GIBSON DUNN

September 29, 2020

THE POTENTIAL IMPACT OF THE UPCOMING VOTER INITIATIVE, THE CALIFORNIA PRIVACY RIGHTS ACT

To Our Clients and Friends:

On November 3, 2020, only four months after the California Consumer Privacy Act ("CCPA") became enforceable by the California Attorney General, Californians will vote on Alastair Mactaggart's newest consumer privacy ballot initiative, the California Privacy Rights Act ("CPRA"), styled as California Proposition 24. We previously issued a brief client alert on the CPRA when it secured sufficient signatures to get on the November ballot (available here), and promised to provide additional information on the ballot measure as the vote drew closer. Below, we delve into the pertinent details of the CPRA and analyze how it may change data privacy and cybersecurity regulation in California, and potentially elsewhere, should the initiative pass.

I. Background and Context

The CPRA ballot initiative, sometimes colloquially referred to as "CCPA 2.0," represents an effort to address the perceived inadequacies of the CCPA, which, according to Mactaggart and others, was hastily enacted by the California state legislature to avoid a more restrictive ballot initiative. As we noted in our prior alert, unlike the legislatively-enacted CCPA, should the CPRA be approved by California voters and become state law *as written*, it could not be readily amended by the state legislature. Instead, any significant changes to the law would similarly require further voter action. However, by its terms, the CPRA would not go into effect until January 1, 2023, and thus the CCPA would remain in full force and effect for the interim.

In September 2019, even before the CCPA went into effect, Alastair Mactaggart and the Californians for Consumer Privacy (the non-profit group behind the original CCPA initiative in 2018), proposed the CPRA initiative in an attempt to provide California consumers with expanded privacy rights and to counterbalance efforts by large companies to "actively and explicitly prioritize[] [the] weakening [of] the CCPA,"[1] Californians for Consumer Privacy sponsored the consumer privacy bill, called the Consumer Right to Privacy Act, for the November 2018 ballot. After the initiative was proposed but before it was qualified to appear on the ballot, the California State Legislature agreed to pass what would become the CCPA in exchange for the removal of the ballot initiative by its backers. The CCPA passed in June of 2018, and was signed into law by California Governor Jerry Brown (please see our prior alerts regarding the CCPA here, here, here, here, and here).

In what might feel like a bit of *déjà vu*, on June 24, 2020, the Secretary of State of California announced that the Mactaggart-backed CPRA had enough valid signatures and was qualified to appear on the November 2020 ballot. However, we will not see a repeat of 2018's last-minute, backroom deal-making

to avoid the 2020 CPRA's enactment as a ballot initiative, because the California Elections Code only allows a proponent to remove a "proposed," initiative, and not one that has "qualified" for the ballot.[2]

Though we will have to wait until the ballots are counted in November to know the results, preliminary polling conducted by Goodwin Simon Strategic Research in October 2019 suggested that 88% of California voters would likely vote for the initiative,[3] and more recent polling conducted by the firm and released by the Yes on Prop. 24 in July 2020 similarly suggests that 81% of voters will likely vote for the initiative.[4] That same poll showed that even after being presented with opposition arguments against the measure, as set out in the official voter ballot guide, voters still overwhelmingly supported the initiative, with 72% in favor.[5]

II. Timing – When Would the CPRA Go Into Effect and When Will It Be Finalized?

If the CPRA were enacted, it would largely impose new obligations that would apply only to personal information collected after January 1, 2023; however, it would also provide consumers with a right to access personal information collected in the prior 12 months, which would mean such a right would extend to personal information collected on or after January 1, 2022. As a result, compliance with the CPRA will likely require steps to be taken over a year before the law would go into full effect. Similarly, with respect to implementing regulations—a topic that was quite an ordeal for the CCPA and which resulted in initial regulations being proposed just months before the CCPA took effect, with the final regulations being adopted nearly eight months *after*—the CPRA would grant the California Attorney General the power at the outset to adopt regulations to expand upon and update the CCPA until July 1, 2021, at which point a newly created California Protection Agency (described further below) would assume responsibility for administering the law. In addition, the final regulations arising from the CPRA would need to be adopted by July 1, 2022, a full year before the CPRA becomes enforceable on July 1, 2023.

III. CPRA's Key Rights and Provisions

a. Higher Threshold for Applicability – Who Must Comply with the CPRA?

The CPRA narrows the definition of covered entities, or "businesses" from that set out in the CCPA. Specifically, the CPRA alters the scope of covered entities by clarifying how to measure the gross revenue threshold, increasing the threshold number of consumers or households (eliminating the consideration of devices from this number)[6] from 50,000 to 100,000 (exempting smaller businesses), and extending the source for the threshold percentage of annual revenue to also include revenue derived from *sharing* personal information.

In light of these changes, the CPRA would apply to any "business," including any for-profit entity that collects consumers' personal information, which does business in California, and which satisfies one or more of the following thresholds:

- had annual gross revenues in excess of twenty-five million dollars ($25,000,000) *for the preceding calendar year, as of January 1 of the calendar year*;

- possesses the personal information of *100,000* or more consumers or households; or
- earns more than half of its annual revenue from selling *or sharing* consumers' personal information.[7]

Because many medium-to-large businesses satisfy the threshold requirement just with the revenue threshold, the changes to the scope of covered entities will not practically affect many of our clients.

However, for commonly-controlled business, or businesses that share common branding, the CPRA also narrows the definition of covered entities to require that such businesses also share consumers' personal information. This can be significant for companies with multiple related and commonly-controlled entities that may share common branding, but which operate entirely separately for data privacy purposes, with no comingling of consumer's personal data.

b. New Enforcement Agency: California Privacy Protection Agency

The most significant addition of the CPRA is the proposed creation of a new state agency, the California Privacy Protection Agency, a body vested with full administrative power, authority, and jurisdiction to implement and enforce the CPRA.[8] The California Privacy Protection Agency would be the first enforcement agency in the United States dedicated solely to privacy. It would be provided with funding of $5M during the 2020-2021 fiscal year, and $10M during each fiscal year thereafter, to undertake privacy-related investigations.

The California Privacy Protection Agency would be led by a five-member board. The Governor is to appoint the Chair and one member of the board, whereas the Attorney General, Senate Rules Committee, and Speaker of the Assembly would each appoint one other member.

The California Privacy Protection Agency is to assume enforcement responsibilities for the CCPA from the Attorney General within six months of the agency providing the Attorney General with notice that it is prepared to assume rulemaking responsibilities or, by no later than July 1, 2021.[9] It is unclear how the agency would enforce privacy laws during this period prior to full enforcement of the CPRA, but we expect that the agency may seek to model itself in light of similar regulatory and enforcement agencies abroad like, for example, the data protection authorities or supervisory authorities under the EU's General Data Protection Regulation ("GDPR").

c. New Category of "Sensitive Personal Information" and Right to Restrict Use of Sensitive Personal Information

The CPRA would establish a ***new category of "sensitive personal information,"*** which would be defined to include Social Security Numbers, driver's license numbers, passport numbers, financial account information, precise geolocation, race, ethnicity, religion, union membership, personal communications, genetic data, biometric or health information, and information about sex life or sexual orientation.[10] This definition more closely tracks the definition and distinction of "special categories" of personal data under Art. 9 of the GDPR. Similar to how "personal information" is defined under the

CCPA, "sensitive personal information" would not include publicly available information (as defined narrowly to be public information available from government sources).

In establishing a new category of data, the CPRA would provide consumers with the right, at any time, to direct a business that collects sensitive personal information about the consumer to "limit its use of the consumer's sensitive personal information to that use which is necessary to perform the services or provide the goods reasonably expected by an average consumer who requests such goods or services…"[11] In order to exercise this right, the CPRA includes requirements for a business to provide a "clear and conspicuous link" to consumers on its homepage titled, "Limit the Use of My Sensitive Personal Information" or a "clearly-labeled link on the business's internet homepage(s)" that allows a consumer to opt-out of the sharing of personal information and limit the use/disclosure of sensitive personal information.[12] This would be in addition to the already existing link requirement under the CCPA allowing consumers to opt out of the sale of their personal information. However, businesses can use a single link if it "easily allow[s] a consumer to [both] opt-out of the sale or sharing of the consumer's personal information and to limit the use or disclosure of the consumer's sensitive personal information."[13]

d. New Rights to Correct Personal Information and to Data Minimization, and Storage Limitation Requirements

Like the GDPR, the CPRA would also grant consumers the ***right to correct inaccurate personal information***.[14] Under the CPRA, businesses that collect personal information about consumers must disclose this right to correct to consumers and must use "commercially reasonable efforts" to correct their personal information upon receipt of a verifiable consumer request.[15]

The CPRA further resembles the GDPR by introducing the right to ***data minimization***. Specifically, the CPRA would require 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…"[16] Furthermore, the CPRA provides clarification regarding the CCPA's current prohibition against collecting or using additional categories of personal information for additional purposes without providing the consumer with notice[17]: Per proposed § 1798.100(a)(1), businesses would be further prohibited from collecting or using additional categories of personal information that are "incompatible with the disclosed purpose for which the personal information was collected" without providing the consumer with notice.[18] While these data minimization steps are generally considered best practices in the United States, and are the subject of guidance from the Federal Trade Commission, the CPRA would seek to codify these requirements in California.

Also, whereas the CCPA was relatively silent on retention, the CPRA would impose ***storage limitation requirements***, whereby businesses are prohibited from storing personal information, including sensitive personal information, for longer than is necessary or beyond a disclosed time period. The CPRA would also take it a step further and grant consumers the right to know at or before the point of collection the length of time a business intends to retain each category of personal information.[19]

e. Expanded Right to Opt-Out of "Sale" of Personal Information Explicitly Includes Sharing of Personal Information and Cross-Context Behavioral Advertising

Significantly, in an apparent attempt to clarify the meaning of "sale" of personal information—and in particular, its application to behavioral advertising—the CPRA expands the CCPA's right to opt-out of "sale" of personal information to include "sharing" of personal information.[20] The "sharing" of personal information is specifically defined as the transfer of or making available of "a consumer's personal information by the business to a third party for cross-context behavioral advertising."[21]

Though the CCPA's existing definition of "sale" is widely debated, and some argue already includes various aspects of the AdTech industry, this clarification seeks to settle the debate in the affirmative as to whether businesses need to provide consumers with a right to opt out of third-party sharing for advertising purposes, including through cookie-based collection on their websites and apps.

f. New Automated Decision-Making Right and Restrictions on Profiling

The CPRA would require first the Attorney General, and then the California Privacy Protection Agency, to adopt regulations "governing access and opt-out rights with respect to a business's use of automated decision-making technology, including profiling…"[22] "Profiling" under the CPRA is defined 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."[23] As a result, a business's response to an access request would be required 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."[24]

Businesses already complying with the GDPR, which grants EU citizens the right not to be subject to a decision based solely on automated processing, including profiling, and to request an explanation of how and why an automated decision was reached, may be familiar with this new requirement.[25] However, the right under the CPRA may in fact be broader than its equivalent under the GDPR because the CPRA would grant consumers the right to opt-out of "any form" of automated-decision making, whereas the GDPR restricts the right to not be subject to decisions based solely on automated-processing. Furthermore, this requirement would be the first of its kind in the United States that would require such transparency and limitations on automated decision-making generally.

g. Cybersecurity Audit Requirements for High-Risk Data Processors

The CPRA also introduces audit requirements for high-risk data processors. Once again, first the Attorney General, and then the California Privacy Protection Agency, would be required to issue "regulations requiring businesses whose processing of consumers' personal information presents significant risk to consumers' privacy or security" to perform an annual cybersecurity audit.[26]

Businesses in this category would also be required to perform an annual cybersecurity audit and regularly submit risk assessments with respect to their processing of personal information to the California Privacy Protection Agency, "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 such processing."[27]

h. Loyalty and Rewards Programs Are Not Prohibited

In one clarification of an issue that caused some consternation with regard to the CCPA, the CPRA explicitly allows businesses to offer "loyalty, rewards, premium features, discounts, or club card programs" in exchange for consumer's opt-in consent.[28] Though the final CCPA regulations adopted by the Attorney General and approved on August 24, 2020, provided some needed clarity on this point, the CCPA remains ambiguous as to how to balance the requirement not to discriminate against consumers for exercising their rights, on the one hand, with the offering of programs that require using the very personal information for which the consumer can request deletion, on the other. The CPRA would resolve this ambiguity by expressly allowing such loyalty programs to be conditioned on opt-in consent.

i. New Categories and Obligations for Service Providers, Contractors, and Third Parties

The CPRA would also amend the CCPA's definitions of "service provider" and "third party," and create a new category of "contractor," to impose new obligations for service providers and contractors.[29] The CPRA clarifies that a third party is anyone other than the business, a service provider, or contractor. The newly-defined "contractor" means "a person to whom the business makes available a consumer's personal information for a business purpose pursuant to a written contract…"[30] Among other things, this written contract must prohibit the contractor from selling or sharing the personal information it receives; using or disclosing the personal information for any purpose other than for the contract's business purpose; and combining the personal information with data received or collected through other means, with limited exceptions.[31]

These requirements are indirectly imposed by the definition of "service provider" under the CCPA – in order to considered a "service provider," an entity must "process information on behalf of a business" for a business purpose, pursuant to a written contract that prohibits the entity from "retaining, using, or disclosing the personal information for any purpose other than for the specific purpose of performing the services specified in the contract."[32] However, the definition of "contractor" under the CPRA explicitly limits the service provider's ability to *share* information, or to combine it with information obtained through other means, which is likely designed to exclude behavioral advertisers that create profiles using data from multiple clients from the definition of contractor. Further, the CPRA additionally imposes affirmative obligations on service providers and contractors to cooperate and assist businesses in responding to a consumer's request to delete and correct personal information, and limit the use of sensitive personal information.[33] However, service providers and contractors are not required to comply with consumer requests "received directly from a consumer or a consumer's authorized agent…to the extent that the service provider or contractor has collected personal information about the consumer in its role as a service provider or contractor."[34]

j. Explicit Requirement to Implement Reasonable Security Procedures and Practices for Businesses, Service Providers, and Contractors

Though the CCPA indirectly required businesses to maintain reasonable security procedures and practices by tying the private right of action to a *business*'s failure to implement such measures, the CPRA would create an affirmative requirement for businesses to implement "reasonable security procedures and practices" for all categories of personal information,[35] *and* extends this duty to third parties, service providers, and contractors to provide the "same level of privacy protection" as is required of the business.[36]

IV. Changes to Potential Liability

Under the CPRA, if the California Privacy Protection Agency determines that a violation or violations have occurred, the agency can seek an administrative fine of up to $2,500 for each violation, or up to $7,500 for each intentional violation or each violation involving the personal information of minor consumers, which is similar to the CCPA's current level of potential exposure; the difference being that the CPRA instead provides an administrative fine through the Agency.[37]

To the surprise of many, the CPRA does not include a significantly broader private right of action, but similarly limits the private right of action to breaches of non-encrypted, non-redacted personal information as under the CCPA. Nonetheless, the CPRA expands upon the CCPA to include a private right of action for unauthorized access or disclosure of both an "email address in combination with a password or security question and answer that would permit access to the account…" and personal information, as defined under California's data breach notification law, as opposed to just the latter as under the CCPA.[38]

V. Expanded Moratoria for Employee and B2B Personal Information

The CCPA currently exempts personal information obtained from employees and job applicants in the context of employment as well as certain personal information obtained in certain business-to-business ("B2B") transactions until January 1, 2021 (please see our prior alert here). On August 30, 2020, the California legislature voted to pass Assembly Bill 1281 ("AB 1281"), which extends the CCPA's current employee and B2B exemptions from January 1, 2021 to January 1, 2022—Governor Gavin Newsome has until September 30, 2020 to sign the bill.

If enacted, the CPRA would extend these moratoria even further, until January 1, 2023.[39] However, while the California legislature can extend the exemptions under the CCPA, they will be unable to do so under the CPRA, unless another ballot initiative is approved by California voters.

VI. Certain Consumer Privacy Advocates Are *Against* the CPRA

Perhaps surprisingly, though the CPRA was proposed by consumer advocates Californians for Consumer Privacy as a pro-consumer response to the perceived weakening of the rights granted to consumers under the CCPA, a number of civil rights advocacy groups, including the American Civil Liberties Union

("ACLU") of California, California Alliance for Retired Americans, and Color of Change, have all publicly called on Californians to vote "No" on the ballot initiative in November.

These groups have stated that the ballot initiative is "full of giveaways to social media and tech giants" by giving companies new ways to collect personal information, letting companies profit further from consumers' personal information, and restricting enforcement of privacy rights in court.[40] Specifically, these advocacy groups argue that this ballot initiative is asking Californians to "approve 'pay for privacy," by letting companies charge more for safeguarding consumer personal information, which has "racially discriminatory impacts, disproportionately pricing out working people, seniors, and Black and Latino families." Furthermore, these groups argue that the CPRA would restrict the ability of Californians to enforce their privacy rights in court because it asks them to unpersuasively trust a newly created agency, created during a budget crunch, to enforce consumer rights under the CPRA. Lastly, these groups state: "[The CPRA] was written behind closed doors with input from the same tech companies with histories of profiting off of [] personal information in unfair and discriminatory ways. It puts more power in the hands of tech companies like Facebook that already have too much power. It protects big tech business, not people."[41]

That said, it does not appear that the No on Proposition 24 position has been significantly funded, and the Yes on Proposition 24 position appears to have been funded primarily by Mr. Mactaggart himself.

* * *

As we continue to counsel our clients through CCPA compliance, we understand what a major undertaking it is and has been for many companies. As other states and the federal government continue to grapple with implementing any privacy laws, California is already considering its *second* precedent-setting comprehensive privacy law, causing additional consternation. Given that the CPRA would introduce a host of new consumer rights and related business requirements if enacted, we anticipate that compliance with the CPRA would similarly require a complex and nuanced compliance program for companies.

Specifically, the CPRA would expand upon the CCPA to grant the right to limit the sharing and use of consumers' sensitive personal information, the right to correct personal information, the right to data minimization, and the expanded right to opt-out of the sale of personal information, as well as impose requirements and restrictions on businesses, including new storage limitation requirements, new restrictions on automated decision-making, and new audit requirements. Additionally, the CPRA also establishes an entirely new enforcement agency—the California Privacy Protection Agency—removing enforcement authority for both the CCPA and the CPRA from the Attorney General, and expands breach liability. As such, it will remain to be seen how this new agency would approach enforcement.

In light of this potential sweeping new law, we will continue to monitor developments, and are available to discuss these issues as applied to your particular business.

[1] "A Letter from Alastair Mactaggart, Board Chair and Founder of Californians for Consumer Privacy," Californians For Consumer Privacy (Sept. 25, 2019), available at https://www.caprivacy.org/a-letter-from-alastair-mactaggart-board-chair-and-founder-of-californians-for-consumer-privacy/.

[2] "Initiative and Referendum Qualification Status," California Secretary of State, available at https://www.sos.ca.gov/elections/ballot-measures/initiative-and-referendum-status .

[3] Amy Simon and John Whaley, "Summary of Key Findings from California Privacy Survey," Goodwin Simon Strategic Research (Oct. 16, 2019), available here.

[4] "New Poll From Goodwin/Simon Research Shows Prop 24, The California Privacy Rights Act, Receives 81% Support From Voters," Californians For Consumer Privacy (Aug. 3, 2020), available at https://www.caprivacy.org/new-poll-from-goodwin-simon-research-shows-prop-24-the-california-privacy-rights-act-receives-81-support-from-voters/.

[5] *Id.*

[6] Whereas the CCPA defines "business" in part as a for-profit entity that collects consumers' personal information, which does business in California and possesses "the personal information of 50,000 or more consumers, households, *or devices*," Cal. Civ. Code § 1798.140(c)(1)(B)(*emphasis added*), the CPRA removes devices from consideration. *See* Cal. Civ. Code § 1798.140(d)(1).

[7] Cal. Civ. Code § 1798.140(d)(1).

[8] CPRA Section 24, adding Cal. Civ. Code § 1798.199.10.

[9] CPRA Section 24, adding Cal. Civ. Code § 1798.199.40(b).

[10] CPRA Section 14, adding Cal. Civ. Code § 1798.140(ae).

[11] CPRA Section 10, adding Cal. Civ. Code § 1798.121.

[12] CPRA Section 13, adding Cal. Civ. Code § 1798.135(a)(2).

[13] CPRA Section 13, adding Cal. Civ. Code § 1798.135(a)(3).

[14] CPRA Section 6, adding Cal. Civ. Code § 1798.106(a).

[15] Id.

[16] CPRA Section 4, adding Cal. Civ. Code § 1798.100(a)(3)(c).

[17] Cal. Civ. Code § 1798.100(b).

[18] Cal. Civ. Code § 1798.100(a)(1).

[19] CPRA Section 4, adding Cal. Civ. Code § 1798.100(a)(3).

[20] CPRA Section 9, amending Cal. Civ. Code § 1798.120.

[21] CPRA Section 14, amending Cal. Civ. Code § 1798.140(ah).

[22] CPRA Section 21, adding Cal. Civ. Code § 1798.185(a)(16).

[23] CPRA Section 14, adding Cal. Civ. Code § 1798.140(z).

[24] Id.

[25] GDPR, Article 22.

[26] CPRA Section 21, adding Cal. Civ. Code §1798.185(a)(15).

[27] CPRA Section 21, adding Cal. Civ. Code §1798.185(a)(15)(A)-(B).

[28] Section 11 of the CPRA, amending Cal. Civ. Code § 1798.125.

[29] CPRA Section 14.

[30] CPRA Section 14, adding Cal. Civ. Code § 1798.140(j)(1).

[31] Id.

[32] Cal. Civ. Code § 1798.140(v).

[33] CPRA Section 3, adding Cal. Civ. Code § 1798.100(d).

[34] CPRA Section 12, adding Cal. Civ. Code § 1798.130(2)(B)(3).

[35] CPRA Section 4.

[36] CPRA Section 4, adding Cal. Civ. Code § 1798.100(d).

[37] CPRA Section 4, adding Cal. Civ. Code § 1798.100(e).

[38] CPRA Section 16, amending Cal. Civ. Code § 1798.150(a).

[39] Section 15 of the CPRA, amending Cal. Civ. Code § 1798.145.

[40] "No on Proposition 24 Rebuttal Argument," available at https://consumercal.org/wp-content/uploads/2020/07/No-on-Proposition-24-Rebuttal-Argument.pdf.

[41] Id.

The following Gibson Dunn lawyers assisted in the preparation of this client update: Alexander H. Southwell, Benjamin Wagner, H. Mark Lyon, Cassandra Gaedt-Sheckter, and Lisa V. Zivkovic.

Gibson Dunn's lawyers are available to assist in addressing any questions you may have regarding these developments. Please contact the Gibson Dunn lawyer with whom you usually work, or any member of the firm's California Consumer Privacy Act Task Force or its Privacy, Cybersecurity and Consumer Protection practice group:

California Consumer Privacy Act Task Force:
Benjamin B. Wagner – Palo Alto (+1 650-849-5395, bwagner@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Cassandra L. Gaedt-Sheckter – Palo Alto (+1 650-849-5203, cgaedt-sheckter@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@gibsondunn.com)
H. Mark Lyon – Palo Alto (+1 650-849-5307, mlyon@gibsondunn.com)
Alexander H. Southwell – New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Deborah L. Stein (+1 213-229-7164, dstein@gibsondunn.com)
Eric D. Vandevelde – Los Angeles (+1 213-229-7186, evandevelde@gibsondunn.com)

Please also feel free to contact any member of the Privacy, Cybersecurity and Consumer Protection practice group:

United States
Alexander H. Southwell – Co-Chair, PCCP Practice, New York (+1 212-351-3981, asouthwell@gibsondunn.com)
Debra Wong Yang – Los Angeles (+1 213-229-7472, dwongyang@gibsondunn.com)
Matthew Benjamin – New York (+1 212-351-4079, mbenjamin@gibsondunn.com)
Ryan T. Bergsieker – Denver (+1 303-298-5774, rbergsieker@gibsondunn.com)
Howard S. Hogan – Washington, D.C. (+1 202-887-3640, hhogan@gibsondunn.com)
Joshua A. Jessen – Orange County/Palo Alto (+1 949-451-4114/+1 650-849-5375, jjessen@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)
Deborah L. Stein (+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)

Europe
Ahmed Baladi – Co-Chair, PCCP 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)
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)
Kai Gesing – Munich (+49 89 189 33-180, kgesing@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)
Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)