 30th December, 2020).