Skadden

Privacy & Cybersecurity Update

EU Invalidates Privacy Shield as Means for Transferring Personal Information to the US; Alternative Mechanisms Remain Available

The Court of Justice of the European Union (CJEU) has invalidated the EU-U.S. Privacy Shield framework negotiated between the EU and the U.S., removing a key tool used by companies to transfer personal information from the European Economic Area (EEA) to the U.S. Following the decision, companies will now have to utilize alternative mechanisms to legally continue such transfers.

Introduction

Under the General Data Protection Regulation 2016/679 (GDPR), data transfer mechanisms are used to export data from the EEA to countries outside the EEA that have not been deemed by the European Commission to have an adequate level of privacy protection. The U.S. has not been found to meet this standard. A common mechanism for transferring data to countries with inadequate laws is to use the European Commission Standard Contractual Clauses (SCCs). These are standard form contracts provided by the European Commission that companies can use. In addition, for transfers to the U.S., the European Commission and the U.S. Department of Commerce had negotiated the EU-U.S. Privacy Shield, a self-certification mechanism for data transfers from the EEA to the U.S. A company that was self-certified could transfer in personal data from the EEA, provided it abided by the Privacy Shield terms.

On July 16, 2020, the CJEU ruled in *Irish Data Protection Commissioner vs Facebook and Maximillian Schrems (Schrems II)* that:

- the Privacy Shield was struck down, effective immediately;
- the SCCs are valid, but only subject to the data exporter and data importer carrying out enhanced due diligence on the data protection laws of the applicable importing country;
- where the SCCs' enhanced due diligence returns a negative assessment of the data protection laws of the importing country, and additional safeguards cannot guarantee data subjects' fundamental rights, data exporters must suspend the transfer of personal data to such countries and/or terminate their contract with the data importer; and

- where data exporters do not suspend the transfer and/or terminate their contract with the data importer, EEA supervisory authorities should suspend or prohibit any such transfer.

The CJEU Decision

The Privacy Shield

The CJEU's decision to invalidate the Privacy Shield was based on: (1) the limitations on the protection of personal data under U.S. law, and (2) the disproportionate access and use of EEA personal data by U.S. authorities with no effective redress mechanism for data subjects. In particular, the CJEU found that access to personal data under U.S. surveillance programs could not be regarded as being limited to what is "strictly necessary," and that the Privacy Shield also does not grant individuals based in the EEA actionable rights before U.S. courts against U.S. authorities. According to the CJEU, the Privacy Shield therefore cannot ensure a level of protection "essentially equivalent" to that arising from the GDPR as supplemented by national data protection laws across the EEA, nor can it guarantee individuals' fundamental rights under the EU Charter of Fundamental Rights. Given the broad rationale applied by the CJEU, it will be challenging for U.S. and European officials to replace or modify the Privacy Shield in a manner that complies with the CJEU decision.

The SCCs

While the SCCs remain a valid data transfer mechanism, the court held that it is up to the data exporter and data importer to ensure that, in practice, an adequate level of data protection is provided in the country where the data importer is based. Where a country falls short, the CJEU encouraged parties to enter into "additional safeguards" to those offered by the SCCs, but it did not elaborate on the form such safeguards could take. To date, no EEA supervisory authority has offered guidance.

EU and US Reactions to *Schrems II*

Supervisory authorities across the EEA have had varied reactions to the *Schrems II* judgment. The U.K.'s Information Commissioner's Office (ICO) has been measured in its response, stating that it will take time to analyze and understand the judgment before issuing further guidance. Other supervisory authorities, such as the Berlin supervisory authority in Germany, have taken a stricter approach, explicitly stating that personal data cannot be transferred to the U.S. on the basis of the Privacy Shield and questioning whether such transfers can even be made via the SCCs.

On July 24, 2020, the European Data Protection Board (EDPB) set out its position on *Schrems II* in the form of FAQs. The EDPB confirmed that there was no grace period within which organizations would have time to transition from the Privacy Shield to an alternative — and valid — data transfer mechanism. This position is contrary to the statements of some EEA supervisory authorities and suggests that those organizations relying solely on the Privacy Shield to transfer personal data to the U.S. should promptly consider alternatives. Many key industry players, such as cloud service providers, were quick to issue statements reassuring their customers that despite the *Schrems II* ruling, they would continue to transfer data from Europe to the U.S. in a manner consistent with past practice.

In the U.S., the Department of Commerce and the Federal Trade Commission have both issued statements that the Privacy Shield program has not been discontinued. We expect that there will be further clarification in the future.

Approaches for Companies To Consider

Companies That Previously Relied on the Privacy Shield

As there is no grace period, transfers made on the basis of the Privacy Shield are, according to the EDPB and certain country-specific data protection authorities, illegal as of this moment. As a practical matter:

- European-based data exporters should promptly enter into discussions with U.S.-based data importers regarding how they are addressing this new development; and
- U.S.-based data importers need to determine if they will heed the statements of the EDPB or presume that there is an implicit grace period as U.S. and European officials discuss alternatives. However, as discussed below, even companies that do not plan to take immediate action should start scoping out the alternatives available to them, such as considering entering into a data transfer agreement on the terms of the SCCs.

U.S.-based participants in the Privacy Shield framework should keep in mind that they are still required to comply with their obligations under the framework regarding personal data that has been transferred to the U.S. via the Privacy Shield.

Companies Relying on SCCs

As noted above, under the CJEU ruling, whether a European data exporter can continue to transfer personal data to a data importer located in another country — including the U.S. — using the SCCs will depend on:

- the assessment of the transfer by the data exporter and data importer, taking into account the circumstances; and
- the inclusion of additional safeguards or any supplementary measures as referred to by the EDPB, which parties could implement to ensure that EEA personal data is processed at a level essentially equivalent to that provided by the GDPR.

What this means in practice, without any further guidance, is difficult to predict. In *Schrems II*, the CJEU found that U.S. law does not afford a level of protection equivalent to that under the GDPR. In particular, the court found that U.S. authorities' access to personal data under U.S. surveillance programs could not be regarded as being limited to what is "strictly necessary."

Therefore, additional safeguards will have to be included in order to legitimize data transfers to third countries, including to the U.S. There is not yet clarity as to the form such additional safeguards could take, however, the EDPB in its FAQs has indicated that these supplementary measures would follow a case-by-case analysis of the circumstances surrounding each transfer to ensure that data importer laws do not undermine data protection rights that any EEA-based individuals would be entitled to under applicable data protection laws (including the GDPR). Such supplementary measures would need to ensure that any EEA personal data, once received by data importers in third countries (including the U.S.), would be processed at a level of protection essentially equivalent to that of the GDPR.

There is a risk of regulatory fragmentation across the EEA. Some supervisory authorities (*e.g.*, in the Netherlands and Germany) have indicated that data transfers to the U.S. are currently not possible in light of U.S. surveillance laws and that no additional safeguards can legitimize the transfers. Other supervisory authorities (*e.g.*, in Denmark, France and the U.K.) have indicated that they will provide updated guidance in due course, suggesting that such transfers may be possible. Despite this fragmentation, it is worth bearing in mind that the GDPR requires supervisory authorities across the EEA to work together in order to ensure consistent application of the GDPR.

Given that the practice of using the SCCs as a mechanism to transfer personal data to the U.S. is currently uncertain, organizations should:

- ensure that they have documented their international data flows so they can easily identify the personal data that is transferred to the U.S. from the EEA;
- monitor whether any guidance is issued from the EDPB and any competent supervisory authorities on the exact specification of "additional safeguards"; and
- document their diligence in the form of a Transfer Impact Assessment (TIA), and keep a log of the TIA and any set of supplementary measures in line with the GDPR's accountability principle. These measures may include a transfer checklist for data importers to disclose the standards by which the EEA personal data being imported from the EEA will be processed. It also may include an assessment of the laws of the importing country to determine if the national laws offer an essentially equivalent level of protection to EU data protection laws (including the GDPR). One of the key themes of the *Schrems II* judgment is the access national authorities may be granted to EEA personal data under national surveillance laws. Therefore, an assessment of the national surveillance laws of any third country will be a key component of a TIA to ascertain whether the transfer can proceed.

Special UK Considerations

The U.K. is in a transition period through the end of 2020 as a result of Brexit and has not yet formally left the EU. If the U.K. does not receive an adequacy decision from the European Commission before this date, it will become a "third country" as of January 1, 2021, and EEA-based data exporters will need to implement data transfer mechanisms with U.K.-based data importers.

The U.K.'s national surveillance laws will form part of the assessment for developing the mechanisms. Under the U.K.'s Data Protection Act 2018 (DPA), intelligence services are exempt from compliance with a number of the safeguards in the DPA, including from the prohibition of making any decision based solely on the automated processing of data.[1] In *Schrems II*, the CJEU specifically highlighted the heightened need for effective safeguards where personal data is subject to automated processing. It also is far from clear if there are effective redress mechanisms in place under U.K. law for data subjects for the activities of the U.K. intelligence services, another concern expressed in *Schrems II*.[2]

If the U.K. does not receive an adequacy decision before January 1, 2021, EEA-based data exporters should: (1) along with the data importer, perform a TIA in respect of any proposed transfers to the U.K., (2) enter into SCCs and any additional safeguards as necessary and (3) log their actions to ensure accountability.

Notifying the Competent Supervisory Authority

As of August 1, 2020, the regulatory guidance requires U.S. data importers and non-U.S. "third-country" data importers to take into account the circumstances of the transfer and additional safeguards that could be implemented.

Without specifying what such additional safeguards or supplementary measures would look like, the EDPB FAQs require companies — to the extent they concluded that an essentially equivalent level of protection cannot be ensured — to suspend and/or terminate a transfer in question or, alternatively, to notify their competent supervisory authority. Companies should at least

[1] Section 96(1) DPA.

[2] Sections 110 and 11 DPA; certain other exemptions in Schedule 11 DPA remain untested.

start their data transfer assessment process exercise, pending further clarification from the European Commission and the EDPB on the types of supplementary measures expected to be implemented and the content of such notification.

Binding Corporate Rules (BCRs)

Although not the subject of *Schrems II*, the judgment also has implications for intercompany transfers made via BCRs, which involve transferring EEA personal data to the U.S. using the SCCs. Where intercompany data flows involve transfers of EEA personal data to third countries, including the U.S., companies will be required to perform a similar assessment exercise, including the consideration of additional safeguards, on a case-by-case basis.

For Data Exporters Relying on Article 49 GDPR Derogations (Where Data May Be Transferred to the US)

In the absence of appropriate safeguards and in exceptional circumstances, companies may be able to rely, where appropriate, on specific derogations listed in Article 49 of the GDPR to lawfully transfer EEA personal data to third countries, including the U.S. The Article 49 derogations are intended to be used only for specific situations, so they cannot be utilized as a long-term replacement for the SCCs or the Privacy Shield. The EDPB has confirmed that it is still possible to effect such transfers on the basis of the appropriate derogation set out in Article 49 on a fact-specific basis, emphasizing that:

- transfers based on consent should be informed, including in relation to risks resulting from the fact that the data subject's personal data will be transferred to a country that does not provide adequate protection;
- transfers that are necessary for the performance of a contract can only occur where the transfer is "occasional," and the transfer must be objectively necessary for the performance of the contract; and
- transfers that are necessary for reasons of public interest require an important public interest, regardless of the nature of the organization.

The EDPB did not offer any additional guidance on transfers that are necessary for the establishment, exercise or defense of legal claims.

Key Takeaways

The uncertainty caused by the *Schrems II* judgment gives organizations an opportunity to consider the standards upon which their groupwide data protection compliance program has been built.

Organizations should ensure that they carefully document the diligence undertaken for each EEA personal data transfer to which they are party, both internally and externally. This can be done, for instance, by way of a detailed log or a TIA, where necessary, to assess the adequacy of the importing country's law and whether supplementary measures are necessary, describing such measures if they are required.

While *Schrems II* focused on the U.S., data transfers of EEA personal data to third countries in which national surveillance laws allow disproportionate access to personal data potentially may be deemed to not offer protection essentially equivalent to that of EU data protection laws (including the GDPR). Organizations should monitor any further guidance provided by the EU Commission and the EDPB, which hopefully will clarify the types of supplementary measures expected to be implemented to ensure compliance with the level of protection essentially equivalent to that provided under applicable EU data protection laws. Supervisory authorities are now similarly considering the impact of the CJEU ruling and regulatory guidance as it develops on international data flows and what their actions will mean in practice going forward.

We will monitor how the international data transfer regime evolves in the coming weeks as the authorities reflect on the practical consequences of *Schrems II*.

Return to Table of Contents

US Department of Commerce and Federal Trade Commission Will Continue To Administer and Enforce Privacy Shield

Despite the CJEU's decision to invalidate the Privacy Shield, the Department of Commerce and the Federal Trade Commission (FTC) both said they will continue to administer and enforce the framework.

As discussed earlier in this update, the CJEU's decision to invalidate the Privacy Shield framework negotiated between the U.S. and the EU throws into question the ability of companies to export personal data from the EU into the U.S. Nevertheless, the Department of Commerce and the FTC have each announced that they will continue to enforce the Privacy Shield against companies that have signed on to the framework as well as continue to process companies' submissions to do so.

Department of Commerce

On July 16, 2020, Secretary of Commerce Wilbur Ross issued a statement on the CJEU's decision, which explained. in part:

"The Department of Commerce will continue to administer the Privacy Shield program, including processing submissions for self-certification and re-certification to the Privacy Shield Frameworks and maintaining the Privacy Shield List. Today's decision does not relieve participating organizations of their Privacy Shield obligations."[3]

Federal Trade Commission

On July 20, 2020, the FTC — which enforces the Privacy Shield — issued an update on its Privacy Shield webpage, reading in part:

"We continue to expect companies to comply with their ongoing obligations with respect to transfers made under the Privacy Shield Framework. We also encourage companies to continue to follow robust privacy principles, such as those underlying the Privacy Shield Framework, and to review their privacy policies to ensure they describe their privacy practices accurately, including with regard to international data transfers."[4]

Key Takeaways

Even though the Privacy Shield is no longer a valid means for exporting data from the EU to the U.S., it is clear that the U.S. government will continue to both enforce it against companies that have agreed to abide by its requirements and administer the program itself. The statements by the Department of Commerce and the FTC suggest that these government agencies still view the Privacy Shield certification as a commitment that was made to consumers regarding their data privacy practices that cannot be ignored, even in light of the CJEU decision. While there may be little incentive for companies to sign on to the Privacy Shield in the future or complete their annual recertifications, for the time being, companies will be expected to meet their commitments to it.

Return to Table of Contents

Data Colocation Services Company Settles FTC Privacy Shield Claims

A data colocation services company settled claims filed by the FTC related to its participation in the EU-U.S. Privacy Shield.

On June 30, 2020, NTT Global Data Centers Americas, Inc. (NTT), a California-based data colocation services company and successor in interest to RagingWire, settled a complaint filed against RagingWire by the FTC related to the company's participation in the EU-U.S. Privacy Shield framework. Under the settlement, NTT must comply with certain affirmative obligations for as long as it remains a participant of the framework, including by obtaining an annual outside compliance review from an independent assessor regarding its Privacy Shield statements. As mentioned earlier, because the CJEU struck down the Privacy Shield on July 16, 2020, it is unclear whether the NTT settlement will have any practical impact. Nevertheless, the FTC's actions illustrate that the agency continues to take action against companies that misrepresent their privacy practices, including potentially with respect to the Privacy Shield.

Background

To join the Privacy Shield, a U.S.-based organization must annually self-certify with the Department of Commerce and publicly commit to comply with the framework's principles and related data handling standards. The program also requires companies to be transparent about their privacy policies and describe such practices in a public notice. These commitments are enforceable by the FTC under Section 5 of the Federal Trade Commission Act.

From an EU perspective, the Privacy Shield is now no longer a valid mechanism for U.S.-based companies to comply with EU data protection requirements following the CJEU's ruling. Nevertheless, the Department of Commerce has confirmed that it will continue to administer the program, and that participants are not relieved of their obligations under the framework.

The FTC's Allegations

NTT is a data colocation services company that offers specialized storage facilities for servers owned and operated by its customers. RagingWire obtained its Privacy Shield certification in January 2017, but it lapsed in January 2018, the same year NTT acquired the company. However, RagingWire continued to state in its online privacy policy and sales materials that it was compliant with the Privacy Shield. Between January and October 2018, the Department of Commerce issued two separate warnings instructing RagingWire to remove its Privacy Shield claims or take steps to renew its certification. RagingWire failed to remove its Privacy Shield statements until it was contacted by the FTC in October 2018.

In November 2019, the FTC filed a complaint against RagingWire alleging four counts of misrepresentation, including its misrepresentation as a current participant in the Privacy Shield.

[3] The full statement from Secretary Ross is available here.

[4] The full FTC announcement is available here.

The FTC also alleged that RagingWire failed to adhere to certain Privacy Shield requirements while a participant of the program, including annually verifying the accuracy of its statements about its privacy policies; maintaining a dispute resolution process for customers with privacy-related complaints; and affirming to the Department of Commerce that it would continue to apply Privacy Shield protections to personal data collected while participating in the program, or delete or return the data as required. After NTT acquired RagingWire, it was substituted for RagingWire in the case.

The Settlement

Under the FTC's consent order, NTT must meet several requirements over the next 20 years. Going forward, NTT is prohibited from misrepresenting the company's participation in, and compliance with, the Privacy Shield. Most significantly, NTT must obtain an annual outside compliance review from an independent third-party assessor approved by the FTC regarding its Privacy Shield statements. The review is to demonstrate that the company's assertions about its Privacy Shield compliance are true, and that its practices have been implemented in accordance with the framework's principles. Upon request, the company must provide the FTC with a statement signed by the assessor verifying that the review has been completed.

NTT also must continue to meet Privacy Shield obligations and comply with its reporting, notice, record keeping and monitoring requirements. Even if the company withdraws from the program or its certification lapses, NTT must affirm to the Department of Commerce within 30 days that it will continue to apply the Privacy Shield principles to any personal information collected while a participant; protect the information by alternative means under EU law, such as through the use of SCCs;[5] or return or delete the information. The consent order carries the force of law, and each violation may result in a civil penalty of up to $43,280.[6]

FTC Commissioner Rohit Chopra voted against the no-fine, no-fault settlement, arguing that it should be renegotiated because RagingWire had expressly been using the Privacy Shield as a selling point to its customers. The majority of the commissioners, however, voted to accept the proposed settlement, noting that the order is "more protective of the Privacy Shield Principles than the 14 orders this Commission ... has approved in prior Privacy Shield cases," particularly by requiring the company to obtain third-party assessments.

[5] SCCs are non-negotiable contractual clauses drawn up by the European Commission for use in individual data-handling arrangements with the EU.

[6] The order is available here.

Key Takeaways

The FTC's decision demonstrates its commitment to the enforcement of companies' promises under the Privacy Shield, a significant move toward strengthening the regulatory regime surrounding data privacy practices of U.S.-based companies that transfer data from Europe. Although it remains to be seen what, if anything, will replace the Privacy Shield as an alternative compliance mechanism, as mentioned earlier in this mailing the Department of Commerce has said it will continue to enforce the Privacy Shield for the time being. Accordingly, companies should continue to regularly review any consumer-facing materials that reference their privacy practices and check for any lapses in certification to ensure that they do not face liability for misrepresenting their participation in privacy programs to customers.

Return to Table of Contents

Maine Federal Court Rejects First Amendment Challenge to State's Broadband Privacy Law

A federal district court in Maine ruled against a collection of internet service providers (ISPs) in *ACA Connects v. Frey*, rejecting a First Amendment challenge to the state's broadband privacy law, which is considered to be one of the strictest privacy laws in the U.S.

On July 7, 2020, a Maine federal district court rejected an argument from a group of ISPs that the state's new broadband privacy law violated the First Amendment.[7] The law, which requires ISPs to obtain express consent before using, selling, disclosing or permitting access to a consumer's information, is considered the first of its kind in the U.S. and one of the strongest privacy laws in the country.

Background on Maine's Law

On June 6, 2019, Maine enacted a privacy law that limits the ability of ISPs that operate and bill in the state to collect, use, sell, disclose or permit access to "customer personal information."

Such information includes:

- personally identifying information, such as names, Social Security numbers and billing addresses; and

[7] *ACA Connects v. Frey*, No. 1:20-cv-00055-LEW, 2020 WL 3799767 (D. Me. July 7, 2020).

- information gleaned from a customer's internet usage, such as browsing history, precise geolocation and financial information.

Under the law, ISPs cannot engage in these practices unless the customer has explicitly consented to them, or the ISP is engaging in such practices pursuant to a lawful court order or in connection with presenting existing customers with advertisements of communications-related services to existing customers. The law only applies to companies that offer broadband access, exempting "edge" providers, such as social media sites, from the law's requirements. The legislation also prevents ISPs from refusing service, charging penalties or withholding discounts from customers who do not offer their consent.

The law went into effect on July 1, 2020, with supporters applauding its protections of consumers' privacy and data against ISPs, which can see and track all of their users' web traffic.

The ISPs' Argument and the Court's Decision

In February 2020, the ISPs sought an invalidation of the law on First Amendment grounds, among other claims, arguing that free speech is necessary for an open internet and that the Maine law had violated their First Amendment right to free speech. The ISPs argued that their First Amendment rights include their right to send and target noncommunications-related advertising to consumers as well as to offer price discounts or other loyalty programs in exchange for a customer's consent.

The ISPs argued the law is both speaker- and content-based, and as such, strict scrutiny should apply. Under the heightened standard, the government had to show a "substantial interest" in regulating the specific aspect of privacy at issue and demonstrate that the law is not more extensive than necessary to serve that interest.

In *ACA Connects*, the federal district court rejected the ISPs' First Amendment claim, calling it a "shoot-the-moon argument." Rejecting the ISPs' argument that the strict scrutiny standard should apply, the court applied the less burdensome intermediate scrutiny standard, which under existing First Amendment precedent applies to commercial speech.[8] Precedent in cases such as *Rocket Learning, Inc. v. Rivera-Sanchez* has defined commercial speech as "expression related solely to the economic interests of the speaker and its audience."

Intermediate scrutiny required the government to show (1) that it had a "substantial interest" that it sought to achieve through the law, and that the law "directly advances" that interest and (2) the regulation is "narrowly drawn" to that interest.

- **Prong 1:** To show a "substantial interest," the state of Maine had to show both real harm and that its restrictions will materially mitigate that harm.
- **Prong 2:** To show a "narrowly drawn" interest, the state of Maine had to establish that the regulation reasonably advanced its goal of protecting consumer privacy. The government did not have to show that the statute is the "least restrictive means" or that there is no other alternative.

As the ISPs asked for a motion for judgment on the pleadings, the court made all inferences in favor of the state, holding that there was not enough information to show either that (1) Maine had an unsubstantial interest in enacting the law, or (2) the law overshot the mark on such an interest. On that basis, the court rejected the ISPs' First Amendment claims and upheld the Maine law.

Key Takeaways

State legislatures across the U.S. have been leading the effort to protect consumer information online. The *ACA Connects* case suggests that a First Amendment challenge to a privacy law is unlikely to sway a court, and that a heightened standard of scrutiny likely will not apply. As technology continues to entrench itself in daily life, companies that collect, use and access users' data should be mindful of state efforts in this area.

Return to Table of Contents

Federal Court Finds Potential Negligence Liability for Damages Caused by Hackers

A federal court in Ohio recently held that third-party criminal conduct does not absolve a company of potential negligence liability stemming from a data breach.

On July 1, 2020, a U.S. District Court for the Northern District of Ohio held that Sonic Corp. (Sonic) could be held liable for negligence because of its failure to foresee and prevent a data breach and the resulting harm to customers and financial institutions.[9] The case was filed by a group of financial institutions seeking recovery of losses stemming from a 2017 data breach suffered by Sonic.

[8] *Central Hudson Gas & Elec. Corp. v. Public Serv. Comm'n of New York*, 447 U.S. 557 (1980). A copy of the decision is available here.

[9] A copy of the decision can be found here.

Background[10]

Sonic oversees a chain of approximately 3,500 Sonic Drive-In restaurants across 45 states, though the company itself only owns about 6% of these locations and the rest are franchises. However, Sonic controls the data security policies and security settings implemented at all of its restaurants, and either Sonic or its approved vendors install all of the technology used in the restaurants. As part of its franchisee agreements, Sonic requires full remote access to be enabled for all point-of-sale systems (cash registers), which allows the company to access the technology at all locations.

According to the plaintiffs, in 2015, Sonic experienced a security breach. The company hired a third-party security entity to investigate and, though the damage caused by this breach was limited, the security company told Sonic that the franchise's systems were now more vulnerable to potential attacks. The plaintiffs claim that Sonic did not address the identified vulnerabilities.

The plaintiffs alleged that, in 2017, unidentified hackers installed malware in Sonic's cash registers and servers. The technology in use at some locations at the time was antiquated and did not support encryption of customer data. Hackers were able to access customers' data and obtain customer credit card information, which they then sold on the dark web. Sonic had a system set up to receive alerts of security issues, but it had been configured with an invalid email address, so the company did not immediately detect the malware.

Six months after the attack, a credit card processor notified Sonic of suspicious activity on customers' accounts, and Sonic began an internal investigation. Once it confirmed the breach, Sonic notified the federal authorities and the public, and offered customers two years of free fraud detection and prevention. In October 2018, Sonic reached a $4.3 million settlement with its customers in a multidistrict litigation suit.

Financial Institution Claims Against Sonic

Payment card-issuing credit unions and banks brought a negligence claim against Sonic, seeking to recover their losses from the 2017 breach, including financial loss from having to reissue cards, close accounts, block transactions, increase fraud monitoring and refund affected customers. Sonic filed a motion to dismiss the plaintiffs' negligence claim, arguing that it had breached no duty to these institutions because there was no obligation for it to predict or prevent the criminal conduct of third parties. The financial institutions argued that Sonic, through its delayed implementation of new technology and misconfiguration of its security systems, affirmatively created vulnerabilities that hackers then exploited, and that the company should have been aware of this risk.

District Court's Decision

Since it was deciding on a motion to dismiss, the court took all of the financial institutions' factual allegations at face value and ruled solely based on whether, if all of the allegations were true, Sonic could be found negligent under Oklahoma law. Although Oklahoma law generally does not impose negligence liability for the criminal acts of a third party, there is an established exception when the defendant's own affirmative act created or exposed the plaintiff to a "recognizable high degree of risk of harm."

In this case, the court agreed with the financial institutions, concluding that based on the facts they presented, a reasonable person would have foreseen both the data breach risk and its effects on the plaintiffs. Although criminal acts are not generally foreseeable, the court concluded that in this case Sonic did have reason to anticipate the hack, since the company controlled all of the franchises' technological systems and policies, had been hacked two years prior and had been advised that its systems were vulnerable. Finally, by using outdated technology and misconfiguring its security alert system, the court concluded that Sonic exposed franchises to increased risk.

The court also rejected Sonic's argument that the so-called "economic loss doctrine" did not permit the application of tort law negligence to a purely commercial dispute. Under Oklahoma law, "[w]hen a party's loss is purely economic and does not entail personal or property damage, such losses have traditionally not been protected by application of tort law." In rejecting this argument, the court noted that Oklahoma has not applied the economic loss doctrine outside of products liability cases, and declined to do so in this case. This approach is different from that in many other states, which would arguably have applied the doctrine to bar a negligence claim in this instance.

Key Takeaways

Although tort law generally does not impose a legal responsibility to predict the results of third-party criminal acts, this case illustrates that a breached company might be responsible for the resulting damage if it exercises control over its cybersecurity systems and does not take reasonable precautions to prevent a breach. In finding that Sonic should have foreseen this security breach, the court focused on the company's failure to take action after its first breach in 2015 as well as the number of high-profile data breaches suffered by other companies that had occurred in the

[10] This recitation of facts is based solely on the plaintiff financial institutions' allegations.

intervening years. Companies should continue to closely monitor their own cybersecurity policies and systems and keep an eye on the vulnerabilities exposed by other companies' data breaches.

Return to Table of Contents

The P2B Regulation: EU Adopts First Regulation of Online Business Platforms

The EU has adopted a new regulation addressing the conduct of online business platforms and their relationships with the businesses that use them, imposing a number of requirements on providers of platform services.

Introduction

The EU's Platform to Business Regulation (P2B Regulation) went into effect on July 12, 2020, regulating online business platforms by promoting fairness and transparency for business users of online intermediation services (OISs).[11] The regulation is Europe's first-ever legislation that aims to regulate the contractual relationship between operators of online platforms and those businesses across the EU that rely on such platforms to reach their consumers.

The P2B Regulation, which is directly applicable in all EU member states, is premised upon creating a fair and transparent environment for businesses and consumers alike when using OISs and online search engines, both of which have seen ever-increasing popularity since their inception, leading many to view them as "gatekeepers" of access to consumers in the modern world. With direct effect at the national level, the EU has taken an interventionist approach in its implementation of the P2B Regulation in hopes of protecting businesses that rely on online platforms to reach their customers.

The regulation is the EU's attempt to implement a harmonized framework that includes minimum transparency obligations and redress rights for business users while protecting businesses depending on online platforms and preserving the innovative potential of such platforms. The rules and obligations set forth in the P2B Regulation apply to online marketplaces, application distribution platforms and price comparison websites, as well as online general search engines.

Scope and Definition of OIS

The P2B Regulation applies to online search engines or operators of OISs (1) provided that the business users with whom they contract are established in the EU and provide their goods or services to consumers who are located in the EU, and (2) is applicable regardless of whether they themselves are established in the EU or not, as well as regardless of any law that may otherwise govern the contract between the operator of the OIS and the business.

The P2B Regulation defines an OIS as consisting of information society services (such as online marketplaces, social media services and software application services), which are characterized by the fact that they "aim to facilitate the initiating of direct transactions between business users and consumers, irrespective of whether the transactions are ultimately concluded." As a result, for operators of OISs to be subject to the P2B Regulation, there is no requirement that there actually be any contractual relationship between the business using the online platform and their consumers; all that is required is that the OIS aims to facilitate the transaction between businesses and consumers (*i.e.*, provides a platform for businesses).

Key Obligations Under the P2B Regulation

The P2B Regulation places a multitude of obligations on operators of OISs and their interactions with business users. These requirements are intended to level the playing field between operators of OISs and businesses looking to use such services to reach out to consumers. The obligations also aim to address the unequal bargaining power between the two by providing the business users with a set of minimum rights and a clear framework through which they can engage operators of OISs. The key obligations under the P2B Regulation are as follows:

- Terms and Conditions (T&Cs). The P2B Regulation mandates the general terms and conditions that operators of OISs must meet, including:
  - **Accessibility.** The P2B Regulation requires that T&Cs be clearly and plainly drafted and should be readily and easily available to business users;
  - **Amendments.** Business users must be provided with at least 15 days' notice of any changes to their T&Cs. The P2B Regulation further states that where the changes necessitate that the business user make technical adaptations, the notice period should be longer. In the event a business user doesn't agree to the amendments, the P2B Regulation affords business users the right to terminate the contract;
  - **Suspension, Restriction and Termination.** T&Cs should make clear the objective reasons the operator of the OIS may suspend, terminate or restrict access to their service;

[11] A copy of the P2B Regulation can be found here.

- The P2B Regulation stipulates that in the event of a restriction or suspension, operators of OISs must, prior to or at the time of the suspension or restriction, provide business users with a clear statement of the reasons for, and specific circumstances that led to, that decision. Where business users have their rights to use the OIS terminated, this statement must be provided at least 30 days before the termination is to become effective.

- **Mediation.** The T&Cs must set out the details of at least two mediators selected by the operators of the OIS for dispute resolution purposes. The P2B Regulation requires that the operators engage in good faith mediation attempts where required and take on a reasonable portion (determined on a case-by-case basis) of the cost of mediation. However, this rule does not apply to OIS providers that are deemed to be a "small enterprise" (*i.e.*, have fewer than 50 employees and an annual balance sheet total of less than €10 million); and
- **Rankings.** In an effort to promote algorithmic transparency, the P2B Regulation requires T&Cs to set out the parameters that are used for rankings of the businesses on online platforms. Where rankings may be prejudiced by remunerating the operators of the OIS, T&Cs must set out a description of how rankings are affected by remuneration.

Noncompliance With the P2B Regulation

Where operators of an OIS fail to incorporate the requirements set out above as part of their T&Cs, those provisions being relied on by the operator of the OIS (but not the T&Cs in their entirety) will be considered null and void and not enforceable against business users. By rendering any noncompliant terms null and void, the P2B Regulation aims to not only protect business users but also provide both sides with a transparent and clear regulatory framework within which they can conduct their business.

Application Outside the EU and Brexit

The P2B Regulation applies to any operator of an OIS that is providing services to business users and consumers based in the EU, regardless of whether the OIS or its operator is within the EU. Accordingly, the EU could seek to apply it to U.S.-based OIS and — post-Brexit — U.K.-based OISs as well.

Key Takeaways

The P2B Regulation imposes numerous obligations on providers of platform services. By regulating the contractual relationship that operators of OISs have with their business users, such business users are now afforded minimum contractual protections when interacting with platform providers. This follows the trend of wider consumer protection legislation in the EU, which has developed over the past decade to protect consumers (*e.g.*, through the implementation of implied terms and obligations on businesses to act fairly) against the lack of bargaining power between businesses and consumers. OIS operators should, as soon as possible, review their T&Cs with business users; practices regarding suspension, restriction and termination of services; compliance procedures and use of mediators; and transparency surrounding their ranking mechanisms for compliance with the P2B Regulation.

For business users that utilize online platforms to reach consumers, the P2B Regulation will be welcomed, as it provides a transparent regulatory framework in which they can conduct their business. Business users are now afforded further clarity and fairness in T&Cs governing their relationship with operators of OISs as well as a more effective complaint-handling process. Businesses should await revised T&Cs from the operators of OISs that they engage to reach their consumers, including their new rights as set out under the P2B Regulation.

Return to Table of Contents

New York Files First Cybersecurity Enforcement Action Against Major Title Insurance Company

The New York State Department of Financial Services (DFS) has filed its first charges against a financial institution for violating its cybersecurity regulation, signaling the need for covered entities to be mindful of their cybersecurity obligations.

On July 22, 2020, the DFS brought its first action under its groundbreaking cybersecurity regulations, delivering on the regulator's promise to prioritize enforcement. The DFS alleges that First American Title Insurance Company, the second-largest real estate title insurer in the U.S., exposed the personal and financial information of millions of consumers due to a website vulnerability that First American had known about from a routine penetration test required under the DFS cybersecurity regulations.[12] The vulnerability, which allegedly went undetected for years, created a flaw in the company's web-based document delivery system, enabling anyone to view up to 850 million documents, including many that contained sensitive nonpublic information, without needing a password.

This action comes about a year after the DFS established its Cybersecurity Division, which the agency described as the "first of its kind at a banking or insurance regulator," and appointed a

[12] The statement of charges and notice of hearing is available here.

former cybercrime prosecutor to serve as its leader. Against that backdrop, covered DFS-regulated banks, insurance companies and other financial institutions should expect future enforcement.

The Cybersecurity Regulations

New York's cybersecurity regulations, the first of their kind at the state level, require covered entities to establish and maintain cybersecurity programs designed to protect consumers and the financial services industry from the threat of cyberattacks. Announced in 2017, the regime's various provisions were phased into effect over the course of two years, with all requirements becoming fully effective by March 2019. Key requirements include:

- written cybersecurity policies and procedures to protect information systems and the nonpublic information on those systems, including information systems and nonpublic information accessible to, or held by, third-party service providers;
- a written cybersecurity event response plan, including a 72-hour notification requirement;
- periodic risk assessments, an annual penetration test and a biannual vulnerability assessment;
- data retention policies and controls, including encryption, to protect nonpublic information, including for information held by third-party service providers;
- regular cybersecurity awareness training for all personnel;
- submission of the chief information security officer's report on the company's cybersecurity program to the board (or a senior officer); and
- an annual written statement to the DFS certifying that the entity is in compliance with the cybersecurity regulations.

Analysis

As these regulations have come into force, the DFS warned that failure to comply with the requirements may lead to enforcement, a threat the regulator followed through on with its statement of action against First American. The details from that statement provide insights into both the priorities and expectations of the DFS and the manner in which other regulators may interpret similar data security laws that have been adopted by states across the U.S. Organizations should consider the following in light of the First American case:

Remediate Identified Vulnerabilities Promptly: The DFS' action highlights how the mandate to conduct periodic penetration testing and vulnerability assessments can expose covered entities to enforcement risk. These tests are standard in most sectors and routinely uncover vulnerabilities, even at organizations with robust security programs. Most organizations have a policy for remediating the identified vulnerabilities within a time frame in accordance with their severity. These remediation processes will now take on heightened significance after the DFS codified these best practices into a regulatory mandate, as the First American action reveals.

The DFS complaint alleges that First American identified the vulnerability at issue pursuant to a mandated penetration test but underestimated the risk it posed, leading the company to conclude that it had 90 days to remediate under its policies. The DFS also criticized the company for assigning "a new employee with little experience in data security" to remediate the vulnerability and for reviewing only 10 out of the potentially hundreds of millions of documents exposed, which the DFS characterized as "unacceptably minimal." In-house cybersecurity experts at the company also advised further review of the vulnerability, the DFS claims, but nothing came of that recommendation. Finally, the DFS detailed the company's noncompliance with its own remediation policies, including its failure to remediate within 90 days and appropriately follow up on the risk assessment.

These allegations underscore the need for companies to remediate vulnerabilities identified during penetration tests and vulnerability assessments in a timely manner with capable personnel, and to document those efforts in contemporaneous records. A failure to follow through on those processes may be judged harshly by an enforcement agency.

Perform and Document Risk Assessments: The state's cybersecurity regulations require a periodic risk assessment of information systems, and the statement of action reveals that the DFS may scrutinize the scope and depth of those assessments, including which particular systems were reviewed. In its statement, the DFS highlighted the lack of a documented risk assessment of the document delivery system at issue as a key failure for First American, in addition to its failure to identify that the system contained nonpublic information, and to identify the availability and effectiveness of controls to protect that information. Thus, covered entities should consider taking proactive measures to identify each information system involving nonpublic information, and perform and document appropriate risk assessments.

Provide Cybersecurity Awareness Training for Key Personnel: A regulatory inquiry from the DFS following an incident may include questions about cybersecurity awareness training, which is required by the regulations. The DFS deemed First American's training to be inadequate because the company allegedly delegated the effort to individual business units to design training "at their own discretion" without any centralization or coordination. That failure, the DFS asserts, was compounded by the fact that the company's sole control to prevent the storage and

transmission of sensitive information on the document delivery system was an employee policy against doing so. In view of these allegations, covered entities should coordinate and vet their cybersecurity training programs while also paying special attention to employees who handle and control access to sensitive information.

Beware of Potential Penalties, Even Without Alleged Harm to Consumers: Although the cybersecurity regulations do not provide for penalties, they empower the DFS to pursue enforcement "under any applicable laws." In announcing the action against First American, the DFS invoked Section 408 of the New York Financial Services Law and claimed penalties of up to $1,000 for "each instance of nonpublic information encompassed within the charges," a potentially substantial liability for an incident that may involve hundreds of millions of consumer records.[13] Notably absent from the DFS' statement was an allegation of direct consumer harm arising from the exposure — a key detail that often influences the amount of financial exposure a company faces in the wake of an incident. Given that data breaches routinely involve the exposure of millions of records, the DFS' position on enforcement raises the specter of staggering penalties even without identifiable harm to consumers.

Key Takeaways

Although it remains unclear how frequently the DFS will resort to enforcement actions, the case against First American provides important clues. Covered entities that suffer an incident should expect their policies, procedures and practices to come under close scrutiny. The risk of significant financial penalties provides even more reason for covered entities to reassess their compliance with the cybersecurity regulations before an attack strikes.

Return to Table of Contents

European Commission Issues Report on Past Two Years of the GDPR

The European Commission has released its report on the last two years of the GDPR, noting how the privacy law has been implemented and enforced, and recommending areas in which further action should be taken.

On June 24, 2020, the European Commission published its report on the application and functioning of the GDPR, as required under Article 97 of the regulation.[14] The report takes into consideration contributions from the European Council, the European Parliament, the EDPB and national supervisory authorities. In particular, Article 97(2) requires the report to examine international data transfers as well as cooperation and consistency mechanisms. In this case, the report covered a broader range of topics and identified a number of areas where the regulation could improve. Below, we summarize the main findings of the report, the most significant follow-up actions that the commission has set for itself and others, and our key takeaways.

Report Summary

Generally, the commission believes that the GDPR has successfully strengthened the protection of individuals' personal data and guaranteed the free flow of personal data within the EEA. The report goes into more detailed analysis of where the regulation has succeeded and areas where it could be more impactful.

Enforcement

Supervisory authorities have been "balanced" in their approach to enforcement action, according to the report, with a range of corrective measures being used. Cooperation and consistency among supervisory authorities is emerging, but they have not yet made full use of the tools that are available to them by the GDPR (*e.g.*, prohibitions on processing). The report also notes that while many supervisory authorities have markedly increased their resources since 2016, many would benefit from additional staff, particularly in those countries where large, multinational technology organizations reside.

Fragmentation

The report states that because the GDPR requires EEA jurisdictions to legislate in some areas (*e.g.*, in relation to the age of children's consent), the regulation creates a degree of fragmentation. The commission is monitoring these divergent approaches and encourages the development of codes of conduct under Article 40 of the GDPR to ensure greater consistency. Creating common standards by which the adherents to the codes of conduct would abide would facilitate cross-border processing of personal data. The commission cites the supervisory authorities' processing operations as an example of the need to carry out a Data Protection Impact Assessment (DPIA) as an example of an opportunity to improve further harmonization. In light of the CJEU's judgment in Schrems II, and the subsequent diverging reactions from supervisory authorities, the extent to which supervisory authorities' approaches will take heed of the commission's desire to avoid fragmentation remains to be seen.

[13] DFS Press Release, July 22, 2020, outlining the charges is available here.

[14] The full report is available here.

Data Subject Rights

The report notes that the GDPR has helped people become increasingly aware of their data protection rights. The commission is of the opinion that the right to data portability, which allows individuals to move their personal data from one service provider to another, has been underutilized, yet has the potential to put individuals at the heart of the data economy by allowing them to easily switch service providers. While individuals are increasingly aware of their data protection rights and are making further use of them, the commission identifies a need to facilitate the exercise and enforcement of these rights. To this end, the commission welcomes Directive COD/2018/0089 on representative actions, which sets out a framework for collective actions brought by consumers in areas such as data protection, and which will lower the costs of cross-border actions. The final text of the directive was agreed upon on June 22, 2020, and member states have two years from that date to implement it.

New Technology

The GDPR is technology neutral, so it can cover new technologies as they emerge and become more commonplace, such as facial recognition technology. However, the report notes that the GDPR faces challenges in figuring out how to apply its principles to technologies such as artificial intelligence and blockchain. Interestingly, the commission specifically mentions the need for strong enforcement against large digital platforms, particularly in online advertising and micro-targeting, in order to protect individuals.

International Data Transfers

The report mentions the EU-Japan mutual adequacy decision of January 23, 2019, and the progress made in the same field with South Korea. The commission also is currently carrying out an adequacy assessment of the U.K. ahead of the end of the Brexit transition period. The report was released a few weeks before the *Schrems II* judgment, so it does not account for the impact of the CJEU's ruling on international data transfers. However, the report notes that the commission is working on modernizing the SCCs to account for the GDPR.

Under Article 97 of the GDPR, the commission's next report is due by May 25, 2024.

Key Takeaways

Based on the report, it is clear that:

- the commission would like to see greater use of the variety of enforcement tools available under the GDPR, such as prohibitions on processing. The report notes that this could have a greater deterrent effect than other enforcement tools and has the potential to be very disruptive to businesses;
- the commission encourages the EDPB to ensure effective enforcement against organizations based in third countries that fall within the GDPR's territorial scope. We note that, to date, no international cooperation mechanisms have been developed under Article 50 of the GDPR in order to facilitate the effective enforcement of the GDPR;
- the commission is monitoring areas in which the GDPR allows for fragmentation and is encouraging greater cooperation and consistency to limit such fragmentation (*e.g.*, in relation to the age of children's consent). For such harmonization to take place, EEA jurisdictions may need to refresh their existing compliance programs;
- organizations working with new technologies that involve the processing of personal data should ensure that their processing is compliant with the GDPR, including by conducting DPIAs where necessary and maintaining compliance records in relation thereto;
- the commission is working on finalizing updated versions of the SCCs in line with GDPR requirements. In light of *Schrems II*, SCCs will likely be the predominant data transfer mechanism for transferring personal data out of the EEA. Organizations should keep abreast of the latest developments to ensure that they implement the latest version of the SCCs; and
- the commission has called on EEA jurisdictions to provide supervisory authorities with adequate funding, which will be necessary to support the exercise of supervisory authorities' broader powers, including in relation to the increased monitoring of data transfers following *Schrems II*.

Return to Table of Contents

New UN Regulation Mandates Automotive Cybersecurity Measures

The United Nations adopted a new regulation obliging car manufacturers to comply with an array of cybersecurity measures for their "smart" cars. New responsibilities include approval, reporting and mitigation measures.

On June 23, 2020, the United Nations adopted a new regulation mandating that "smart" car models — which include an ability to connect to external networks — be built with certain cybersecurity protections in place.[15] Companies will now need to implement forensic technology to identify attempted attacks, inform authorities about the effectiveness of their measures and

[15] Full text of the document is available here.

report other relevant information. Similarly, car manufacturers will need to ensure that suppliers are compliant with the new cybersecurity rules or potentially face sanctions.

To date, only 53 countries have adopted the regulation, but these include countries that are home to major international automakers, including Japan and South Korea, and nations within the EU. Each jurisdiction plans to implement the regulation's requirements at different points in time, with the EU aiming for 2022, South Korea for 2021 and Japan for this year. The U.S. did not adopt the regulation, but U.S. companies will need to abide by the new rules if selling smart cars in markets that have adopted them.

Greater Risks of Attack

Smart car models have dominated the global car market over the last several years, and the global smart car market is projected to reach a valuation of $219.2 billion by 2025, with a variety of major automakers having launched successful intelligent services into their vehicles. This advanced technology is being used to create personalized content and experiences for drivers, as the cars generate mass amounts of data that is sent to automakers and partner companies. However, as cars have become more advanced and capable of tracking greater amounts of personal data, concerns have grown over the possibility of vehicle cyberattacks and data breaches.

Prior to the regulation, there had not been any general standards for automotive cybersecurity; other worldwide initiatives have failed to advance past the drafting stage. However, cybersecurity awareness in the industry has grown through frameworks that describe industry best practices, such as the Alliance of Automobile Manufacturers' Framework for Automotive Cybersecurity Best Practices and the European Union Agency for Cybersecurity's Good Practices for Security of Smart Cars.

Regulation Requirements

For each type of smart vehicle a manufacturer wishes to sell, a designated approval authority must grant a "type approval" verifying that the manufacturer has satisfied the requirements of the regulation. To obtain approval, automakers must demonstrate compliance with an array of requirements:

- **Certificate of Compliance:** National authorities will need to conduct an assessment of a manufacturer's cybersecurity management system before granting the requisite approval.
- **Reporting Provisions:** Vehicle manufacturers will need to report, at least annually, the results of their monitoring activities, as well as any relevant new information on cyberattacks and the effectiveness of their cybersecurity mitigations.
- **Threats and Mitigations:** The regulation considers a number of potential vulnerabilities in smart cars and provides suggested protections. Generally, the regulation names information breaches, unauthorized access, corrupted applications, manipulation of vehicle data and malicious software as examples of potential risks. Recommended mitigations include access and security control techniques, authenticity verifications and detection measures.

Key Takeaways

The regulation will likely have a lasting effect on the global auto industry and cybersecurity spending. Even though the U.S. did not adopt the regulation, U.S. automakers selling within the EU or large parts of Asia will have to comply with its requirements. While smart technology in cars have myriad advantages, including providing added safety, it is no surprise regulators are finding it increasingly important to ensure the technology is not vulnerable. Overall, the regulation is an important step in overseeing the expansion of this technology before it outpaces legislative efforts.

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