GIBSON DUNN

June 15, 2022

INSIGHTS ON NEW CALIFORNIA PRIVACY LAW DRAFT REGULATIONS

To Our Clients and Friends:

At long last, and just over a month before the drafts were originally scheduled to be finalized, the California Privacy Protection Agency (CPPA) released its draft regulations for the California Privacy Rights Act (CPRA) on May 27, 2022, in advance of the CPPA's June 8, 2022 meeting. The CPRA will go into effect January 1, 2023. Finalization of the regulations before the July 1, 2022 deadline is unlikely, according to the CPPA itself, and whether this delay will impact the CPRA's enforcement date (as some commentators suggest) remains to be seen.

In August 2020, the California Attorney General released the final regulations for the California Consumer Privacy Act or CCPA, which is the comprehensive state privacy law that will be replaced by the CPRA in January 2023. The May 2022 draft CPRA regulations redline the August 2020 CCPA regulations and mostly focus on the CPRA's changes to the preexisting CCPA concepts.[1] The draft regulations offer businesses a long-awaited roadmap to compliance with the law, albeit a roadmap with clarifications and finalization that remain outstanding. Key regulations addressed by this initial draft include those relating to dark patterns, expanded rules for service providers, third-party contracts, third-party notifications, requests to correct, opt-out preference signals, data minimization, privacy policy rules, revised definitions, and enforcement considerations. But this roadmap is subject to debate and change, and is not comprehensive. Indeed, a number of key issues and inconsistencies were—to the disappointment of many observers—left unaddressed.

Days after the CPPA's release of the draft regulations, both businesses and consumers expressed desire for further clarity on key issues during the CPPA's June 8, 2022 Board Meeting, during which the Board formally voted 4-0 to begin the rulemaking process. Once the Board files the notice and it is published in the California Regulatory Notice Register, the formal rulemaking process will actually commence. Filing the notice will then begin a public comment period of at least 45 days during which stakeholders and interested parties can submit written comments, and a public hearing will be scheduled. The earliest date that the regulations theoretically could be finalized would be late July. Finalization is more likely to extend into Q3 or Q4, as additions and revisions are highly likely. At the meeting, businesses requested at least a six-month enforcement deadline extension, noting (as the Board has previously recognized) that it will necessarily miss the July 1 deadline to finalize regulations.

Below, we discuss the key changes to the regulations, then discuss two key concepts that were not addressed by the first draft. These revised regulations create significant impacts for all businesses and fill in key gaps created by the first draft of regulations. The CPPA's effort here indicates that it plans to take a very active role in defining the law and its vision of enforcement.

Table of Contents

Key Updates in the Initial Regulations

Although the regulations are subject to change, they still provide helpful guidance for businesses that can be implemented now. Below, we've highlighted what we believe to be some of the most interesting and potentially impactful draft regulations.

(1) Dark Patterns

Similar to recent discussions and writings from the FTC,[2] the CPRA sought to address issues relating to dark patterns, which the CPRA defines as "[a] user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision-making, or choice, as further defined by regulation."[3] The CPRA introduced a new concept that was not contemplated directly by the CCPA: the concept that dark patterns cannot be used to obtain valid consent (e.g., consent to track and share personal information).[4] Draft regulation Section 7004 bears a "consent" heading and makes clear that any dark patterns used to obtain consent would vitiate consent.[5] This section also concerns

dark patterns affecting "methods for submitting CCPA requests."[6] In other words, these dark pattern rules also apply to other design choices such as the form a website uses to collect correction right requests, which is potentially broader than the dark pattern concerns expressed in the CPRA.[7]

The regulations define a dark pattern as any user interface that "has the effect of substantially subverting or impairing user autonomy, decisionmaking, or choice, regardless of a business's intent" or anything that would otherwise "not comply" with the consent rules in Section 7004(a).[8] This section provides about three pages of new content (as compared to the CCPA regulations) explaining how consent may be obtained, and announces five guiding principles to avoid vitiating consent via dark patterns.[9] Specifically, user interface architecture must (1) be "[e]asy to understand[,]" (2) provide "[s]ymmetry in choice[,]" (3) "[a]void language or interactive elements that are confusing to the consumer[,]" (4) "[a]void manipulative language or choice architecture[,]" and (5) be "[e]asy to execute."[10] The regulations also include a number of illustrations and examples. The substantial subversion concept, however, still warrants further elaboration, and one commenter during the June 8, 2022 CPPA Board Meeting suggested that the Agency adopt a "design practice[] that amount[s] to consumer fraud" standard instead.

This guidance suggests that, at least in the eyes of the CPPA, many widely used business practices may violate the CCPA. Of note, according to the CPPA, dark patterns may include simply making consumers feel bad about their choices. As one example provides, "[w]hen offering a financial incentive, pairing choices such as, 'Yes' (to accept the financial incentive) with 'No, I like paying full price' or 'No, I don't want to save money,' is manipulative and shaming."[11] The "symmetry in choice" concept would also require material changes for many businesses. As one example provides, "[a] website banner that serves as a method for opting out of the sale of personal information that only provides the two choices, 'Accept All' and 'More Information,' or 'Accept All' and 'Preferences,'" is explicitly not permissible for opting out of the sale or sharing in this draft.[12] These draft regulations signal that many businesses need to start thinking now about how their consent flows may fall into these broad definitions of dark patterns, given how common such practices are.

(2) Rules for Service Providers and Contractors, Including Expanded Agreements and Service Provider Potential Liability

The draft regulations include several new and modified provisions impacting service providers and vendors, i.e., entities that collect and process data in the context of providing a service (including software-as-a-service or SaaS businesses) to another entity. The regulations impose different obligations on the service provider and on the person or entity to whom the relevant services are provided. The changes provide additional helpful detail regarding the CPRA's requirements, including: (i) expanding the applicability of service provider provisions while excluding cross-contextual advertising services; (ii) adding product or service improvements to the list of reasonable uses of personal information; and (iii) instituting explicit and specific requirements for contracts with service providers and contractors.

First, whereas the CCPA regulations applied only when the service provider provided a service to a "business"—as defined by the CCPA—the draft regulations state that a business that "provides services to a person or organization that is not a business, and that would otherwise meet the requirements and

obligations of a 'service provider' or 'contractor'" should still be considered a service provider or contractor.[13] Therefore, the provisions now also may be read to apply to a service provider whose customer is, for example, a non-profit organization and not a business. This expanded service provider definition does not apply to cross-contextual advertising services, i.e., services for online advertising where a customer provides a list of its own customers' email addresses to the vendor.[14] In that case, the vendor would not be considered a service provider, even if it otherwise met all of the requirements, if the customer was not a "business." Advertising services that do not rely on any transfer of personal information provided by the business are not considered cross-contextual advertising services.

This suggests that the draft intends service providers to be covered by the CPRA, even if its customers are not; nonetheless, service providers also have significantly reduced obligations under the CCPA and CPRA, as compared to a business. For example, because a service provider does not determine the means and processing of the personal information it receives, it does not have to ensure that the information is being retained and processed only in the manner and for the purposes for which consent was obtained or disclosures were properly made. Those concerns remain the province of the entity providing the information and may flow through to the service provider, but are not as restricting. Still, the CPRA is of interest to all parties, in applying varying levels of requirements on entities processing personal information.

Second, in what may be a significant relief to many service providers, the draft regulations would explicitly allow service providers to use data, including personal information, obtained from one customer to improve the product or service for all customers, provided the personal information is not "used to perform services on behalf of another," such as by marketing to the business' customers on behalf of another company.[15] Without this allowance, service providers may have been forced to include provisions in their agreements with businesses that would explicitly permit such a use of the personal information, which would in turn possibly have required businesses to disclose such uses by their service providers to consumers or even obtain opt-in consent (or opt out of sale). Given the many difficulties likely to be encountered in obtaining all such contractual agreements and consents, many service providers could see their business models hamstrung and their product-improvement objectives severely undermined.

Third, the draft regulations flesh out the CPRA's requirements that seek to restrict the service provider's control of the personal information it receives from a business such that the service provider grants the same level of privacy protection as the business that is directly regulated by California privacy laws. For instance, the CPRA requires that a service provider be contractually limited to processing personal information for the business purposes for which it has received the personal information from the business. The draft regulations additionally require that the business purposes be listed with specificity beyond a mere reference to the purpose of the contract.

These requirements, particularly in combination with requirements for service provider agreements under other state privacy laws taking effect in 2023, are likely to require businesses and service providers to renegotiate their agreements. Businesses may also need to revise their workflows and methods of cooperation to account for implementing consumer requests.

(3) Rules Expanding Contractual Requirements with Third Parties

In addition to the service provider requirements, the draft regulations impose obligations on third parties that receive personal information from an entity other than the individual to whom the personal information belongs. The term "third party" is not explicitly defined in the draft regulations, but appears to refer to any person or entity that receives personal information from a business and is not considered service provider or contractor. The third party must honor requests to delete or opt out of the sharing of personal information as well as requests forwarded to the third party from the business from which the third party obtained the personal information.[16]

A business that *sells or shares personal information with a third party*[17] must also enter into an agreement with that third party that includes requirements substantially similar to those in service provider contracts.[18] Among other requirements, the agreements with third parties must: (i) require the third party to only use and retain the personal information for the narrow purposes for which the personal information is being sold or disclosed; (ii) require the third party to comply with the CPRA and the draft regulations, including by providing the same level of privacy protection; and (iii) allow the business to require the third party to verify its compliance with its obligations under the agreement as well as the CPRA and the draft regulations.[19] Finally, any third party that does not have such an agreement in place would not be permitted to retain or process the personal information it receives from a business in any way.

Similar to service providers and contractors, the draft regulations apply to third parties receiving personal information from any entity, whether the entity is itself a "business" subject to the CPRA and the draft regulations or not. Specifically, whether or not the contracting entity is a business, third parties cannot store or process personal information absent a compliant contract with the entity, and the third party must adhere to the terms of the contract under which it received personal information and otherwise comply with the CPRA and the draft regulations.

Finally, failure on the part of a business to conduct due diligence of any third parties with which it shares personal information may prohibit the business from using ignorance of any misuse of the personal information as a defense in the face of a breach or violation of the CPRA or the draft regulations. This encourages businesses to ensure their due diligence processes are sufficient, and third parties such as data brokers may face some additional inquiries and contractual requirements.

(4) Notifications by a Business regarding Third-Party Data Collection

The draft regulations add a new concept requiring the notification of third-party involvement in the collection of personal information.[20] Specifically, if one business interacts with a consumer but another party is involved and "controls" the collection of personal information (e.g., a cookies analytics provider), then the first business needs to inform the consumer of the third-party collection and the identity of the third party. The draft regulations indicate that this is also true for physical businesses that may allow a third party to collect personal information. The CPPA provided the following example: if a coffee shop allows a business providing Wi-Fi to collect personal information, then the coffee shop

needs to inform customers of that third-party data collection through a sign or other signals of that collection.[21]

(5) Sensitive Personal Information

The draft regulations operationalize the new right to limit the use of sensitive personal information under the CPRA. The draft regulations add Section 7027, which concerns consumer requests to limit the use and disclosure of sensitive personal information. The section primarily contemplates giving consumers the ability to limit use and disclosure "to that which is necessary to perform the services or provide the goods reasonably expected."[22] Businesses that process sensitive personal information for certain purposes must provide a notice of such processing. Businesses using or disclosing personal information of this kind would be required to provide two or more designated methods for submitting requests to limit, and at least one of the methods must reflect the manner in which the business primarily interacts with the consumer (such as restrict processing to only permissible purposes through a "Limit the Use of My Sensitive Personal Information" link).[23] However, businesses are permitted to use or disclose sensitive personal information without being required to offer consumers a right to limit when the information is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests those goods or services; to detect security incidents to resist malicious or illegal attacks on the business; ensure the physical safety of natural persons; for short-term, transient use; perform services on behalf of the business; or verify or maintain the quality or safety of the business—a list that was not yet specified until the draft regulations.[24]

(6) Consumer Requests to Correct Information

The draft regulations also operationalize the CPRA's new right to correct inaccurate personal information. The draft regulations add an entirely new section on consumer requests to correct information.[25] At first glance, this regime is quite burdensome: in evaluating whether personal information is accurate, businesses must first consider the totality of the circumstances, including the nature of the information, how it was obtained, and documentation relating to the accuracy of the information.[26] While businesses may comply with a consumer's request to correct by correcting the information and ensuring that the information it (and its service providers and contractors) holds remains correct, a business may also choose to delete the information if such deletion does not negatively impact the consumer or the consumer consents to the deletion. Then, if the business were to deny the request for correction, they would be required to inform consumers of the basis for that denial, further outlining a procedure for consumers to respond in writing.[27] This section also provides specific examples relating to data brokers: if a business receives a request to correct information that it received from a data broker, it must both correct the information and ensure that it is not overridden by inaccurate information later re-received from the data broker. Where a business is not the source of the inaccurate information, the business is required to disclose the name of the source (such as a data broker) supplying the inaccurate information to the consumer.[28]

(7) Opt-Out Preference Signals

The draft regulations add a definition of an "opt-out preference signal," which is a signal sent by a platform, technology, or mechanism on behalf of the consumer that communicates the consumer's choice to opt out of the sale and sharing of personal information and that complies with the requirements set forth in the draft regulations. Notably, the draft regulations *require* businesses to process all consumer opt-out preference signals that meet certain requirements.[29] The details for these opt-out mechanisms are outlined in the new Section 7025. This section dictates that when a business detects an opt-out signal, it must treat it as a bona fide opt-out request and cannot require additional information to be provided. If the signal conflicts with a privacy setting or participation in some program, like a business's financial incentive program that requires the consumer to consent to the sale or sharing of personal information, the business must provide notice to the consumer. Businesses are instructed to process these opt-out signals in a frictionless manner. Businesses are also required to display whether or not they have processed consumers' opt-out preference signals, with the draft regulations suggesting the use of a banner, toggle, or radio button indicating to consumers that they have opted out of the sale of their personal information.

Revisions to Section 7026, meanwhile, indicate that requests to opt out of sales and/or sharing need not be verifiable and must be communicated to third parties. Crucially, the draft regulations indicate that a self-serve cookie management control process alone would not be sufficient to effectuate requests to opt out of sales and/or sharing, because "cookies concern the collection of personal information and not the sale or sharing of personal information."[30]

For those less familiar with the development of the CCPA and CPRA, opt-out signals (sometimes described as do-not-track signals) have been a source of ongoing confusion for businesses. While the draft regulations provide additional clarification, technical questions remain as to how these signals may or may not be communicated to a business, and what choices business have to present opt outs, links, or otherwise to ensure they effectively respond to consumers' opt-out signals. Standardization of these signals may be necessary for businesses to meaningfully comply.

(8) Data Minimization and Retention

The draft regulations include a section on the new data minimization requirement, which requires businesses to collect, use, retain and/or share consumers' personal information in a way that is "reasonably necessary and proportionate" to the original purpose for collecting it. The draft regulations define this standard tautologically as "what an average consumer would expect." Any collection, use, retention, or sharing that does not meet this standard requires additional notice and the consumer's explicit consent.

Of particular note are the examples provided in this section. Impermissible collection, use, retention, and sharing examples include:

- Collecting geolocation information through an app that does not primarily perform a geolocating function—e.g., a flashlight app.

- Using personal information provided to a SaaS company to research and develop "unrelated or unexpected new products"—e.g., where the service provided is cloud storage and the new product is a facial recognition service.

- Using personal information provided as part of a transaction for the marketing of other business' products.

- Retaining customer files stored as a service after the customer deletes their account.

- Sharing geolocation information with data brokers without the consumer's explicit consent, where the original collection was permissible as part of the suite of services the company provides—e.g., an internet service provider collecting geolocation information.

This new section drastically changes permissible practices with respect to consumer data, particularly around research for marketing purposes, and provides a hook for the enforcement agency to find impermissible processing of information, a concept that was largely missing from the CCPA. We expect contentious debate around these new restrictions at the next stakeholder sessions.

Additionally, the draft regulations update the Privacy Policy and Notice sections to include a new requirement that businesses disclose how long they intend to retain personal information.[31] To comply, businesses will need to develop data retention policies and a data purge protocol, and revise their privacy policies to note the relevant retention periods.

(9) Privacy Policy

Section 7011 specifies the privacy policy requirements under the CCPA and CPRA. The draft regulations in this section struck about three pages of text. First, the regulations begin by largely reinstating disclosure requirements concerning the categories, purposes, and sources of personal information, as well as relevant third parties.[32]

Second, the amendments require that the privacy policy include a description of a consumer's rights under the CCPA, including the new rights:

- the right to correct inaccurate personal information;

- the right to opt out of the sale *or sharing* of personal information; and

- the right to limit the disclosure of sensitive personal information.[33]

Third, the regulation amendments require privacy policies to include an explanation of how consumers exercise these rights, and notably add a requirement on how an opt-out request will be processed for the consumer (i.e., whether the opt-out preference signal applies to the device, browser, consumer account, and/or offline sales, and in what circumstances).[34] Finally, the policy must also include the date it was last updated and, if applicable, a link to certain reporting requirements under Section 7102 for businesses that handle the personal information of more than 10,000,000 consumers in a calendar year.

(10) Significant Definitions

The draft regulations propose numerous changes to the definitions section that inform entirely new provisions introduced as part of the CPRA and work to modify existing provisions by altering or refining the meanings of existing terms.[35]

Notable newly added terms include:

- "Disproportionate effort," meaning instances where the effort on the part of the business to comply with a consumer's legitimate request would be significantly out of proportion with the benefit to the consumer; and

- "Unstructured" as it relates to the nature of the data in which personal information is contained, including text, audio, or video files that contain personal information as part of their content but do not have a defined internal structure (as opposed to a database storing that same information).

"Disproportionate effort" and "unstructured" begin to grapple with the daunting realities faced by businesses attempting to comply with consumers' requests. Under the proposed regulations, businesses would be able to tailor their compliance to take into account overly burdensome or unreasonable requests based on the nature of the data at issue (e.g., large video files that are both cumbersome to access and difficult to search) and the burden that complying with such a request would place on the business. These additions take a step toward balancing consumers' legitimate rights and interests with the practical realities faced by businesses.

A notable change to the pre-existing terms: the term "household" has been deleted, sunsetting a term that caused consternation for businesses seeking to comply with the regulations.

(11) Enforcement

The draft regulations include a new section on enforcement actions. Section 7300 provides guidance for filing a sworn complaint with the enforcement agency, including the requirements for identifying the alleged violation of the CCPA. Sections 7302 outlines how the Agency shall conduct "probable cause hearings" which require notice to the alleged violator before conducting an "informal[]" hearing at which it makes a "probable cause determination," later issued in writing. Notably, notices of probable cause and probable cause determinations are not public, nor admissible in evidence in any action other than one enforcing the CCPA. Section 7304, meanwhile, empowers the Agency to audit businesses to ensure compliance with the CCPA.

What Is Not Addressed by the First Draft

The CPPA has had little time to untangle a Gordian knot of competing consumer privacy interests, business compliance issues, and a hodgepodge of public demands. The delay started early in the process and staffing and key developments came late (for example, the CPPA's Executive Director was only selected in October 2021). So it is not surprising that these regulations left many issues unaddressed,

particularly those concerning measures added by the CPRA, including restrictions for automated decision-making, cybersecurity audits and data protection risk assessments.

One of the most conspicuous omissions concerns the lack of parameters for automated decision-making. The CPRA defines "profiling" as "any form of automated processing of personal information, *as further defined by regulations* pursuant to paragraph (16) of subdivision (a) of Section 1798.185, 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," leaving the contours relatively amorphous in scope.[36] Contrary to the scope defined by other comprehensive state privacy laws (let alone the EU's GDPR), commenters have pointed out that the CPRA's language casts an incredibly wide net that could be argued to cover everything from pernicious forms of facial recognition in public places to humdrum automated processes like calculators and spellcheckers that may process personal information. As expressed in many CPPA public record comments, numerous stakeholders hoped the initial set of regulations would at least clarify this definition, for example, by limiting it to automated technologies that could create a material impact on a person, similar to the EU's GDPR.[37] That task was punted in the current draft regulations, with an unknown timeline, leaving many in limbo.

Another significant omission concerns the CPRA's requirement for businesses to conduct annual cybersecurity audits and risk assessments for businesses "whose processing of consumers' personal information presents significant risk to consumers' privacy or security."[38] This risk assessment was not contemplated by the CCPA. The CPRA noted two key factors " to be considered in determining when processing may result in significant risk to the security of personal information[,]" "the size and complexity of the business and the nature and scope of processing activities."[39] The CPRA required this risk assessment to be submitted to the CPPA on a regular basis. This task will require an assessment of "whether the processing involves sensitive personal information, and identifying and weighing the benefits resulting from the processing to the business, the consumer, other stakeholders, and the public, against the potential risks to the rights of the consumer associated with that processing, with the goal of restricting or prohibiting the processing if the risks to privacy of the consumer outweigh the benefits resulting from processing to the consumer, the business, other stakeholders, and the public."[40] Businesses will need to make careful decisions about how to describe their business processes.

In addition, the proposed draft regulations do not extend the current partial exemptions for employees, job applicants, and independent contractors. Since the draft regulations do not address limitations on the rights of these data subjects, businesses may need to be prepared to fully comply with all CCPA and CPRA obligations for employees, job applicants, and independent contractors by January 1, 2023, unless the law is amended.

***

These draft regulations are a key milestone for the CPPA's rulemaking responsibilities and fill in key gaps to help businesses comply with the law. We will continue to monitor regulatory developments, and are available to discuss these issues as applied to your particular business.

---

[1] The regulations only explicitly reference the CCPA, but should be understood to concern the CPRA as well.

[2] Last year, the FTC hosted a workshop to explore pernicious dark pattern trends and issued a thorough report to explain the phenomenon. *Bringing Dark Patterns to Light: An FTC Workshop*, Federal Trade Commission (April 29, 2021), *available at* https://www.ftc.gov/news-events/events-calendar/bringing-dark-patterns-light-ftc-workshop. Invigorated by the workshop, the FTC issued a policy statement and announced that it would prioritize enforcement against dark patterns—specifically those relating to recurring subscription fees. *FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions* (Oct. 28, 2021), *available a*t https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-illegal-dark-patterns-trick-or-trap-consumers-subscriptions.

[3] Cal. Civ. Code § 1798.140(l).

[4] *Id*. § 1798.140(h).

[5] Draft Regulations § 7004(b).

[6] *Id*. § 7004(a).

[7] This expansion of the CPRA's concept of dark patterns operates under the California Civil Code, subsections 1798.185(a)(4)-(7), which give the CPPA authority to establish rules and procedures to facilitate and govern the submission of consumer requests under the CCPA.

[8] Draft Regulations § 7004(b)-(c).

[9] *Id*. § 7004.

[10] *Id.* § 7004(a).

[11] *Id.* § 7004(a)(4)(A).

[12] *Id.* § 7004(a)(2)(C).

[13] *Id.* § 7050(a).

[14] *Id.* § 7050(c).

[15] *Id.* § 7050(b)(4).

[16] *Id.* § 7052.

[17] Whereas the focus of "selling" under the CCPA was on whether there was monetary or other valuable consideration for the disclosure of personal information, the concept of "sharing" under the CPRA focuses on whether personal information is used by third parties for cross-context behavioral advertising (whether or not for monetary or other valuable consideration). Under the draft regulations, businesses may be required to offer the opportunity to opt out of any sharing (through a "Do Not Sell *or Share* My Personal Information" link) and provide notice of the right in their privacy notices.

[18] *See* Draft Regulations § 7053.

[19] *Id.* § 7053(a).

[20] *Id.* § 7012(g).

[21] *Id.* § 7012(g)(4)(B).

[22] *Id.* § 7027(a).

[23] *Id.* § 7014.

[24] *Id.* § 7027(l)(1)-(7).

[25] *Id.* § 7023.

[26] *Id.* § 7023(b).

[27] *Id.* § 7023(f).

[28] *Id.* § 7023(i).

[29] *Id.* § 7025(b).

[30] *Id.* § 7026(4).

[31] *Id.* § 7012.

[32] *Id.* § 7011(e)(1).

[33] *Id.* § 7011(e)(2).

[34] *Id.* § 7011(e)(3).

[35] *Id.* § 7001.

[36] Cal. Civ. Code § 1798.140(z) (emphasis added).

[37] The GDPR uses an impact to risk-based approach—only governing processing "which produces legal effects concerning him or her or similarly *significantly* affects him or her." GDPR at Art. 22(1) (emphasis added). For example, this may include loan or employment applications.

[38] Cal. Civ. Code § 1798.185(a)(15).

[39] *Id*.

[40] *Id*.

The following Gibson Dunn lawyers prepared this client alert: Alexander Southwell, Ryan Bergsieker, Cassandra Gaedt-Sheckter, Abbey Barrera, Snezhana Stadnik Tapia, Tony Bedel, Warren Loegering, Raquel Sghiatti, Courtney Wang, Samantha Abrams-Widdicombe, and Leon Freyermuth.

Gibson Dunn lawyers are available to assist in addressing any questions you may have about these developments. Please contact the Gibson Dunn lawyer with whom you usually work, the authors, or any member of the firm's Privacy, Cybersecurity & Data Innovation practice group:

United States

Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
S. Ashlie Beringer – Co-Chair, PCDI Practice, Palo Alto (+1 650-849-5327, aberinger@gibsondunn.com)
David P. Burns – Washington, D.C. (+1 202-887-3786, dburns@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)
Svetlana S. Gans – Washington, D.C. (+1 202-955-8657, sgans@gibsondunn.com)
Nicola T. Hanna – Los Angeles (+1 213-229-7269, nhanna@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Robert K. Hur – Washington, D.C. (+1 202-887-3674, rhur@gibsondunn.com)
Kristin A. Linsley – San Francisco (+1 415-393-8395, klinsley@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Karl G. Nelson – Dallas (+1 214-698-3203, knelson@gibsondunn.com)
Ashley Rogers – Dallas (+1 214-698-3316, arogers@gibsondunn.com)
Alexander H. Southwell – Co-Chair, PCDI Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Deborah L. Stein – Los Angeles (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Michael Li-Ming Wong – San Francisco/Palo Alto (+1 415-393-8333/+1 650-849-5393, mwong@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)

GIBSON DUNN

Europe

Ahmed Baladi – Co-Chair, PCDI Practice, Paris (+33 (0) 1 56 43 13 00, abaladi@gibsondunn.com)
James A. Cox – London (+44 (0) 20 7071 4250, jacox@gibsondunn.com)
Patrick Doris – London (+44 (0) 20 7071 4276, pdoris@gibsondunn.com)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@gibsondunn.com)
Bernard Grinspan – Paris (+33 (0) 1 56 43 13 00, bgrinspan@gibsondunn.com)
Penny Madden – London (+44 (0) 20 7071 4226, pmadden@gibsondunn.com)
Michael Walther – Munich (+49 89 189 33-180, mwalther@gibsondunn.com)
Alejandro Guerrero – Brussels (+32 2 554 7218, aguerrero@gibsondunn.com)
Vera Lukic – Paris (+33 (0) 1 56 43 13 00, vlukic@gibsondunn.com)
Sarah Wazen – London (+44 (0) 20 7071 4203, swazen@gibsondunn.com)

Asia

Kelly Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)
Connell O'Neill – Hong Kong (+852 2214 3812, coneill@gibsondunn.com)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)