Skadden

Privacy & Cybersecurity Update

Final Proposed California Consumer Privacy Act Regulations Submitted for Administrative Review

On June 1, 2020, California's attorney general submitted the final version of the California Consumer Privacy Act (CCPA) implementing regulations. The California Office of Administrative Law (OAL) has 30 working days, plus an additional 60 calendar days (due to a COVID-19-related executive order) to confirm that the regulations comply with state regulatory adoption requirements. Following such approval, the attorney general's regulations will be enforceable by law.

California Attorney General Xavier Becerra submitted the final version of the CCPA implementing regulations to the OAL to ensure proper procedural adherence to regulatory adoption requirements. The submission follows several months of public input (including hearings and comment periods) and three rounds of publicly released drafts. A Final Statement of Reasons (FSOR) also accompanied the June 1 regulations release, providing valuable insight into the reasoning behind the attorney general's changes over time.

While regulatory adoption is frequently seen as a routine process in many contexts, in this instance the CCPA itself instructed the attorney general to solicit broad public input and develop new rules in a number of core areas to define Californians' CCPA rights, such as the requirements of a verifiable consumer request or a consumer opt-out. The statute also permitted the attorney general to adopt regulations going beyond the scope of the law's own requirements in order to further the purposes of the CCPA. As a result, businesses must carefully evaluate both the statute itself and the regulations in order to identify the full array of applicable CCPA obligations.

Overall Process Observations

Prior to the release of these finalized regulations, the attorney general had released an initial draft on October 11, 2019, a first set of modifications on February 10, 2020, and a second set of modifications on March 11, 2020. While each set of modifications featured various language edits, the attorney general appeared to pursue three underlying goals in each iteration: increased disclosure specificity to consumers, increased accessibility of consumer disclosures, and improved commercial feasibility to reduce the burden of new practices and procedures on businesses. Changes in each area helped to move the regulations toward a right-sized compliance framework that reflects the

commercial realities of the modern business while maximizing consumer utility. Details of the revisions include:

- **Disclosure Specificity:** The revisions added additional clarifications regarding how consumer disclosures must be presented in order to make such information useful. For example, any disclosure of the business or commercial purposes for collecting and selling personal information must be "meaningfully understandable" to the consumer. The FSOR explains that this standard was included to create a "performance-based approach" for evaluating consumer disclosures rather than implement an exhaustive and inflexible list of disclosure requirements.
- **Consumer Accessibility:** The later versions of the regulations also specified that consumers must be able to easily assert their rights through any type of device or user interface and, in certain instances, be presented with specific notice disclosures that are contextually relevant rather than a long, generally applicable policy. The FSOR indicates that these additions were meant to provide businesses with the flexibility to implement disclosures and other consumer rights within their existing business practices, but prevent a business from choosing obscure request submission methods that could potentially thwart consumer rights.
- **Commercial Feasibility:** As the regulations were further refined, the FSOR suggests that the attorney general thoughtfully considered the input of the business community and modified several initial requirements to avoid imposing commercially burdensome obligations that do not reflect how a typical business operates, such as in the areas of service provider restrictions and consumer request submissions.

Key Clarifications to the CCPA's Base Requirements

In the CCPA statute, the California Legislature directed the attorney general to adopt regulatory requirements in several key areas that state legislators chose not to address in the law. While one reason for this was likely the relatively rushed timeline on which the CCPA was adopted, these areas also required some of the most nuanced considerations and largest amount of business community input of any CCPA requirements in order to ensure the rules were commercially practicable and resulted in benefits to consumers. Three particular areas where the attorney general provided important input on statutory-derived requirements were in the areas of defining the requirements of a verifiable consumer request, establishing opt-out rules and procedures relating to the sale of data, and creating rules surrounding the exercise of consumer rights for household-related personal information.

- **Verifiable Consumer Request:** Determining how to verify a consumer request to learn about their personal information or how to have that information deleted were among the most important and least defined aspects of the CCPA. The regulations explain that in order for businesses to properly implement verification requirements, they must take into account the nature of the request and relation of the consumer to the requestor (if not the same individual), establish varying verification measures based on the nature of the request, and utilize data and personal information already possessed by the business — whenever possible — to limit the privacy impact to consumers exercising such rights.
- **Opt-Out Rules and Procedures:** The regulations added important clarifications to enable businesses to implement consumer opt-outs in their products and services, but also imposed new obligations that go beyond the CCPA's statutory requirements. The FSOR suggests that the attorney general expects the right to opt out to be among the most frequently asserted consumer rights, since it allows individuals to easily exert control over their information while still maintaining a relationship with the business. However, in addition to providing some compliance clarity, the regulations also injected new obligations and confusion for businesses by creating the possibility of "user-enabled global privacy controls" that a consumer could exercise through a browser plugin, privacy setting, device setting or other mechanism. The regulations do not limit the forms such user indications may take or identify a particular standard for browser providers, hardware manufacturers, or other hardware and software intermediaries to implement and transmit an opt-out signal. While the CCPA statute also directed the attorney general to develop and promote the use of a recognizable and uniform opt-out button, the FSOR notes that the proposed button was removed in the second set of modifications due to public comments. The attorney general will continue to study and evaluate the use of a uniform logo or button to support consumer opt-out.
- **Household-Related Personal Information:** The amended CCPA specifically provided the attorney general with the option to adopt additional regulations in the area of household-related request verifications. The regulations provide important clarifications to explain how a business must verify a household-related request and confirms that, much like processing a standard consumer request, businesses that have established an online account with the household from which they collect personal information will likely find it substantially easier to implement request and verification procedures.

Notable Additions Going Beyond the Original Statutory Requirements

In addition to developing the regulations required by the California Legislature, the attorney general also adopted new regulations that go beyond the requirements of the CCPA itself. Notable deviations include, in certain instances, requiring consumer

disclosures even if the requestor cannot be verified, creating new service provider personal information usage exceptions, requiring the calculation and publishing of request compliance statistics for some businesses, and requiring businesses to confirm the receipt of a consumer's request to know or delete.

- **Disclosures Where Request Not Verified:** The regulations provide that even where a non-accountholder request cannot be verified for purposes of a consumer's specific request, the business should still evaluate the request to see if it should be complied with in a lesser manner.
  - For example, if three items of personal information cannot be verified, as is required for the consumer's request to know specific information, then even if not requested by the consumer, the business should still evaluate the request as if they had asked for categories of personal information (which requires a lower standard of verification).
- **Service Provider Usage Exceptions:** The attorney general provided additional flexibility for service providers that use personal information received from a business for purposes beyond the core provision of services to that business, such as to build or improve the quality of its services. While the statute itself is fairly restrictive of personal information usage by service providers, the attorney general's regulation reflects the input of the business community by considering that limited additional usage may be necessary for the service provider to operate, even if the usage only provides indirect benefits to the associated business or end consumer.
- **Compliance Statistics:** The attorney general introduced an entirely new requirement that certain businesses handling a high volume of consumer personal information (*i.e.*, a company that buys, sells, receives for commercial purposes or shares for commercial purposes, the personal information of 10 million or more consumers in a calendar year) must compile certain metrics regarding their request processing (such as number of requests that the business received, complied with or denied) and publish such information in the company's privacy policy. This requirement is meant to meaningfully increase the public accountability of businesses that process the personal information of a large number of California consumers. The FSOR further explains that the attorney general hopes publishing such statistics will empower the general public, academic institutions, consumer advocates and business groups to analyze such information in ways that further consumer privacy rights and discourage the systematic rejection of consumer requests by businesses.
- **Request Receipt Confirmation:** The attorney general created a new obligation for businesses to confirm the receipt of a consumer's request to know or delete within 10 business days. At that time, the business must inform the consumer how the request will be processed, and include verification steps and an expected response time (unless the request has already been granted or denied). The confirmation may be provided in the same manner in which the request was received (*e.g.*, via phone call), though use of the same method of communication is not required.

Key Takeaways

With the attorney general's regulations set to go into effect imminently, businesses that have not already taken steps to update their privacy policy and compliance posture in alignment with the latest regulations should identify any required updates to their current practices and implement such changes as soon as feasible. Since the attorney general's office has signaled that it intends to begin enforcing the law and regulations as soon as permitted,[1] businesses should not expect to see an enforcement delay due to COVID-19-related business interruptions.

Return to Table of Contents

California Privacy Rights Act Will Appear on the November Ballot

A proposed law that would expand privacy protections for personal information for California residents has collected enough signatures to be added to the 2020 general election ballot.

On June 24, 2020, California Secretary of State Alex Padilla announced that the California Privacy Rights Act of 2020 (CPRA)[2] had received enough signatures to be included on the ballot for the general election on November 3, 2020. Californians for Consumer Privacy submitted more than 900,000 signatures in support of the CPRA, which, if adopted, would expand the CCPA by implementing rights and obligations similar to Europe's General Data Protection Regulation (GDPR). Californians for Consumer Privacy is the same nonprofit that led the 2018 initiative to put the CCPA on the ballot. Negotiations to have that initiative removed from the ballot led to the rapid enactment of the CCPA.

If passed, the CPRA would become effective on January 1, 2021. However, the CPRA would only apply to information collected after January 1, 2022, and the majority of compliance obligations would not become effective until 2023. Accordingly,

[1] See *Forbes* article "Citing COVID-19, Trade Groups Ask California's Attorney General To Delay Data Privacy Enforcement" (March 19, 2020).

[2] See the text of the CPRA.

businesses would still need to comply with the CCPA until 2023. Unlike the Consumer Right to Privacy Act of 2018, which was withdrawn prior to being certified to the ballot while the CCPA was negotiated and passed, the CPRA can no longer be withdrawn given the California Election Code's June 25, 2020, cutoff for withdrawal and deadline requiring certification by the Secretary of State in order to appear on the November 2020 ballot. left until the election.

The CPRA would expand the protections afforded under the CCPA by increasing obligations on businesses, broadening consumer rights and creating a new enforcement mechanism. The law also would increase the threshold that triggers whether a business must comply with the CCPA from collecting personal information from 50,000 to 100,000 California consumers or households per year. This will exempt a larger tier of small- to medium-sized businesses.

Additionally, if passed, the CPRA would:

- eliminate the 30-day cure period for certain violations currently allowed under the CCPA;
- establish the California Privacy Protection Agency, which would have the authority to investigate and enforce violations of the CPRA;
- require businesses, upon a verifiable consumer request, to use commercially reasonable efforts to correct inaccurate personal information;
- extend the CCPA's exemptions for personal information collected in the (1) employment and (2) certain business-to-business contexts to January 1, 2023;
- require businesses to inform consumers about their data retention policies, including the length of time each category of personal information will be retained, and prevent business from retaining personal information longer than is reasonably necessary for the purpose for which it was disclosed by the consumer;
- increase protections for sensitive personal information, which would include precise consumer geolocation, email or text content, philosophical or religious beliefs, and health information. Consumers would be allowed to opt out of the sharing of such information with third parties, including service providers, and businesses would be required to add a second link for this opt-out option;
- limit businesses' use of personal information to purposes "reasonably necessary and proportionate to achieve the purposes for which the personal information was collected or processed," or for another purpose that is in line with the context in which the information was collected;
- require that businesses enter into written agreements with third parties regarding compliance with the CPRA and, upon receipt of consumer deletion requests, notify third parties with whom they have shared personal information;
- allow consumers to opt out of any sharing of personal information (in addition to the sale of such information); and
- introduce opt-out rights for automated decision-making.

Key Takeaways

According to polling conducted in 2019 by Goodwin Simon Strategic Research, nine out of 10 California voters would support a ballot measure such as the CPRA that would expand privacy protection for personal information. While the CPRA would offer significant time to prepare for compliance in 2023, applicable businesses should monitor requirements under the act in the event it passes on Election Day.

Return to Table of Contents

Indiana Court of Appeals Holds That Losses From a Ransomware Attack Are Not Covered Under Policy's Computer Fraud Provision

The Indiana Court of Appeals recently held that losses incurred as a result of a ransomware attack were not covered under the commercial crime coverage part of a multiperil commercial common insurance policy, finding that although the hijacker's actions were illegal, they were not fraudulent — a requirement for policy coverage.

On March 31, 2020, the Indiana Court of Appeals affirmed a trial court's decision that insurer Continental Western Group (Continental) did not owe coverage under a multiperil commercial common insurance policy issued to its insured, G&G Oil Company of Indiana (G&G), for losses sustained as a result of a ransomware attack.[3] On June 4, 2020, the court denied G&G's petition for rehearing.

The Ransomware Attack

In November 2017, G&G suffered a ransomware attack that prohibited the company from accessing its servers and most of its workstations. A hijacker had gained access to G&G's computer network, encrypted its servers and most workstations, and password-protected its drives. After G&G complied with

[3] *G&G Oil Co. of Indiana v. Cont'l W. Ins. Co.*, 145 N.E.3d 842 (Ind. Ct. App. 2020), *reh'g denied* (June 4, 2020).

the hijacker's initial bitcoin demand, the hijacker refused to restore the company's control over its computer servers absent additional payment. Ultimately, G&G made three further bitcoin payments before the hijacker gave the company the passwords to enable decryption of its computers and regain access to its servers.

G&G's Insurance Claim

G&G submitted a claim under its multiperil commercial common insurance policy, issued by Continental, for the losses it incurred from the ransomware attack. The computer fraud provision of the Commercial Crime Coverage part of the policy covered "loss of ... 'money' ... resulting directly from the use of any computer to fraudulently cause a transfer of that property." Continental denied coverage, contending that G&G's losses did not result directly from the use of a computer to fraudulently cause a transfer of the company's funds. G&G then filed an action against Continental in Indiana state court seeking coverage under the policy.

The Trial Court's Decision

On cross-motions for summary judgment, the trial court ruled in Continental's favor, holding that "[u]nlike the fraudster, a hacker, like the burglar or a car thief is forthright in his scheme. The hacker deprived G&G Oil of use of its computer system and extracted bitcoin from [G&G] as ransom. While devious, tortious and criminal, fraudulent it was not." The trial court also concluded that G&G's losses did not directly result from the use of a computer but from a "voluntary payment to accomplish a necessary result."

The Indiana Court of Appeals' Decision

The Indiana Court of Appeals affirmed the trial court's no-coverage decision, holding that "the hijacker did not use a computer to *fraudulently* cause G&G to purchase bitcoin to pay as ransom." In reaching its decision, the court rejected G&G's argument that "fraud," a term left undefined by the policy, should be interpreted broadly to include any "deceptive and unconscionable" act. Rather, resorting to dictionary definitions, the court reasoned that the term "fraud" is commonly understood as the "intentional perversion of truth in order to induce another to part with something of value or to surrender a legal right." The court determined that even though the hijacker's actions were illegal, there was no deception involved in the hijacker's demand for ransom in exchange for restoring G&G's control over its computer system. Accordingly, the court concluded that G&G's insurance claim was not covered under the policy, and thus there was no need to consider whether the company's losses resulted "directly" from the use of a computer.

Key Takeaways

The *G&G* decision illustrates the fundamental point that, as with all insurance policies, coverage for cyber-related losses will be based on the specific facts of the claim and the language of the insurance policy at issue. In this case, the court determined that losses arising out of a ransomware attack where a hijacker gained control over a company's computers were not covered by a computer fraud provision because the losses were not fraudulently caused, serving as an important reminder for insurers and policyholders alike to closely review and fully understand the terms and conditions of their policies.

Return to Table of Contents

Ninth Circuit Finds California Law Requiring Removal of User Ages Unconstitutional

On June 19, 2020, the U.S. Court of Appeals for the Ninth Circuit held that a 2016 California law that would have required commercial online entertainment employment service provider sites, upon request, to remove the age of any subscriber on any site under the provider's control was unconstitutional.

Background

In September 2016, California passed Assembly Bill 1687 (A.B. 1687), which was sponsored by the Screen Actors Guild – American Federation of Television and Radio Artists (SAG) and designed to address age discrimination in the entertainment industry. A.B. 1687 would have required commercial online entertainment employment service providers to, upon a service subscriber's request, remove the subscriber's age or date of birth from their paid-for profile as well as from any companion website under the provider's control. The law also would have required removal of information even where the public had updated or provided the content without prior review by the provider.

Internet Movie Database, known as IMDb.com (IMDb), filed suit in opposition of A.B. 1687 in the U.S. District Court for the Northern District of California in November 2016. In addition to a publicly available and comprehensive online movie database, IMDb also operates a subscription-based employment service for industry professionals, known as IMDbPro, that connects job-seeking subscribers with producers and casting agents. IMDb alleged A.B. 1687 violated both the First Amendment and the commerce clause of the Constitution, as well as the Communications Decency Act, 47 USC §230(f)(2). The district court granted IMDb's motion on First Amendment grounds and

entered a preliminary injunction prohibiting enforcement of the statute. The court later granted IMDb's motion for summary judgment on its facial challenge to A.B. 1687, finding that, while combating age discrimination in the entertainment industry is in fact a compelling government interest, the state of California and SAG failed to introduce evidence to show A.B. 1687 was necessary, or narrowly tailored, to meet that interest.

The Decision

In its decision, the Ninth Circuit unanimously upheld the district court's finding. The Ninth Circuit focused primarily on the A.B. 1687's requirement to remove age information from IMDb's public "companion" websites, such as IMDb.com, noting that subscribers already have the capability to revise their own paid-for profiles on IMDbPro, a fact neither party disputed.

As an initial matter, the Ninth Circuit held A.B. 1687 imposed a content-based restriction on speech, invoking First Amendment strict scrutiny. It rejected the state's argument that A.B. 1687 regulated contractual obligations, and thus was not subject to constitutional analysis, as it found A.B. 1687 extended well beyond the terms of any contractual agreement with a subscriber when it restricted the publication of information submitted by the public with no contractual relationship with IMDb.

The Ninth Circuit also rejected the state's argument that A.B. 1687 regulated a category of speech subject to a less demanding standard of review than strict scrutiny, as A.B. 1687 did not regulate commercial speech, speech that facilitated illegal conduct or speech that implicated privacy concerns. Regarding the state and SAG's commercial speech argument, the Ninth Circuit found that the free, publicly available profiles offered on IMDb.com is "encyclopedic, not transactional" in nature. That IMDb has a financial interest in these public profiles was not sufficient to characterize the publication of information on those sites as commercial. The court also declined to find — and stated neither it nor the Supreme Court has ever found — that content-based restrictions that implicate only privacy concerns can evade strict scrutiny. This, the court stated, is particularly true of those restrictions on lawfully obtained age information. The Ninth Circuit also distinguished A.B. 1687 from state and federal statutes that regulate data collection and disclosure without implicating the First Amendment, as, unlike A.B. 1687, these statutes regulate the misuse of information by entities that obtain the information through an exchange between individuals. By contrast, A.B. 1687 prohibits the publication of information to the public regardless of how that information was obtained.

Under its strict scrutiny analysis, the Ninth Circuit held that A.B. 1687 was facially unconstitutional. Although it did find reducing incidents of age discrimination to be a compelling government interest, the court held that the state and SAG failed to show A.B. 1687 was the least restrictive means and narrowly tailored to meet that interest. Specifically, it stated the state and SAG "[did] not explore, or even consider, a less restrictive means" to combat age discrimination in the entertainment industry, nor did it dispute that other speech-neutral remedies exist, including various laws targeted at discrimination "at [the State's] disposal."

The Ninth Circuit also suggested A.B. 1687 seemed to specifically target sites such as IMDb, as it left unrestricted "every other" avenue through which age information may be disseminated. The court also found A.B. 1687 to be underinclusive, as it failed to reach other potential sources of age information and protected only industry professionals who both subscribe to such a service and choose to have their information removed.

Key Takeaways

The Ninth Circuit's decision highlights the challenge in regulating public forums and the tensions that may arise between First Amendment rights and the right to privacy in these spaces. Ultimately, the ruling shows that when content-based restrictions are in question, some courts are reluctant to avoid First Amendment strict scrutiny review, even when privacy concerns are at issue.

Return to Table of Contents

Progress Report on the EU's Draft ePrivacy Regulation Published by Presidency of the European Council

On January 10, 2017, the European Commission adopted a proposal to replace the Privacy and Electronic Communications Directive 2002 (directive) with a regulation (Draft ePrivacy Regulation) in order to bring it into line with the GDPR. The stated aim of the Draft ePrivacy Regulation was to reinforce "trust and security in the Digital Single Market." Since it was first proposed in 2017, the Draft ePrivacy Regulation has gone through various iterations, the latest of which was published on February 21, 2020. On June 3, 2020, the Presidency of the European Council (presidency) published an update on the status of the regulation. Below, we explain how the Draft ePrivacy Regulation complements the GDPR and consider the key takeaways from the report.

Draft ePrivacy Regulation and the GDPR

While the GDPR is *lex generalis*, regulating all processing of personal data in the European Economic Area (EEA) generally, the Draft ePrivacy Regulation is *lex specialis*, governing electronic communication services and the data processed by

electronic communication services. Once it is enacted, the specific provisions in the Draft ePrivacy Regulation will take precedence over the more general provisions of the GDPR.

In practice, the key areas the Draft ePrivacy Regulation will cover are (1) the rules in relation to direct marketing communications and (2) the circumstances in which cookies or similar technologies can be placed on a user's device. The Draft ePrivacy Regulation should therefore be on the radar of any organization that has a website geared towards consumers in the EEA, as well as any organization that wishes to market its products via email to consumers in the EEA.

Details of the Report

The report details that the key modification in the latest iteration of the Draft ePrivacy Regulation is the addition of "legitimate interest" as a legal ground. Under Article 6(b) of the Draft ePrivacy Regulation, providers of electronic communications networks and services are permitted to process electronic communications metadata, including cookies, only where there is valid legal ground. In previous drafts, obtaining the consent of the user was, in many cases, the only viable legal ground to process such electronic communications metadata. This also is the case with the directive. In practice, this means that the website operator has to obtain the consent of the user in order to place cookies on their device, unless the cookies are essential for the operation of the website. Consent is usually obtained through a cookie banner that appears on the website on a user's first visit. However, the Draft ePrivacy Regulation permits the processing of electronic metadata where "it is necessary for the purpose of the legitimate interests pursued by the electronic communications service or network provider." This is a major departure from the previous draft and the current directive, and, in practice, could mean that cookie banners obtaining a user's consent are no longer necessary in order to place nonessential cookies on a user's device.

The reliance on legitimate interests is subject to the following safeguards contained in Article 17(c) of the Draft ePrivacy Regulation:

- a data protection impact assessment should be carried out and, where appropriate, a supervisory authority should be consulted;
- the metadata should not be shared with third parties, unless it has been anonymized;
- where necessary, appropriate security measures such as encryption and pseudonymization should be implemented; and
- the end-user must be provided with information about the processing and be given the right to object to the processing.

As is the case in the GDPR, legitimate interests cannot be used where the fundamental rights and freedoms of the individual override those legitimate interests. EU member states' reactions to the introduction of legitimate interests were, according to the report, "rather mixed." The report outlines that some member states want to revert to the more granular — and limited — legal grounds from the previous draft, while others have welcomed the Draft ePrivacy Regulation's alignment with the GDPR.

Key Takeaways

The Draft ePrivacy Regulation, once finalized and enacted, will have a major impact on website operators, particularly if the legitimate interests legal ground remains. Under the directive, consent must be obtained in order to place cookies on a user's device, with the stringency of the consent requirements differing between jurisdictions because of divergent regulatory guidance. This lack of harmonization could be a costly compliance exercise for businesses and could result in a multitude of differing cookie banners between jurisdictions. If businesses can rely on legitimate interests in order to place cookies on a user's device, most website cookie banners likely would disappear. This may be a positive for individuals from a usability perspective, but it may come at a cost to users' privacy. Given the high privacy standards afforded to data subjects in the GDPR, this would be a surprising development.

The report also notes that further discussions have been disrupted because of the COVID-19 pandemic. The expert-led Working Party on Telecommunications and Information Society was due to review the Draft ePrivacy Regulation at the beginning of June, but deliberations have been suspended. The next stage of legislative scrutiny is a trialogue involving negotiations between representatives from the European Parliament, the Council of the EU and the European Commission. The trialogue will consider the Draft ePrivacy Regulation and attempt to reconcile differences between the three entities. The inclusion of legitimate interests as a legal ground will form a central part of the negotiations.

Return to Table of Contents

Privacy & Cybersecurity Update

Contacts

Stuart D. Levi
Partner / New York
212.735.2750
stuart.levi@skadden.com

James Carroll
Partner / Boston
617.573.4801
james.carroll@skadden.com

Brian Duwe
Partner / Chicago
312.407.0816
brian.duwe@skadden.com

David Eisman
Partner / Los Angeles
213.687.5010
david.eisman@skadden.com

Patrick Fitzgerald
Partner / Chicago
312.407.0508
patrick.fitzgerald@skadden.com

Todd E. Freed
Partner / New York
212.735.3714
todd.freed@skadden.com

Marc S. Gerber
Partner / Washington, D.C.
202.371.7233
marc.gerber@skadden.com

Rich Grossman
Partner / New York
212.735.2116
richard.grossman@skadden.com

Michael E. Leiter
Partner / Washington, D.C.
202.371.7540
michael.leiter@skadden.com

Amy Park
Partner / Palo Alto
650.470.4511
amy.park@skadden.com

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

Jason D. Russell
Partner / Los Angeles
213.687.5328
jason.russell@skadden.com

David Schwartz
Partner / New York
212.735.2473
david.schwartz@skadden.com

Ingrid Vandenborre
Partner / Brussels
32.2.639.0336
ingrid.vandenborre@skadden.com

Helena Derbyshire
Of Counsel / London
44.20.7519.7086
helena.derbyshire@skadden.com

Jessica N. Cohen
Counsel / New York
212.735.2793
jessica.cohen@skadden.com

Peter Luneau
Counsel / New York
212.735.2917
peter.luneau@skadden.com

James S. Talbot
Counsel / New York
212.735.4133
james.talbot@skadden.com

Eve-Christie Vermynck
Counsel / London
44.20.7519.7097
eve-christie.vermynck@skadden.com

Skadden, Arps, Slate, Meagher & Flom LLP
One Manhattan West
New York, NY 10001
212.735.3000