FCPA Update

A Global Anti-Corruption Newsletter

Also in this issue:

Click here for an index of all *FCPA Update* articles

If there are additional individuals within your organization who would like to receive *FCPA Update*, please email ssmichaels@debevoise.com or pferenz@debevoise.com

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Table of Contents

I. Introduction

The Court of Justice (the "CJEU") of the European Union (the "EU") has, in a landmark judgment handed down on October 6, 2015 (the "Judgment"),[1] invalidated the European Commission decision (the "Commission Decision") on the Safe Harbor Privacy Principles (the "Safe Harbor Principles" or "Safe Harbor").[2] This article discusses the practical consequences, which may be summarized as follows.

- Companies that have been relying on the Safe Harbor to transfer data from the EU to the United States may no longer rely on it. It is possible that

Continued on page 2

1. Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, 2015 E.C.R. ---, http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en. *See also* Debevoise & Plimpton, Client Update, "Transfers of Personal Data to the United States: European Court of Justice Rules the Safe Harbour Protocol Is Potentially Invalid" (Oct. 6, 2015).
2. Commission Decision 2000/520, 2000 O.J. (L 215) 7 (EC), pursuant to Directive 95/46 on the adequacy of the protection provided by the Safe Harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce.

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 1

EU data, however, may be considered lawfully transferred by using methods that, in substance, conform with the requirements of the Safe Harbor, subject to review by the relevant EU Member State Data Protection Authority (or, where it is allowed, the data exporter) for adequacy.

- Companies transferring data should review their data transfer arrangements in view of the official guidance that has been issued, and with an eye to further guidance to come. If necessary, they should either work out solutions based on standard contractual provisions promulgated by the European Commission or pre-approved agreements within a corporate group, or determine if one of a number of other exceptions to the restrictions on data transfer apply. The most relevant exceptions are based on contract performance, legal claims, advice and defenses, and consent. Because some official bodies of the EU have called into question the continuing legal viability of the standard contractual provisions and the agreements within a corporate group, companies should consider carefully whether any exceptions are available.
- To the extent possible in light of business operations, companies may wish to consider retaining personal data in the EU and delaying any transatlantic transfers until they are able to implement lawful solutions.
- The governmental bodies of the EU and United States are working to reach a solution that will facilitate the continued transatlantic flow of personal data. All those transferring or intending to transfer personal data should stay tuned for further developments.

II. Background

Until the Judgment, the Safe Harbor Principles were one of the routes that permitted, under certain conditions, the transfer of personal data from the EU to organizations in the United States that self-certified their adherence to the Safe Harbor to the U.S. Department of Commerce.

Under EU law, "personal data" is defined as any data that relate to a living individual. This definition captures a broad array of information pertaining to personal identity, including names, phone numbers, email addresses, bank accounts, and similar information.

EU law requires adherence to certain protocols when personal data are transferred from the EU to so-called "third countries" ("Third Countries") including the United States. For some businesses, depending on the amount, type, and use of data being transferred, compliance with these protocols has consumed business resources. For compliance professionals at multinational enterprises,

Continued on page 3

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 2

such compliance may have posed challenges because it slows the pace of managing corporate enterprises and needs to be considered in the course of third-party and employee due diligence, internal investigations, responses to whistleblowing, and an array of other compliance related communications.

The Safe Harbor Principles were agreed to by the U.S. Department of Commerce and the European Commission (the "Commission") as a means of providing certainty to companies seeking to transfer EU-originating personal data to the United States.[3] They came into effect as a Commission Decision in November 2000, and had, until now, been relied upon by approximately 4,000 registrants, including those operating transatlantic business units connected through real-time data systems. The Judgment invalidated the Decision.

"The impact of this central jurisdictional holding is that the Commission (until challenged), the various DPAs in the EEA, as well as the CJEU, can all shape the regulatory regime governing transfers of personal data from the EU to the United States. So, too, can the domestic courts of the EU Member States[.] The multitude of players increases the uncertainty for companies whose businesses require transatlantic data flows."

In one of the core aspects of its ruling, the CJEU concluded that the Commission does not have the authority to restrict the power of the independent data protection supervisory authorities (the "DPAs") in each of the 28 EU Member States (the "Member States") to challenge the validity of Commission decisions authorizing data transfers to countries outside the European Economic Area (the "EEA").[4] Those countries outside of the EEA, including the United States, are referred to under EU data protection law as Third Countries.

The impact of this central jurisdictional holding is that the Commission (until challenged), the various DPAs in the EEA, as well as the CJEU, can all shape the regulatory regime governing transfers of personal data from the EU to the United States. So, too, can the domestic courts of the EU Member States when reviewing the DPAs' interpretation of EU law or deciding data protection issues in civil or criminal proceedings. The multitude of players increases the uncertainty for companies whose businesses require transatlantic data flows.

Continued on page 4

3. The Commission is the EU executive body.

4. The European Economic Area (the "EEA") consists of the 28 EU member states and, by way of the EEA agreement that also binds to the Directive, of Iceland, Liechtenstein, and Norway.

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 3

III. The Context of the Judgment

Both the Charter of Fundamental Rights of the European Union (the "Charter")[5] and the EU Data Protection Directive (the "Directive"),[6] which has been implemented by all of the Member States in their domestic laws, provide for the protection of the personal data of an individual in the EU. The Directive sets forth restrictions on how that data may be processed. As noted above, the definition of personal data has a broad scope, encompassing any information relating to an identified or identifiable natural person.[7] Any use of personal data, including a transfer to a Third Country, is defined as "processing."[8] A transfer of personal data outside the EEA is prohibited, unless (i) the Third Country ensures an adequate level of protection[9] or (ii) an exception[10] applies.

In applying the Directive and decisions based on the Directive, the CJEU and all other authorities applying data protection law are mandated by the Charter to take into account the fundamental rights to respect for private and family life[11] as well as the right for an individual to have an effective remedy in response to a breach of those rights.[12]

The Directive authorizes both the Commission (as, the Judgment held, subject to review by the CJEU) and the Member State DPAs to assess the adequacy of the protection afforded by the relevant Third Country in the light of all the circumstances surrounding data transfers.[13] The Commission may determine that a Third Country ensures an adequate level of protection by reason of (i) the Third Country's domestic law or (ii) the international commitments the Third Country has made. Such an assessment is binding upon Member States

Continued on page 5

5. Charter of fundamental rights of the European Union, Oct. 26, 2012, 2012 O.J. (C 326) [hereinafter, "Charter"].
6. Council Directive 95/46, 1995 O.J. (L 281) 31 [hereinafter, "Directive"] (regarding the protection of individuals with regard to the processing of personal data and on the free movement of such data).
7. *See id.* art 2(a) ("'[P]ersonal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.").
8. *See id.* art 2(b) ("'[P]rocessing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.").
9. *Id.* art. 25.
10. *Id.* art. 26.
11. Charter, art. 7.
12. *Id.* art. 47.
13. Article 25 paragraph 2 of the Directive requires giving particular consideration to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the Third Country in question and the professional rules and security measures which are complied with in that country. Directive, art. 25 ¶ 2.

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 4

unless successfully challenged before the CJEU. Member State DPAs have similar authority within their own nations to interpret the criteria set forth in the Directive.

The Commission has made such a determination as to the adequacy of privacy protection in respect of a number of Third Countries.[14] With respect to the United States, the Commission did not find that the country as a whole afforded an adequate level of protection; rather, the Commission Decision found that an adequate level of protection for the transfer of data would be attained only if U.S. data importers – and only those subject to the jurisdiction of the Federal Trade Commission or Department of Transportation – complied with the Safe Harbor Principles, as follows:

(i) organizations must notify individuals about the purposes for which they collect and use information about them;

(ii) individuals must be given the opportunity to choose (that is, to opt out as to) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized;

(iii) organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration, and destruction;

(iv) individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate; and

(v) individuals must have access to a mechanism for redressing disputes against organizations that violate the Safe Harbor Principles.[15]

Enterprises wishing to take advantage of the Safe Harbor with respect to their transfers of EU personal data to the United States were required to self-certify their adherence to the Safe Harbor Principles.

The Safe Harbor Principles themselves recognize that complying with them does not relieve an adherent from also having to comply with U.S. national security, public interest, or law enforcement requirements.[16]

Continued on page 6

14. Andorra, Argentina, Canada (commercial organizations only), Faeroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay. *See* Commission homepage, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (Oct. 26, 2015).

15. For additional information about the substance of the Safe Harbor protocols, see U.S.-EU Safe Harbor List, https://safeharbor.export.gov/list.aspx (last visited Nov. 10, 2015).

16. Commission Decision 2000/518, Annex I, 2000 O.J. (215) (EC).

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 5

As noted above, a transfer of personal data can be made to a Third Country, even if its protection is not adequate, if the transfer falls within an exception. The exceptions fall within two sets.

The first set involves the so-called "derogations." Most significantly, these include the data subject's unambiguous consent or the necessity of the transfer for the establishment, exercise, or defense of legal claims.[17]

The second set encompasses the situation in which the data controller adopts "adequate safeguards." The data controller is the person who determines the purposes and means of the processing of personal data.[18] The Directive does not define the term "adequate safeguards," but refers, as an example of such safeguards, to "appropriate contractual clauses" purporting to protect the data in the Third Country.[19] As a consequence, Commission-issued standard contractual clauses (the "Standard Contractual Clauses")[20] and DPA-approved Binding Corporate Rules ("BCRs") are considered to be adequate safeguards.[21]

The independent national DPAs are each vested with the power to investigate data flows to Third Countries and impose a temporary or permanent ban on such transfers. The Commission Decision identified the circumstances under which a DPA could suspend a transfer made or to be made pursuant to the Safe Harbor Principles. Where an EU data subject's data protection rights are infringed, the DPA may also impose monetary sanctions on the infringing data controller and data processor.[22]

Finally, EU law provides that every person has a right to a judicial remedy for any breach of his or her data protection rights and is entitled to claim compensation for any damage suffered.[23]

Continued on page 7

17. Directive, art. 26 ¶ 1.
18. *Id.* art. 26 ¶¶ 2-4.
19. Directive, ¶ 59.
20. The Commission issued two sets of Standard Contractual Clauses, one for controller to Third Country controller-transfers (Commission Decision 2001/497, 2001 O.J. (L 181) (EC) and 2004/915, 2004 O.J. (L 385) (EC)) and the other for controller to Third Country processor-transfers (Commission Decision 2010/87, 2010 O.J. (L 39) (EU)).
21. The Directive authorizes DPA to authorize other adequate safeguards and requires it to inform the Commission and the other Member States of the authorization. If a Member State or the Commission objects on justified grounds, the Commission shall take appropriate measures.
22. Directive, art. 28.
23. *Id.* art. 22, 23.

Continued from page 6

IV. The *Schrems* Case and the CJEU Judgment

In the wake of former U.S. National Security Agency contractor Edward Snowden's revelations about U.S. authorities' allegedly indiscriminate surveillance of electronic communications, Maximilian Schrems, an Austrian Facebook user, began proceedings in the High Court in Ireland. Those proceedings commenced after the Irish Data Protection Commissioner refused to investigate his concerns about the "Safe Harbor" system, which allowed Facebook's Irish subsidiary to send Schrems' personal data to Facebook Ireland's parent company located in the United States. The Irish Data Protection Commissioner reasoned that it could not do so because of the Commission Decision.

"The CJEU ruled, however, that the Commission Decision did not limit the national DPAs' powers. As a result, national regulators are able and even required to examine whether an at-issue transfer of data to a Third Country complies with the applicable legal requirements, regardless of any previous determinations by the Commission."

The CJEU ruled, however, that the Commission Decision did not limit the national DPAs' powers. As a result, national regulators are able and even required to examine whether an at-issue transfer of data to a Third Country complies with the applicable legal requirements, regardless of any previous determinations by the Commission. Therefore, the CJEU ruled, the Irish regulator should have made its own ruling on whether data transferred pursuant to a Safe Harbor self-certification would receive an adequate level of protection in the United States.

The CJEU then stated that, if an EU regulator did find that transfers pursuant to the Safe Harbor provided inadequate protection,[24] legal proceedings aimed at invalidating the Commission Decision must be commenced before the CJEU, as only that court had jurisdiction to declare a Commission decision invalid. The CJEU went on to consider whether the Commission Decision was valid: it held it was not.

The CJEU determined that, for two independent reasons, the Safe Harbor does not afford adequate protection in the United States for EU personal data.

Continued on page 8

24. This applies equally to transfers pursuant to other Commission determinations regarding the adequacy of data protection in other Third Countries.

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 7

First, the CJEU said that companies subject to U.S. law are bound to disregard the Safe Harbor rules and protocols protecting data privacy if they conflict with the national security, public interest, and law enforcement requirements of the United States. As a result, in the opinion of the CJEU, the Safe Harbor does not prevent, and indeed enables, interference by U.S. public authorities with the fundamental rights of individuals under EU law. The Judgment criticized the Commission Decision for allowing this, referring to the Decision as legislation[25] that is "not limited to what is strictly necessary [because] it authorises, on a generalised basis, storage of all the personal data of all the persons whose data has been transferred from the European Union to the United States without any differentiation, limitation or exception being made in the light of the objective pursued and without an objective criterion being laid down by which to determine the limits of the access of the public authorities to the data, and of its subsequent use" and, in particular, "legislation permitting the public authorities to have access on a generalised basis to the content of electronic communications." As such, the Decision did not limit exceptions to what is strictly necessary in respect of privacy under the Charter.

Second, the CJEU considered individuals' rights of redress against surveillance by U.S. authorities. The court found that individuals subject to government review of their personal data in the United States could not pursue adequate legal remedies in order to access, rectify, or erase the data. Again, the CJEU considered that the Commission Decision, in allowing transfers under circumstances in which data importers may make the personal data transferred available to the United States government, did "not provid[e] for any possibility for an individual to pursue legal remedies in order to have access to personal data relating to him, or to obtain the rectification or erasure of such data." It held that the absence of such rights compromised the fundamental right to effective judicial protection under EU law.

As a matter of CJEU procedural law, the United States was not a party to the proceedings (nor was Facebook). And, under the Directive, the assessment of individual transfers is a matter for national DPAs to decide in accordance with each Member State's law.

Following the Judgment, and a further hearing on October 20, 2015 before the Irish High Court quashing the Irish Data Protection Commissioner's decision, the Data Protection Commissioner has confirmed that her office will now investigate the substance of the complaint with all due diligence.[26] If the Irish Data Protection

Continued on page 9

25. The words used in the French and German texts are better translated as "regulation" than "legislation."

26. *See* Statement from the Irish Data Protection Commissioner, Helen Dixon in respect of High Court Case 2013/765 JR - Schrems (Oct. 20, 2015), https://www.dataprotection.ie/docs/20-10-2015-Statement-from-Data-Protection-Commissioner-Helen-Dixon-in-respect-of-High-Court-Case-2013-765-JR-Schrems/1498.htm.

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 8

Commissioner determines that Facebook's data protection arrangements made under the Safe Harbor Principles do not provide for an adequate standard of protection and there are no other legal bases for a transfer, the Irish Data Protection Commissioner may prohibit or suspend the flow of personal data from Facebook Ireland to Facebook, Inc. in the United States.

One of the most important take-aways from the Judgment is that, as the CJEU makes clear, DPAs have the power to make their own determinations about the validity of transfers. But it remains to be seen how this power will be used. The Article 29 Working Party – the group consisting of representatives of all 28 Member States' DPAs and representatives of the European Data Protection Supervisor and the Commission – has stated that it considers that data transfers from the EU to the United States based solely on the Commission Decision – *i.e.*, made pursuant to the Safe Harbor – can no longer be considered lawful.

It was not entirely surprising that the CJEU would be critical of the Safe Harbor system. Indeed, the Commission itself identified in 2013 a number of weaknesses in the Commission Decision, and concluded that the then-current implementation of the Safe Harbor could not be maintained permanently.[27] However, the Commission determined that revocation of its approval of the Safe Harbor Principles would adversely affect the interests of EU and U.S. companies and thus decided to enter into negotiations with the United States over potential improvements to the Safe Harbor.[28] The CJEU clearly had no such qualms. The Judgment in fact now pushes the EU to take stronger positions in the ongoing diplomatic negotiations for an updated Safe Harbor Framework. It is thus unlikely that the current Safe Harbor, with only minor modifications, will be the foundation of further agreements between the United States and the Commission.

V. Practical Consequences of the Judgment

One result of the Judgment is that companies transferring or intending to transfer personal data from the EU to the United States ought to consider the methods they are using or intending to use in order to determine whether they can continue in the same way or need to make changes. There is no need for panic or precipitous action: many of the current methods of data transfer remain available for use and companies may also be able to use other methods they have not previously considered. Nonetheless, the situation is very much in flux: companies must remain vigilant and aware because further changes are expected in the next few months.

Continued on page 10

27. The Commission adopted the Communication from the Commission to the European Parliament and the Council, *Rebuilding Trust in EU-US Data Flows*, COM (2013) 846 final (Nov. 27, 2013).

28. *See* Communication from the Commission to the European Parliament and the Council, *Rebuilding Trust in EU-US Data Flows*, at 7, COM (2013) 846 final (Nov. 27, 2013).

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 9

A. Companies Previously Relying on the Safe Harbor

Decision making is most urgent for the approximately 4,000 companies that previously relied on the Safe Harbor. As a result of the Judgment, the Safe Harbor no longer serves as a legal basis for EU data transfers to the United States. One of the significant benefits of using the Safe Harbor was the certainty that it provided – this has now been eliminated.

Technically, until local DPAs or the courts within Member States – or the European Commission – rule that current transfers using data protection standards that also formed part of the Safe Harbor do not ensure an adequate level of protection, companies are not enjoined to halt such transfers. Such rulings are likely to come from some DPAs,[29] however, though other DPAs may be less willing to bring enforcement action.[30]

"Technically, until local DPAs or the courts within Member States – or the European Commission – rule that current transfers using data protection standards that also formed part of the Safe Harbor do not ensure an adequate level of protection, companies are not enjoined to halt such transfers. Such rulings are likely to come from some DPAs, however, though other DPAs may be less willing to bring enforcement action."

For this reason, companies that continue to transfer EU data to the United States by relying solely on the data protection measures that were required by the Safe Harbor Principles may find themselves subject to enforcement action. They would be well advised, therefore, to utilize one of the other options, discussed below, for the legitimate transfer of data; in some cases, these will be methods of transfer they have not previously used.

As for transfers predating the Judgment, DPAs should be sympathetic to companies that had relied in good faith on the Safe Harbor procedures, though that is not guaranteed.[31] For those past transfers, companies should consider whether they can rely on other methods to maintain the data in the United States. If they are unable to do so, depending on the nature and public profile of the business and

Continued on page 11

29. The German DPAs, in a position paper at their Data Protection Conference, dated October 26, 2015, indicated that they would prohibit transfers that are solely based on Safe Harbor and would assess the other means of transfers used. *See* https://www.datenschutz.hessen.de/ft-europa.htm#entry4521 [hereinafter, "German DPA Position Paper"].

30. The UK's DPA, the Information Commissioner's Office, stated that companies should not "rush to change" their arrangements, and stated that it was "certainly not rushing to use [its] enforcement powers." David Smith, "The US Safe Harbor – breached but perhaps not destroyed!," *Information Commissioner's Office blog* (Oct. 27, 2015), https://iconewsblog.wordpress.com/2015/10/27/the-us-safe-harbor-breached-but-perhaps-not-destroyed/.

31. The Judgment has retroactive effect. Treaty on the Functioning of the European Union, art. 264, Oct. 26, 2012, 2012 O.J. (C 326).

Continued from page 10

the quantity and type of personal data involved, they may wish to consider the possibility of repatriating the data to the EU.

B. Other Methods of Transfer

As noted above, the Safe Harbor has never been the only lawful means for transfer of personal data from the EU to the United States. Under the Directive and decisions of the Commission and the Article 29 Working Party, the following methods are all available, depending on the circumstances:

1. Transfer necessary for the execution of a contract with the data subject (the "Contract Performance Exception")
2. Transfer necessary in connection with legal proceedings, for the purpose of obtaining legal advice, or establishing, exercising or defending a legal right (collectively, the "Legal Exception")
3. Transfer with the consent of the data subject (the "Consent Exception")
4. Transfers subject to Standard Contractual Clauses (embodied in "Data Transfer Agreements" or "DTAs")
5. Transfers subject to BCRs

In addition, a transfer that does not include personal data (either where none was collected, or the data have been redacted) is also acceptable.

As each of the methods remains available, which to choose depends on the circumstances. Companies transferring data to the United States should conduct a risk assessment, based on the following factors, before determining which method is right for them:

1. The type of business being operated.
2. The types of personal data being transferred to the United States.
3. The volume of personal data to be transferred to the United States.
4. The purposes of the transfers.
5. Whether it is necessary to transfer all of such data to the United States.

Companies may find, in conducting this exercise, that they need to use different methods for different transfers: transfers of employee data, for example, may be based on the Contract Performance Exception or covered by DTAs, while transfers of customer data may be based on the Consent Exception.

We review below each of the available methods and discuss when it should be used.

Continued on page 12

Continued from page 11

C. The Exceptions

The Judgment has no impact on the Contract Performance Exception, the Legal Exception, or the Consent Exception, as these exceptions apply irrespective of the data protection standards in the Third Country. Therefore, companies that have been legitimately using them can continue to rely on them. Companies that have previously relied on the Safe Harbor should consider whether they can now rely on one of the exceptions, which are described in more detail below.

C.1 The Contract Performance Exception

This exception is commonly used by companies that provide services in the United States to EU data subjects. The paradigmatic example is that of a hotel company that, in the EU, takes the reservation of an EU customer for a U.S. hotel and sends that customer's personal details to that hotel. If the hotel in the United States did not have the personal details of the customer, it would not be able to hold the reservation and provide a room to the customer, as the company is obliged to do by contract. Transfer is permitted under this exception.

For this exception to apply, however, the transfer must be necessary to perform the contract, not just convenient. So, for example, in the context of an employment contract, an EU company cannot use this exception to transfer all its employees' payroll data to a back office in the United States solely in order to save money and time; mere convenience and efficiency does not equate to necessity.

C.2 The Legal Exception

This is the most relevant exception in the context of corporate investigations.

For example, when a European company complies with an information request from the U.S. government, whether a subpoena or a request for voluntary compliance, the company may rely on the Legal Exception to transfer data from the EU to the United States. The Judgment does not have any impact on this exception.

This point has just been made in the United States Court of Appeals for the Second Circuit, in which Microsoft Corporation has been resisting the U.S. government's attempt to use a search warrant to compel production of customer emails housed on a server in Ireland and argued that the Judgment could expose it to liability if it acceded to the transfer. The Department of Justice has responded that the Judgment deals with voluntary transfers of data and did not address the transfer of data to the United States pursuant to a warrant. In other words, it claims transfers necessary for legal proceedings remain unaffected by the Judgment.[32]

Continued on page 13

32. *See In the Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*, No. 14-2985, 28(j) Letter (2d Cir. filed Oct. 17, 2015).

Continued from page 12

Where no legal process has been initiated by an arm of the U.S. government, however, such as when a company is simply conducting a preliminary inquiry or internal investigation, this group of exceptions is not necessarily available. The company would need to determine the extent to which the transfer is necessary to gain legal advice or establish its legal rights. In some cases, that necessity may well exist, where for example the company's lawyers and legal department are all in the United States, along with the bulk of the evidence. If so, the transfer may be lawful. Some DPAs are more amenable to the use of this exception than others: the United Kingdom's Information Commissioner Office, for example, has stated that the exception applies to "future proceedings not yet underway . . . proceedings [that] do not . . . involve [the data exporter or the data subject] as a party and . . . legal rights that [are not the data exporter or the data subject's]."[33] Other DPAs view the Legal Exception more restrictively.

It is therefore important, before making use of the Legal Exception, to determine which DPA or DPAs will have jurisdiction over the transfer, and its (or their) interpretation of it.

C.3 The Consent Exception

The Consent Exception, although often invoked, is, in practice, not always available or helpful.

First, in several Member States, the requirements for unambiguous consent can be strict, particularly when it comes to that of an employee. The Article 29 Working Party has noted that there may be a strong presumption that consent is ambiguous in the employment context, although, again, different DPAs and local courts reach different conclusions on this issue.[34] Most DPAs require extensive description of the intended use of the data following the transfer and proof in writing that the advice has been given. Another context in which consent is treated with suspicion is if it is hidden in lengthy online terms of use to which customers are expected to give their assent. In such cases, consent to transfers from the EU to the United States may even be the subject of express provisions. If, however, the relevant language is not obvious – buried within a multi-page set of terms, for example – most DPAs may not consider the consent as being unambiguous, informed, and freely given.

Second, it may not be practical to obtain consent if the data subject is not readily available or willing to cooperate, or if large scale transfers are involved.

Continued on page 14

33. ICO, Sending Personal Data Outside the European Economic Area (Principle 8).

34. Article 29 Working Party, "Opinion 15/2011 on the definition of consent" (July 13, 2011).

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 13

In the context of investigations and litigation, in situations in which companies copy individual employees' hard drives, the Consent Exception may sometimes be used (if employee consent is considered valid in that Member State) – but companies frequently run the risk that employees will refuse or revoke their consent.

Finally, consent for data transfers potentially might be even more cabined if DPAs rule that any consent given without telling the data subject that his or her personal data may be the subject of surveillance by the U.S. authorities is not fully informed.

Therefore, companies intending to rely on the Consent Exception should be careful and use caution in determining whether it is available.

"BCRs were designed by the Article 29 Working Party. They are a code of practice that multinational companies or groups of companies draw up and follow voluntarily to facilitate data transfers by a company or group from the EU to a Third Country. The transfer may be, for example, from an EU parent company to a U.S. subsidiary, from an EU branch to U.S. headquarters, or from one EU affiliate to a U.S. affiliate."

D. Standard Contractual Clauses and BCRs

As noted, two additional mechanisms are available for data transfers to a Third Country: Standard Contractual Clauses, as embodied within DTAs, and BCRs.

Standard Contractual Clauses have been written by the Commission.[35] If the clauses are used without amendment in agreements between data exporter and data importer, they can be the legal basis of data transfers to Third Countries.

BCRs were designed by the Article 29 Working Party. They are a code of practice that multinational companies or groups of companies draw up and follow voluntarily to facilitate data transfers by a company or group from the EU to a Third Country.[36] The transfer may be, for example, from an EU parent company to a U.S. subsidiary, from an EU branch to U.S. headquarters, or from one EU affiliate to a U.S. affiliate. A BCR requires the approval of one of the DPAs with jurisdiction – known as the "lead authority" – over the EU-based entity that is exporting data to the United States. The exporting entity proposes which DPA should be the lead authority but the final decision is taken by the DPAs acting in concert. The process for approval can therefore be lengthy.

Continued on page 15

35. *See* Directive, art. 28.

36. The Article 29 Working Party has issued "Transfers of personal data to Third Countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers" (June 3, 2003), a series of Working Documents establishing criteria for approval of BCRs.

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 14

DTAs have one other advantage over BCRs: they can be used to transfer data from one entity to another completely unaffiliated entity, whereas BCRs can be used only for transfers among the entities of a single corporate group.

The most important point is that, in the wake of the Judgment, and as noted in a communication from the Commission to the European Parliament and the European Council,[37] DTAs and BCRs remain available for use, both for companies that are now relying on them and for those Safe Harbor registrants now looking for ways to come into compliance with the EU law on transfer of personal data to the United States.

Nevertheless, the Judgment is being read to throw into some doubt the future legality of these two methods for data transfer. In response to the Judgment, the Article 29 Working Party said:

> [T]he Working Party is urgently calling on the Member States and the European institutions to open discussions with US authorities in order to find political, legal and technical solutions enabling data transfers to the territory of the United States that respect fundamental rights.
>
> …
>
> In the meantime, the Working Party will continue its analysis on the impact of the CJEU judgment on other transfer tools. During this period, data protection authorities consider that Standard Contractual Clauses and Binding Corporate Rules can still be used. In any case, this will not prevent data protection authorities to investigate particular cases, for instance on the basis of complaints, and to exercise their powers in order to protect individuals.
>
> If by the end of January 2016, no appropriate solution is found with the US authorities and depending on the assessment of the transfer tools by the Working Party, EU data protection authorities are committed to take all necessary and appropriate actions, which may include coordinated enforcement.[38]

Continued on page 16

37. *See* "Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems)," http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/files/eu-us_data_flows_communication_final.pdf.

38. Article 29 Data Protection Working Party, "Statement on the implementation of the judgement of the Court of Justice of the European Union of 6 October 2015 in the Maximilian Schrems v Data Protection Commissioner case (C-362-14)" (Oct. 16, 2015), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2015/20151016_wp29_statement_on_schrems_judgement.pdf (emphases added).

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 15

On the one hand, that the Standard Contractual Clauses and BCRs can continue to be used is reassuring. On the other hand, the Working Party's statement is deliberately vague and can be read as an implicit threat.

Entities relying on these mechanisms cannot be certain what the Working Party or Member State DPAs will do if they are not satisfied with progress by the end of January 2016, or even whether there is consensus amongst the DPAs. The German DPAs have already indicated that they consider the Standard Contractual Clauses and BCRs as being affected by the Judgment, and have stated that they do not consider the Clauses are a sufficient basis for a transfer;[39] the UK's Information Commissioner's Office, by contrast, stated that the Standard Contractual Clauses "do still stand, and can be relied on by businesses, certainly for the time being," while noting that the Judgment "inevitably cast some doubt on the future of" the Clauses.[40] It is not inconceivable that actions will be taken, either by DPAs acting alone or in concert, that render invalid one or both of the Standard Contractual Clauses and BCRs. Given the large number of companies that use these methods, that would have an even greater impact than the Judgment's invalidation of the Safe Harbor.

Nonetheless, in many cases, DTAs and BCRs may remain viable options for transfers, subject to certain qualifications discussed at D.1 and D.2 below.

Some or all DPAs may, however, start requiring additional protections before allowing the continued use of DTAs and BCRs. Companies that wish to prepare themselves for such an eventuality should consider applying some or all of these additional safeguards to their arrangements:

- Limiting data transfers to the United States to that which is absolutely necessary;
- Using encryption, with accelerated changes of encryption keys;
- Ensuring that data are deleted as soon as they are no longer required; and
- Inserting obligations in DTAs and BCRs requiring the data importer to notify the data exporter if a third party attempts to access the data and to take any legal measures available to the data importer to defend and protect the rights of the data exporter and the data subjects.

Continued on page 17

39. *See* German DPA Position Paper, *supra* note 29.

40. Smith, *supra* note 30.

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 16

D.1 Standard Contractual Clauses/DTAs

DTAs can be implemented relatively quickly and, in the cases of intra-corporate transfers, with minimum complications.

There are, however, some potential shortcomings to the use of DTAs.

First, there is no flexibility in implementing the DTAs: they must incorporate the Standard Contractual Clauses in the form required by the Commission. Any deviation or variation from the specified language invalidates the DTAs. Of course, many companies have learned to live with this and accept all of the provisions of the Standard Contractual Clauses. Some others may have decided against entering into DTAs because they cannot be varied and they cannot comply with one or more of the specified provisions. Those that opted for Safe Harbor over DTAs may now need to revisit their decision.

"DPAs may take the position that U.S. national security and law enforcement laws are in conflict with the adequacy of protection, if those laws are seen as having a 'substantial adverse effect on the guarantees' provided by the Standard Contractual Clauses, as the CJEU itself indicated in the Judgment."

Second, DTAs may be less attractive following the Judgment because the U.S.-based data importer must warrant to the data exporter

> that he has no reason to believe that the legislation applicable to him [here, U.S. law] prevents him from fulfilling his obligations under the contract and that in the event of a change in that legislation which is likely to have a substantial adverse effect on the guarantees provided by the Clauses, he will notify the change to the data exporter and to the supervisory authority where the data exporter is established, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract.[41]

Continued on page 18

41. *See* Commission Decision 2001/497, contractual clause 5(a), 2001 O.J. (L 181) (EC) and Commission Decision 2010/87, contractual clause 5(b), 2010 O.J. (L 39) (EU) (emphasis added). There is a similar clause in Commission Decision 2004/915, clause IIc, 2004 O.J. (L 385) (EC). Under one type of transfer using the Standard Contractual Clauses (a transfer from a "Data Controller" to a "Data Processor"), the data importer must notify the data exporter about any binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited. *See* Commission Decision 2010/87, contractual clause 5d (i), 2010 O.J. (L 39) (EU).

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 17

What this means is that the data importer in the United States has an affirmative obligation to make disclosure to the data exporter and relevant DPA if U.S. legislation makes it unable to fulfill its contractual duties.[42] DPAs may take the position that U.S. national security and law enforcement laws are in conflict with the adequacy of protection, if those laws are seen as having a "substantial adverse effect on the guarantees" provided by the Standard Contractual Clauses, as the CJEU itself indicated in the Judgment. In such case, U.S. data importers may be called upon to assess whether U.S. legislation is compatible with their DTA obligations and make appropriate disclosures of U.S. legislation – or any assessed incompatibility – to data exporters and the relevant DPA. The consequences of any such disclosure could be serious.[43] The relevant DPA could (and is probably required to) exercise its powers to prohibit or suspend data flows pursuant to that DTA.

On a related point, a current or prospective data importer may decide that, in light of the Judgment, it may not feel comfortable making the warranty set forth above. In such case, it could not agree to a DTA and the Standard Contractual Clauses would not be available to the data exporter.

Third, entering into a DTA does not assure the data exporter and data importer that data transfer is, for all time, confirmed to be lawful. As noted, the use of DTAs to export data to the United States may be challenged or even prohibited, perhaps in the next few months. Further, because some Member States' legislation provides that the DPA has the power to approve or disapprove DTAs, it is quite possible that the Judgment will increase the risk of disapprovals by DPAs. In any event, in those Member States, the process of obtaining approval may be time-consuming due to understaffing and the increased interest, given the unavailability of the Safe Harbor, in using DTAs to transfer personal data from the EU.

These shortcomings should not detract from the fact that, for now, DTAs remain available for data transfer. They will not be invalidated without further legal proceedings. Accordingly, DTAs continue to offer a straightforward and relatively quick means of enabling transatlantic flows of personal data, including for data exporters that had previously relied on the Safe Harbor.

Continued on page 19

42. *See* the Commission document, Frequently Asked Questions relating to transfers of personal data from the EU/EEA to third countries, at 27 and 41, http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/international_transfers_faq.pdf.

43. *Id.* at 27.

Continued from page 18

D.2 Binding Contractual Rules

BCRs, like DTAs, remain available to transfer personal data to the United States. For data exporters that had relied on the Safe Harbor, however, BCRs cannot provide an immediate solution. That is because the approval process for a set of BCRs typically requires an extended review by the corporate entities involved, followed by an approval process by the relevant DPAs that usually takes several months. Even longer approval periods should be expected at a number of DPAs that are understaffed. Therefore, it is unlikely that a corporate group applying now for approval of a BCR would receive approval before the Working Party's end-of-January 2016 deadline.

Nonetheless, those corporate groups that currently transfer EU data under BCRs can continue using them. Although BCRs are more flexible than the Standard Contractual Clauses, they have some of the other shortcomings of DTAs discussed above.

First, all BCRs, as opposed to just some DTAs, require the approval of the relevant DPA both for initial and for continued use. The Judgment increases the chance that individual DPAs will refuse approval for new BCRs and withdraw approval for existing ones.

Second, BCRs, like DTAs, require disclosures regarding Third Country legislation. In May 2015, the Article 29 Working Party specified, in accordance with prior recommendations, that a clear provision in the BCRs is required indicating that if a member of the group of companies has reason to believe that existing or future legislation applicable to that member may prevent it from fulfilling the instructions received from the EU transferor of the data or its obligations under the BCR, it will promptly disclose this fact to (i) the transferor of the data which is entitled to suspend the data transfer; (ii) the EU headquarters or EU group member companies or (parent companies, subsidiaries, or affiliates) exporting the data, which consequently possess data protection responsibilities, or the relevant data processor/privacy officer function; and (iii), importantly, the DPA that has jurisdiction over the data controller.[44] Therefore, as with DTAs, if such a disclosure were to be made to a DPA, the DPA potentially would have to, or, in any event, could, withdraw its approval of the BCR.

Continued on page 20

44. Article 29 Data Protection Working Party, "Explanatory Document on the Processor Binding Corporate Rules," sec. 2.3.4 (Apr. 19, 2013).

Continued from page 19

Although the use of BCRs may be open to challenge in the near future, at present, at any company that operates under them they can continue to be used until a DPA affirmatively withdraws its approval in respect of that company. Ultimately, it is unlikely that the Working Party will opt to do away with BCRs altogether, given that DPAs are able to exercise control over them. In short, over the longer term, BCRs may become a more common method for transferring EU data to the United States.

E. Not Exporting Personal Data from the EU

If none of these methods is practical or suitable, companies may need to consider options for *not* transferring EU personal data to the United States. Perhaps, they can restructure their operations so that processing of data could be carried out within the EU. For many companies, of course, this solution may not be practical and it may increase the expense of processing data.

Sometimes, companies may be satisfied with using personal data in an anonymized form. Such data is not covered by the EU data protection regime. In some cases, companies transferring personal data might have the option of considering whether their business purpose could still be met if the data were anonymized. This is more likely to be the case, however, for small-scale, intermittent transfers rather than frequent or continuing transfers of personal data in bulk.

As a last resort, data exporters may want to consider repatriating EU personal data from the United States or from a U.S.-based cloud. This may be quite unworkable for many companies, though it would remove all risks of non-compliance with the EU data protection regime.

VI. What Happens Next?

A. Working Party Deliberations

As noted above, the Article 29 Working Party has issued a statement that offers some short-term comfort that the Standard Contractual Clauses and BCRs can continue to be used, at least unless a national DPA exercises its powers to suspend transfers under those mechanisms. The Working Party may revisit this view, however, and national DPAs may take action, collectively or otherwise, after January 2016 – if no diplomatic solution is reached between the EU and the United States. The national DPAs are expected to start making their views known shortly. Companies and governments on both sides of the Atlantic will no doubt be watching to see whether there are any differences in approach.

Continued on page 21

EU Data Transfers to the United States: Practical Consequences of the European Court of Justice's Recent Decision

Continued from page 20

B. Updated Safe Harbor Framework

In the Commission's October 6, 2015 statement, it stressed the need to continue the work that began in 2014 towards a renewed and safe framework for the transfer of personal data across the Atlantic.[45] According to Věra Jourová, European Commissioner in charge of Justice, Consumers and Gender Equality, the EU and United States had already been close to an agreement before the CJEU rendered the Judgment.[46] The need for the parties to reach an agreement has now become even more urgent. Jourová and her U.S. counterparts are committed to holding further meetings.[47]

"On October 26, Commissioner Jourová announced that the United States and the EU had an agreement in principle to update the Safe Harbor framework. She said that the two sides were still discussing how best to ensure that commitments would be binding."

On October 26, Commissioner Jourová announced that the United States and the EU had an agreement in principle to update the Safe Harbor framework. She said that the two sides were still discussing how best to ensure that commitments would be binding. According to the Commissioner, the United States has addressed transparency and enforcement concerns by committing to stronger oversight by the U.S. Department of Commerce, cooperating with European data protection regulators and directing complaints to the Federal Trade Commission.[48]

Continued on page 22

45. European Commission Press Release STATEMENT/15/5782, First Vice-President, Timmermans and Commissioner Jourová's press conference on Safe Harbour following the Court ruling in case C-362/14 (Schrems) (Oct. 6, 2015), http://europa.eu/rapid/press-release_STATEMENT-15-5782_en.htm [hereinafter Safe Harbor Press Release].

46. Lucie Bednárová, "Věra Jourová: We will be strict with the US on Safe Harbour," *EurActiv* (Mar. 13, 2015, 8:08 AM, updated Oct. 15, 2015, 10:29 AM), http://www.euractiv.com/sections/infosociety/vera-jourova-we-will-be-strict-us-safe-harbour-312856.

47. *See* European Commission Press Release SPEECH/15/5916, Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties, Justice and Home Affairs (Libe) (Oct. 26, 2015), http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm. The United States and EU have recently reached preliminary agreement in another area of data protection: the so-called "Umbrella Agreement," which allows data transfers for law enforcement purposes. *See* European Commission Press Release STATEMENT/15/5610, Statement by EU Commissioner Věra Jourová on the finalisation of the EU-US negotiations on the data protection "Umbrella Agreement" (Sept. 8, 2015), http://europa.eu/rapid/press-release_STATEMENT-15-5610_de.htm. The Umbrella Agreement has no effect on the ability of private parties to transfer data, but demonstrates that data protection agreements between the United States and EU remain possible.

48. *See* European Commission Press Release SPEECH/15/5916, Commissioner Jourová's remarks on Safe Harbour EU Court of Justice judgement before the Committee on Civil Liberties, Justice and Home Affairs (Libe) (Oct. 26, 2015), http://europa.eu/rapid/press-release_SPEECH-15-5916_en.htm.

Continued from page 21

The parties, as well as businesses on both sides of the Atlantic and the U.S. Congress, are fully aware of the Working Party's looming deadline of the end-of-January 2016.

C. Transfers to Other Third Countries

For transfers of EU data to other Third Countries (*i.e.*, not the United States) based on Commission adequacy decisions,[49] the Judgment raises the very small risk that those decisions could be challenged by various parties and invalidated by the CJEU. That risk is low because those decisions were made in reliance on the protections of nationwide data protection legislation in each of the Third Countries, not on their national analogues to the Safe Harbor.[50]

D. Other Litigation

Data protection activists may now have incentives to bring actions to protect their data protection rights before national DPAs and national courts. For example, Maximilian Schrems, who started the proceedings that culminated in the Judgment, has already filed an action in Austria, on behalf of more than 20,000 Facebook users, for damages and an injunction.[51] Works councils or discontented employees in international corporate groups or individual companies could follow suit.

E. EU Data Protection Reform

All this comes in the midst of a complete overhaul of EU data protection law. In January 2012 the Commission proposed a comprehensive reform of the Directive.[52] Since then, negotiations have been held among the Commission, the European Parliament and the Council of the European Union.[53] The review remains on track, and a new law could be finalized this year.[54] Because new legislation almost certainly will need to take the Judgment into account, enactment may be delayed.

Continued on page 23

49. *See supra* note 14.
50. In addition, the Commission has announced its intention to replace provisions in its adequacy decisions that may limit the powers of national DPAs. *See supra* note 37.
51. *See* Europe v. Facebook page relating to Facebook class action (http://www.europe-v-facebook.org/EN/Complaints/Class_Action/class_action.html (Oct. 23, 2015)) and the materials of the procedure (https://www.fbclaim.com/ui/page/updates (Oct. 23, 2015)).
52. *See* European Commission data protection reform page, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (Oct. 23, 2015).
53. *See id.*
54. Safe Harbor Press Release, *supra* note 45.

Continued from page 22

VII. Conclusion

The Judgment has made significant headlines. That was not at all surprising, given the state of relationships between the United States and the EU with respect to privacy issues, particularly in the wake of the Snowden disclosures. Although diplomatic efforts will undoubtedly accelerate to avoid significant harms to commerce, for the time being the Judgment will prove disruptive and, possibly, costly for the firms that have relied on the Safe Harbor. DTAs and BCRs, notwithstanding their limitations, will become attractive alternatives for lawful transfer of EU data to the United States, particularly for businesses with global operations that collect and process personal data, and for cloud storage providers. We will continue to monitor developments closely and publish additional updates as warranted.

Dr. Thomas Schürrle

Jeffrey P. Cunard

Jim Pastore

Matthew Getz

Christopher Garrett

Dr. Friedrich Popp

Dr. Thomas Schürrle is a partner, and Dr. Friedrich Popp is an associate, in the Frankfurt office. Jeffrey P. Cunard and Jim Pastore are partners in the Washington, D.C., and New York offices, respectively. Matthew Getz is an international counsel, and Christopher Garrett is an associate, in the London office. They are each members of the firm's Cybersecurity and Data Privacy Practice. The authors may be reached at tschuerrle@debevoise.com, jpcunard@debevoise.com, jpastore@debevoise.com, mgetz@debevoise.com, cgarrett@debevoise.com, and fpopp@debevoise.com. Full contact details for each author are available at www.debevoise.com.

FCPA Update

FCPA Update is a publication of
Debevoise & Plimpton LLP

919 Third Avenue
New York, New York 10022
+1 212 909 6000
www.debevoise.com

Washington, D.C.
+1 202 383 8000

London
+44 20 7786 9000

Paris
+33 1 40 73 12 12

Frankfurt
+49 69 2097 5000

Moscow
+7 495 956 3858

Hong Kong
+852 2160 9800

Shanghai
+86 21 5047 1800

Paul R. Berger
Co-Editor-in-Chief
+1 202 383 8090
prberger@debevoise.com

Sean Hecker
Co-Editor-in-Chief
+1 212 909 6052
shecker@debevoise.com

Andrew M. Levine
Co-Editor-in-Chief
+1 212 909 6069
amlevine@debevoise.com

Steven S. Michaels
Executive Editor
+1 212 909 7265
ssmichaels@debevoise.com

Erich O. Grosz
Co-Managing Editor
+1 212 909 6808
eogrosz@debevoise.com

Jane Shvets
Deputy Managing Editor
+1 212 909 6573
jshvets@debevoise.com

Bruce E. Yannett
Co-Editor-in-Chief
+1 212 909 6495
beyannett@debevoise.com

Karolos Seeger
Co-Editor-in-Chief
+44 20 7786 9042
kseeger@debevoise.com

David A. O'Neil
Co-Editor-in-Chief
+1 202 383 8040
daoneil@debevoise.com

Matthew Getz
Co-Managing Editor
+44 20 7588 4180
mgetz@debevoise.com

Philip Rohlik
Co-Managing Editor
+852 2160 9856
prohlik@debevoise.com

Ashley Fillmore
Assistant Editor
+1 212 909 6137
afillmore@debevoise.com

Please address inquiries regarding topics covered in this publication to the editors.

Please note:
The URLs in FCPA Update are provided with hyperlinks so as to enable readers to gain easy access to cited materials.