Skadden

Privacy & Cybersecurity Update

EU Rejection of US-EU Safe Harbor: What Companies Need to Know

Events following the EU Court of Justice's *Schrems* decision invalidating the U.S.-EU Safe Harbor framework highlight the ongoing uncertainty of data transfers to the U.S. under EU data privacy laws. Meanwhile, the EU has set a three-month grace period and deadline for developing a new framework.

The October 6, 2015, ruling by the Court of Justice of the European Union invalidating the U.S.-EU Safe Harbor framework sent shock waves through the U.S. and European business communities. It highlights two key issues. First, we have entered a new era in which EU privacy rights could have a direct and significant impact on commerce between the EU and U.S. The decision also comes at a time when there are serious concerns within the business community that the EU data protection law the General Data Protection Regulation — which may be finalized by the end of the year — will impose new and significant obligations on companies that handle any EU personal data, with potentially large sanctions for failing to comply. Second, access by the U.S. government to personal information for intelligence purposes is having an impact on commercial uses of data.

In our special October 7, 2015, edition of our *Privacy & Cybersecurity Update*, we described in detail the Court of Justice's decision in *Schrems v. Data Protection Commissioner*.[1]

Background

Under the EU Data Protection Directive, personal information about EU citizens can only be transferred from the EU to countries with "adequate" data protection. Only a small handful of countries satisfy this requirement, and the U.S. is not one of them. The European Commission has provided a few mechanisms for companies to conduct such transfers if they are not located in a country that meets the adequacy requirement.

[1] The court's ruling and related documents are available here.

In the U.S., one of these mechanisms is the Safe Harbor, which was negotiated between the European Commission and the U.S. Department of Commerce and went into effect in 2000. To enjoy the benefits of the Safe Harbor, a company needed to self-certify to the Department of Commerce that it complied with specified EU privacy standards. Once the company had self-certified, it could receive personal data from the EU. As of 2015, over 4,500 U.S. companies had joined the Safe Harbor.

In *Schrems*, the Court of Justice found that the Safe Harbor was invalid since it does not address the U.S. government's nearly unrestricted access to much of this data, as revealed through Edward Snowden's and other revelations regarding U.S. intelligence practices. The court also found that, even though the European Commission determined that the Safe Harbor provided an adequate level of protection for personal data, individual data protection commissioners in the EU member states have "complete independence" to conduct their own investigations and make their own determinations of adequacy, and are free to challenge the European Commission's decisions before the Court of Justice.

Without the Safe Harbor's protection, businesses that transfer personal data from the EU to the U.S. are left with limited options to comply with the law, including:

- Obtaining express consent from the data subject (although this consent can be revoked, rendering this approach potentially cumbersome to administer);
- Entering into "model contracts" based on form agreements approved by the European Commission for this purpose;
- Where the transferor and transferee are part of the same multinational corporation, adopting binding corporate rules that are approved by the local data protection authority or authorities (though the approval process typically takes 18 months or more); and
- Relying on certain other express exceptions to the prohibition on such data transfers, including where the transfer is necessary for the performance of a contract between the data subject and the data controller (which the EU has interpreted narrowly to exclude, for example, transfer of employment information from an EU-based subsidiary to a U.S.-based parent).

Are 'Model Contracts' Also at Risk?

After *Schrems*, many media reports noted that companies that relied on the Safe Harbor would likely switch over to the model contracts approach, even though it can be cumbersome for companies that take in data from multiple sources in Europe. However, the model contracts themselves now are also under a cloud of uncertainty given that they present the same issue as the Safe Harbor — namely, that the U.S. intelligence community has broad access to EU data stored in the U.S.

Indeed, one EU data protection authority already has adopted that position. Shortly after the *Schrems* decision, Marit Hansen, head of the ULD (the data protection authority in the German state of Schleswig-Holstein) issued a press release and position paper questioning the validity of the "model contracts" approach.[2] Hansen wrote that "a lasting solution can only be in a significant change in U.S. law" and that local businesses that transmit personal information to the U.S. should review their procedures as soon as possible and "consider alternatives" for processing in the United States. Hansen further argued that companies that use the standard model contracts should cancel them and do a complete review of all data transfers. In conducting this review, Hansen indicated that companies should consult with the ULD in virtually every instance.

Despite the ULD's pronouncement, on October 16, 2015, the Article 29 Working Party, which is primarily comprised of representatives from the data protection authorities of each EU member state,[3] issued a statement declaring that, pending further analysis, EU data protection authorities considered the model contracts a still-viable means of transferring data to the U.S.[4]

In an interview, European Data Protection Supervisor Giovanni Buttarelli sounded a cautionary note, stating that while mechanisms such as the model contracts and obtaining a data subject's consent were not affected by the *Schrems* ruling, they "need to be analyzed" and may ultimately need to be amended.[5]

In short, although the European Commission is taking the positon that the model contracts remain a valid means for enabling transfers of data from the EU to the U.S., there is a realistic possibility that this view will change. Whether the EU authorities or courts ultimately decide to dispense with the model contracts altogether, amend them or leave them unchanged, businesses that transfer personal data from the EU to the U.S. will have to pay close attention to this issue.

Will Other Countries Follow Suit?

A limited number of other countries have data protection laws that are similar to the EU directive, and some follow the EU's lead on determining whether a country's data protection laws provide adequate protection for personal data. Following the *Schrems* decision, these countries also may decide to no longer permit transfers of personal data to the U.S. on the basis of the Safe Harbor.

[2] Schleswig-Holstein German State, Center for Data Protection, "Position Paper of the ULD to Safe Harbor Court of Justice of the European Union of 6 October 2015 C-362/14."

[3] The Working Party also includes representatives from the European Commission and the European data protection supervisor. The European data protection supervisor is a position created by the directive to play a variety of roles within the EU data privacy regime, including providing supervisory and consultative functions among the various member state data protection authorities.

[4] The Article 29 Working Party (Oct. 16, 2015) statement is available here.

[5] A video of the interview is available here.

Israel is one such country, and its data protection laws explicitly rely on the EU's judgment of adequacy. On October 19, 2015, the Israeli Law, Information and Technology Authority announced that it was revoking its approval of data transfers to the U.S. that were based on the Safe Harbor.[6] The Israeli data protection law includes exceptions that are similar to those in the directive, including consent and the EU's model contracts, but any decisions by the EU limiting the validity of those approaches will impact Israel/U.S. data transfers as well.

Replacing the Safe Harbor

Even before the *Schrems* decision, representatives from the United States and the European Union were negotiating a replacement for the Safe Harbor. The decision has placed a new urgency on these negotiations, but the rationale behind the Court of Justice's opinion may create an unsurmountable hurdle to developing a replacement framework that satisfies the court's concerns.

In 2013, the EU published a list of 13 recommendations to revise the Safe Harbor to provide greater protection for personal data, many of which stemmed from the same Snowden revelations that inspired the *Schrems* suit and, ultimately, the court's verdict. The recommendations included requiring Safe Harbor companies to publish the privacy requirements of any contracts they enter into with subcontractors that would have access to personal data, strengthening Department of Commerce monitoring of whether self-certifying Safe Harbor companies were actually obeying the Safe Harbor's requirements and tightly narrowing the Safe Harbor's exception for national security matters.

The EU and U.S. entered into negotiations soon after the EU published the recommendations, and those negotiations are ongoing. In 2014, however, Federal Trade Commissioner Julie Brill stated that the recommendations relating to national security matters could not be negotiated by the U.S. representatives, as they were outside the jurisdiction of the organizations responsible for negotiating the Safe Harbor regime: the Department of Commerce and the Federal Trade Commission.

In light of Brill's announcement, and the court's decision invalidating the Safe Harbor primarily because of the very national security exceptions that Brill announced could not be negotiated, it is unclear whether the ongoing Safe Harbor negotiators will be able to find common ground.

Further, even if EU and U.S. negotiators agree on a new Safe Harbor, the *Schrems* decision makes clear that national data protection authorities retain the authority to review data protection practices on their own. These authorities could decide that an agreement does not meet local standards — for example, if it does not adequately limit the U.S. government's access to personal data. Those negotiating a new Safe Harbor may therefore seek the tacit approval of each data protection authority so that they do not negotiate a Safe Harbor that is then rejected by one.

EU Offers Three-Month Grace Period

In its October 16, 2015, statement, the Article 29 Working Party announced that it would give U.S. and EU negotiators until the end of January 2016 to agree on a revised Safe Harbor. Until then, EU data protection regulators will not take enforcement actions against companies that were using other means to address data protection matters, such as the EU's model contracts.

The Working Party has threatened potentially dire consequences if no Safe Harbor regime has been agreed by its deadline. The group announced that after January 2016, if no replacement Safe Harbor has been put into place, and if EU regulators determine that the other mechanisms do not afford adequate data protections, national authorities will take "all necessary and appropriate actions" to protect personal data. These may include "coordinated enforcement actions" against violators. Under the directive, these actions could result in fines of up to 5 percent of a violator's operational costs.

Key Next Steps

In response to the uncertainties regarding EU-U.S. data transfers, many companies have quickly put model contracts in place to facilitate the transfer of personal data from the EU to the U.S. As noted, however, even these contracts may be in jeopardy based on the *Schrems* decision, and it is conceivable that no set of model contracts, and no replacement Safe Harbor regime, will satisfy all of the data protection authorities in all the EU member states.

It is important, therefore, for all businesses that transfer data from the EU to the U.S. evaluate their data practices. This evaluation should include an understanding of all data transferred from the EU to the U.S. so that any required changes can be implemented quickly. Companies may also want to start considering their options should they encounter a period of time during which there is no permissible way to transfer that data to the United States. While this is a highly unlikely scenario, many also did not believe the Court of Justice would invalidate the Safe Harbor.

The Department of Commerce and various EU-based data protection authorities are expected, in the coming weeks, to release advice and updates to companies seeking to transfer personal data from the EU to the U.S. Companies should be on the lookout for these releases and evaluate their data practices accordingly.

Return to Table of Contents

[6] An unofficial translation of the statement is available here.

Senate Passes Long-Delayed Cybersecurity Bill

The Senate has passed a long-negotiated cybersecurity bill that seeks to encourage companies to share cyberthreat information, amid concerns over consumer privacy issues. The bill must be reconciled with similar House bills before being sent to the president for his signature.

On October 27, 2015, after a six-year effort, the Senate passed its version of the Cybersecurity Information Sharing Act (CISA), a bill that seeks to encourage companies to voluntarily share cybersecurity threat data among themselves and with the U.S. government.[7] The bill allows companies to share this information regardless of other laws — such as antitrust laws and laws regarding consumer privacy — that might otherwise prevent such sharing. Consumer advocates have objected that CISA does not sufficiently protect consumer information, although the bill does require that participating companies remove any personally identifiable information before sharing the data.

The House of Representatives has passed similar bills in the past, and CISA will need to go through the conference committee process so that House and Senate negotiators can develop a final, compromise bill. The White House has signaled support for the Senate bill, so it appears likely that if the House and Senate can agree on a compromise bill, it will quickly become law. When and if such a law is signed, we will provide further information in this newsletter.

Return to Table of Contents

California Passes Law Limiting Law Enforcement Access to Digital Records

California has passed a law seeking to limit government access to electronic information. The law may become a model for other states to follow, but it will not have a direct impact on federal government access to electronic records.

On October 8, 2015, California Gov. Jerry Brown signed into law the California Electronic Communications Privacy Act (CalECPA). This law updates California's existing privacy laws by requiring any department or agency of the state of California, including state law enforcement, to obtain a warrant to access digital records such as images, emails, texts, metadata and location information.

Background

In most states, many of the types of data now protected by CalECPA remain subject to warrantless searches under the federal Electronic Communications Privacy Act (ECPA). The courts — including the U.S. Supreme Court, which unanimously held in *Riley v. California*[8] that the warrantless search of a smartphone violated the Fourth Amendment — seek to strike a balance between the government's ability to access electronic records and the privacy of the individuals to whom such records belong. But privacy advocates and other stakeholders agree that new legislation is required to provide clear guidance and procedures for obtaining such records. In addition, technology companies such as Facebook, LinkedIn, Twitter and Google — which receive an ever-increasing number of requests for information from law enforcement, often without a warrant — have long advocated for clearer laws protecting them from having to disclose this information. These companies have come under increasing public pressure and scrutiny in recent years as a result of the revelation that the U.S. government had been extensively collecting digital communications and other data without a warrant.

CalECPA and Existing Federal Law

CalECPA represents a significant step in the direction of protecting technology companies and their customers from the type of open-ended access to personal information that has drawn so much scrutiny. Under the new law, law enforcement and other agents of the California government may not, subject to certain specified exceptions, require service providers to disclose digital records unless (i) such service provider is served with a warrant that complies with federal and state law,[9] and (ii) the government entity serves the identified target of the warrant with notice thereof, including a description of the information being sought and the nature of the government investigation.[10] Notably, the law protects not only digital communications and metadata related thereto but also "the current and prior locations of [a] device."[11]

CalECPA, however, does not apply to requests for information from the federal government, which will continue to be governed by the federal ECPA. Under that law, digital information such as emails and other data that have remained in storage for over 180 days may be obtained by administrative subpoena and notice to the individual whose information is being sought, though such notice may be delayed if the government provides the court with "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are

[7] S.754 - Cybersecurity Information Sharing Act of 2015.

[8] 134 S. Ct. 2473 (2014).

[9] Cal. Penal §§ 1546.1(b), (c), (d)(3) (2015).

[10] Cal. Penal § 1546.2(a) (2015).

[11] Cal. Penal § 1546(g) (2015).

relevant and material to an ongoing criminal investigation."[12] While many attempts have been made to similarly update the federal ECPA, thus far all such attempts have stalled.

Impact of the New Law

All U.S. companies that receive requests from law enforcement for digital records should familiarize themselves with this new California law, as historically, privacy laws enacted in California have later been adopted by other states. Several states already have laws similar to CalECPA,[13] and as noted above, the federal government is also considering an update to the federal law, which likely will include many of the same procedures as are found in CalECPA.[14]

Furthermore, in light of the European Court of Justice's *Schrems* ruling invalidating the U.S.-EU Safe Harbor program — in part because of the kinds of widespread government access to data that CalECPA seeks to curtail — laws such as these may help EU data protection regulators come to accept the United States as a safe recipient of personal data from the EU.

Return to Table of Contents

Eleventh Circuit Finds Users of Free TV Mobile App Are Not 'Subscribers' Under Video Privacy Law

A Court of Appeals has ruled that a mobile app provider can share user information with third parties without violating the Video Privacy Protection Act. Because the users could view the content without paying a fee, they were not "subscribers" protected under the Act, the court found.

The U.S. Court of Appeals for the Eleventh Circuit affirmed on October 9, 2015, that a television network did not violate the Video Privacy Protection Act (VPPA or the Act) by sharing information about users of its free mobile application (app) with third parties. In *Mark Ellis v. The Cartoon Network, Inc.*, the court held that such users are not "subscribers" within the meaning of the Act.[15] The decision follows in the wake of various other class action litigations seeking to apply the Act to disclosure of mobile app user information, and some expect it will incentivize service providers to stream free content to reduce their exposure under the Act.

Cartoon Network's App

At issue was the Cartoon Network's free CN app, which smartphone users can download to their phones to stream clips or episodes of Cartoon Network shows. Though app users can access additional content by logging into the app with their cable provider information, merely downloading and streaming the basic content does not require users to create a login account or provide any registration information.

When downloaded to an Android smartphone without the identifying login information, Cartoon Network's app identifies the user through his or her mobile device identification (Android ID) and tracks the user's viewing history. Each time the Android user exits the CN app, the network sends a record of the user's history — the user's Android ID and a list of content streamed — to Bango, a data analytics company. Bango, which tracks users across multiple devices and services, can automatically identify an individual by compiling information linked to the Android ID from other websites, applications and sources. As a result, Bango, upon receiving the plaintiff's viewing history from the Cartoon Network, was able to link the Android ID and viewing history to the individual — despite the CN app never asking users to consent to the Cartoon Network sharing or otherwise disclosing personally identifiable information to third parties.

The Video Privacy Protection Act

In the *Mark Ellis* case, the plaintiff argued that the CN app violated the VPPA, a statute with a storied legislative history that courts and claimants have struggled to apply in the context of more modern technologies. In 1998, a newspaper published a profile of U.S. Supreme Court nominee Robert Bork that included the titles of 146 videos he and his family had rented from a local video store.[16] Congress responded by enacting the VPPA, which sought "to preserve personal privacy with respect to the rental, purchase, or delivery of video tapes or similar audio visual materials."[17]

Amended in 2012, the VPPA generally prohibits service providers from knowingly disclosing to a third party personally identifiable information concerning any consumer without informed consumer consent. The Act defines a "consumer" as a renter, purchaser or subscriber of goods or services from a video tape service provider,[18] and it is the last definition — the

[12] 18 U.S.C. §2703(d).

[13] Laws with similar protections have been enacted in Utah, Maine, Texas and Virginia.

[14] For example, the current draft of S. 356, the Electronic Communications Privacy Act Amendments Act of 2015, would require a warrant for electronic communications data but would not afford the same protections to location data.

[15] *See Mark Ellis v. The Cartoon Network, Inc.*, 14-15046 (11th Cir. 2015).

[16] *See* S. Rep. 100–599, 2d Sess., at 5 (1988), *reprinted in* 1988 U.S.C.C.A.N. 4342.

[17] *See* 134 Cong. Rec. S5396–08, S. 2361 (May 10, 1988).

[18] *See* 18 U.S.C. § 2710(a).

term "subscriber" — that found itself the focus of the Eleventh Circuit analysis. Focusing on the lack of an ongoing relationship between the plaintiff and the service provider, the court ruled that users who merely download an app for free and view streaming content on it are not subscribers, particularly because the user may delete the app at whim and without consequence.[19] Based on this interpretation, the court held that the plaintiff was not a "subscriber" within the meaning of the Act, and that the Cartoon Network therefore did not violate the VPPA by passing his information to Bango.[20]

Impact of Decision

If followed in other circuits, the Eleventh Circuit's ruling in *Mark Ellis* could dramatically limit the Act's relevance to mobile applications. Prior to *Mark Ellis*, the few district courts to consider the question had come to varied, fact-specific conclusions.[21] The *Mark Ellis* holding potentially diminishes the number of potential plaintiffs while providing guidance to companies seeking to avoid liability under the Act. Though payment is not a prerequisite of subscription, the Eleventh Circuit decision emphasizes that a "subscriber" is one who is involved in a give-and-take of some kind with a service provider. Payment, registration, commitment, delivery or access to restricted content are typical examples of this kind of more substantial relationship.[22] Companies seeking to avoid liability under the VPPA could consider altering their product offerings in light of this ruling, such as shifting to free content-delivery systems and foregoing any login requirements.

Return to Table of Contents

[19] *See Mark Ellis v. The Cartoon Network, Inc.*, 14-15046 at *6.

[20] The court declined to consider whether the report Bango received from the CN app qualified as "personally identifiable information" under the VPPA. The district court below had found that the plaintiff qualified as a "subscriber" under the VPPA, but that the information Bango received did not constitute "personally identifiable information." *See Mark Ellis v. The Cartoon Network, Inc.*, 14-15046 at *3, *6 fn. 2.

[21] *Compare Yershov v. Gannett Satellite Info. Network, Inc.*, ––– F.Supp.3d ––––, ––––––––, 2015 WL 2340752, at *9–10 (D.Mass. May 15, 2015) (holding that a person who simply downloads a free app on a mobile device is not a "subscriber") and *Austin–Spearman v. AMC Network Entm't LLC*, ––– F.Supp.3d ––––, ––––––––, 2015 WL 1539052, at *6–8 (S.D.N.Y. Apr. 7, 2015) (stating that "casual consumption of web content, without any attempt to affiliate with or connect to the provider, exhibits none of the critical characteristics of subscription," and holding that a person who merely visits a provider's website and watches video clips is not a "subscriber"), *with, e.g.*, *Locklear v. Dow Jones & Co., Inc.*, ––– F.Supp.3d ––––, ––––––––, 2015 WL 1730068, at *3–4 (N.D.Ga. Jan. 23, 2015) (holding that "if a plaintiff, in addition to visiting a website, pleads that he or she also viewed video content on that website, that plaintiff is a 'subscriber' to a service within the meaning of the VPPA"). *Cf. In re Hulu Privacy Litig.*, 2012 WL 3282960, at *8 (N.D.Cal. Aug. 12, 2012) ("Plaintiffs pleaded more than just visiting Hulu's website. They were subscribers of goods and services.").

[22] *See Mark Ellis v. The Cartoon Network, Inc.*, 14-15046 at *5 (citing *Yershov*, 2015 WL 2340752, at *9).

EU Court Expands Data Protection Authorities' Enforcement Jurisdiction

In a decision relating to the Hungarian data protection authority's right to take action against a Slovakia-based website, the EU Court of Justice has expanded the jurisdiction of each EU member state's data regulators, raising the prospect of a company being subject to sanctions by regulators in multiple countries.

On October 1, 2015, in *Weltimmo SRO v. Nemzeti Adatvedelmi es Informacioszabadsag Hatosag*, the European Union Court of Justice ruled that data protection authorities in EU member states have the authority to take data protection actions against companies with even limited contact with the state in question. The court announced its decision less than a week before it issued its landmark *Schrems* ruling voiding the U.S.-EU Safe Harbor regime under the EU's Data Protection Directive and confirming local data protection authorities' rights and duties to engage in independent reviews of decisions by the European Commission. Taken together with the *Schrems* decision, the court's ruling in *Weltimmo* significantly expands the enforcement powers of local data protection authorities and may signal a new era of aggressive data protection enforcement efforts by the EU and/or its individual member states.

Background

The *Weltimmo* case involved an enforcement action brought by the Hungarian data protection authorities against a company with its registered office in Slovakia operating a website hosted in Slovakia. Weltimmo is a website that ran property ads for Hungarian owners. The site ran ads for free for the first month, then charged a fee to continue running them after that month. According to complaints received by the Hungarian data protection authority, however, Weltimmo ignored requests by property owners to remove their ads and personal data from the service after the first month. Instead, the ads continued to appear on the site and, when the property owners refused to pay for them, Weltimmo sent their personal information to debt collection agencies.

When the Hungarian data protection authority levied a fine against Weltimmo, the site operators appealed to the Hungarian Supreme Court, claiming the Hungarian data protection authorities do not have jurisdiction under the EU directive to take action against the company. Under the directive, data controllers such as Weltimmo only have to comply with data protection laws in the country in which they are established. Weltimmo asserted that, as a Slovakian company with a site hosted in Slovakia, it was not established in Hungary. The Hungarian Supreme Court referred the question of jurisdiction to the European Court of Justice.

The Court's Ruling

The Court of Justice ruled that establishment under the directive is not limited to the country in which a company is registered. Instead, if the data controller engages in real and effective activity through "stable arrangements" in a different country, it can be subject to that country's data protection laws.

The court determined that Weltimmo had sufficient contacts with Hungary to be considered established in Hungary and to confer jurisdiction to the Hungarian data protection authorities. The court noted that Weltimmo's site was available in Hungarian and advertised Hungarian properties. Further, the company had a representative in Hungary (with an address in Hungary) who served as a point of contact for customers and who represented the company in administrative and judicial proceedings, had a bank account in Hungary for recovering debts and used a postal box in Hungary for the management of its ordinary business affairs.

Impact of the Court's Decision

The court's decision in *Weltimmo* raises the possibility of a company being subject to the data protection laws of multiple EU member states simultaneously. Although not different from how many multinational businesses operate outside the EU today, the outcome may surprise those companies that thought they, at least in the EU, were only subject to the jurisdiction of one data protection authority. Companies that operate in multiple EU jurisdictions should evaluate whether — despite being registered in only one member state — their activities in others expose them to enforcement in multiple EU jurisdictions.

Taken together with the *Schrems* decision, the *Weltimmo* ruling may signal a new era of independence among EU member state data protection authorities. No longer presenting a united front, and perhaps abandoning some of their traditional deference to the European Commission and their fellow member states, these data protection authorities may present companies doing business in the EU with a complex web of regulations and regulators with which they must comply.

Return to Table of Contents

If you have any questions regarding the matters discussed in this newsletter, please contact the following attorneys or call your regular Skadden contact.

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

Cyrus Amir-Mokri
Partner / New York
212.735.3279
cyrus.amir-mokri@skadden.com

James R. 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
213.687.5381
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

Lisa Gilford
Partner / Los Angeles
213.687.5130
lisa.gilford@skadden.com

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

Timothy A. Miller
Partner / Palo Alto
650.470.4620
timothy.miller@skadden.com

Timothy G. Reynolds
Partner / New York
212.735.2316
timothy.reynolds@skadden.com

Ivan A. Schlager
Partner / Washington, D.C.
202.371.7810
ivan.schlager@skadden.com

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

Michael Y. Scudder
Partner / Chicago
312.407.0877
michael.scudder@skadden.com

Jennifer L. Spaziano
Partner / Washington, D.C.
202.371.7872
jen.spaziano@skadden.com

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

Gregoire Bertrou
Counsel / Paris
33.1.55.27.11.33
gregoire.bertrou@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

Joshua F. Gruenspecht
Associate / Washington, D.C.
202.371.7316
joshua.gruenspecht@skadden.com