VOLUME 103 NUMBER 1 SPRING 2019
Judicature
Published by the Bolch Judicial Institute at Duke Law. Reprinted with permission.
judicialstudies.duke.edu/judicature

Vol. 103 No. 1

Overseas Obligations

AN UPDATE ON CROSS-BORDER DISCOVERY

By MICHAEL M. BAYLSON AND SANDRA A. JESKIE

An article published in the Winter 2016 edition of *Judicature* provided an overview of case law and approaches for handling cross-border discovery in litigation. Since then, there have been some notable developments in several important case decisions and legislation that United States practitioners seeking overseas discovery, and judges ruling on these issues, must keep in mind.

Section I of this article addresses the recent "*Vitamin C*" Supreme Court decision that establishes a new standard for the application of Federal Rule of Civil Procedure 44.1, entitled "Determining Foreign Law." Section II addresses the Clarifying Lawful Overseas Use of Data (CLOUD) Act, a new statute establishing a process through which countries can work together in criminal investigations to access data from global sources. Section III addresses recent case reliance on the Restatement (Third) of Foreign Relations Law. Section IV addresses the impact of the General Data Protection Regulation (GDPR) on overseas discovery in U.S.-based litigation. Section V reviews the work product of three independent legal groups that provide helpful guidance: The Sedona Conference, the Federal Judicial Center, and the Electronic Discovery Reference Model (EDRM).

I. THE "VITAMIN C" UNITED STATES SUPREME COURT DECISION

In *Animal Science Products, Inc. v. Hebei Welcome Pharmaceutical Co.*[1] (colloquially referred to as the *Vitamin C* decision because vitamin C was the subject matter of the case), the Supreme Court, for the first time, articulated a test that district courts must use in the application of Rule 44.1, dealing with choice of foreign law.

In *Vitamin C*, Chinese manufacturers and exporters of vitamin C were accused of violating Section 1 of the Sherman Antitrust Act.[2] In the district court proceeding, defendants filed a motion to dismiss, arguing that the Chinese government required them to fix the price and quantity of exports pursuant to Chinese law, protecting them from liability under the Sherman Act.[3] The district court denied the motion, relying on plaintiffs' evidence casting doubt upon a statement from the Ministry of Commerce of China.[4] The Second Circuit, finding that the district court erred in denying the motion, articulated a test that was highly deferential to the foreign interest.[5] Justice Ruth Bader Ginsberg, writing for a unanimous Supreme Court, vacated the Second Circuit's decision and relied on the principles of international comity, articulated in the still-leading *Aerospatiale*[6] decision,[7] to hold that a "federal court should accord respectful consideration to a foreign government's submission, but is not bound to accord conclusive effect to the foreign government's statement."[8] The Court emphasized that district judges have discretion in applying Rule 44.1. Justice Ginsberg wrote:

> Given the world's many and diverse legal systems, and the range of circumstances in which a foreign government's views may be presented, no single formula or rule will fit all cases in which a foreign government describes its own law. Relevant considerations include the statement's clarity, thoroughness, and support; its context and purpose; the transparency of the foreign legal system; the role and authority of the entity or official offering the statement; and the statement's consistency with the foreign government's past positions.[9]

Most opinions citing *Vitamin C* have been decided under the Foreign Services Immunity Act (FSIA),[10] and only one touched on discovery issues. In *Funk v. Belneftekhim*,[11] the Second Circuit in a summary order determined that *Vitamin C* did not compel it to find that the district court had abused its discretion when imposing discovery sanctions on Belarusian defendants. The court found no error in the district court's refusal to consider a document, allegedly from the Ministry of Justice of the Republic of Belarus, in determining defendants' FSIA defense.[12]

II. CLOUD ACT

Another major development was Congress's enactment of a statute known as the CLOUD Act, which concerns criminal proceedings but likely will impact civil cases as well.

With the rise of email and cloud computing, law enforcement agencies in the United States and abroad increasingly rely on electronic evidence stored across the globe to investigate and prosecute crimes.[13] The borderless nature of the internet has high- ▸

lighted conflicts between U.S. and foreign data privacy laws, hindering law enforcement's timely access to electronic data.[14] For example, communications providers have been faced with subpoenas and search warrants served by U.S. law enforcement to disclose data located in other countries that conflict with laws in those countries that forbid the requested disclosures.[15]

The CLOUD Act, enacted on March 23, 2018, as part of the Consolidated Appropriations Act of 2018,[16] sought to address conflicts of law by establishing processes through which countries can work together to access data from global providers.[17] The CLOUD Act amended the Stored Communications Act (SCA),[18] which requires technology companies to disclose electronic communications pursuant to warrants issued by U.S. law enforcement.[19] The CLOUD Act added the following provision to the SCA:

> A [service provider] shall comply with the obligations of this chapter to preserve, backup, or disclose the contents of a wire or electronic communication and any record or other information pertaining to a customer or subscriber within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States.

Although the CLOUD Act, by its terms, is limited to criminal matters, its enactment is the first time, at least in recent memory, that Congress has articulated a specific set of factors on "comity" to be applied by the United States in legal relations with other countries. For this reason, judges likely will consider these principles in civil litigation in an effort to resolve existing and possible conflicts between U.S. and foreign law in a manner informed by principles of comity.[20] The CLOUD Act reflects the collaborative effort of the Department of Justice, Congress, data providers, and academics to preserve an open internet in which "rights-respecting" countries can access electronic data for law enforcement purposes regardless of where the data is stored.[21]

The CLOUD Act, enacted as part of the Consolidated Appropriations Act of 2018, sought to address conflicts of law by establishing processes through which countries can work together to access data from global providers.

The CLOUD Act seeks to achieve these objectives with four key components.

First, the CLOUD Act clarifies that a lawful SCA warrant served on a communications provider in the United States applies to data stored overseas as long as the data is within the provider's possession, custody, or control.[22]

Second, the CLOUD Act establishes a new framework in which the United States can enter into bilateral data sharing agreements with "rights-respecting" foreign countries.[23] This framework directly addresses potential conflicts of law that could arise if the United States sought access to data in a foreign country that prohibited disclosure to the United States.[24] Under these agreements, each country agrees to remove legal impediments to disclosure of electronic data so that providers can comply with the other country's lawful order requesting such data.[25] Further, pursuant to these agreements, foreign governments can seek data directly from U.S. technology companies without submitting requests subject to individualized review by U.S. courts.[26]

Third, the CLOUD Act allows providers to challenge a warrant issued for data overseas if their compliance with the warrant would violate the laws of a foreign country.[27] Several companies and attorneys requested clarification on how U.S. courts should balance U.S. and foreign interests when conducting a comity analysis.[28] The CLOUD Act provides such clarification: It includes a defined comity analysis, under which courts must consider several enumerated factors when determining whether to quash or modify a warrant seeking data located in a country that has executed a data-sharing agreement.[29] When the foreign nation at issue has not entered into a data-sharing agreement with the United States, the statutory comity analysis does not apply.[30] However, the CLOUD Act provides that it preserves the common law principles of comity.[31]

Finally, the CLOUD Act provides that providers may disclose to a foreign government that they received a warrant for information stored in that country, so long as the country has executed a data-sharing agreement.[32] That way, the foreign government may

assess compliance with the agreement and intervene diplomatically if the data request is appropriate.[33]

Cases Addressing the CLOUD Act

Since the passage of the CLOUD Act in March 2018, it has been addressed twice by federal courts — first by the Supreme Court in *United States v. Microsoft Corp.*,[34] and most recently by the U.S. District Court for the District of Columbia in *Matter of Leopold*.[35]

United States v. Microsoft Corp.

In *United States v. Microsoft Corp.*, federal law enforcement agents secured a search warrant under the SCA directing Microsoft to disclose the contents of an email account.[36] Microsoft filed a motion to quash, asserting it need not disclose the contents of that account because it was stored in Microsoft's data center in Ireland.[37] The Supreme Court granted certiorari to determine whether, when U.S. law enforcement obtained a warrant under the SCA, a U.S. email provider was required to disclose electronic communications if the provider stored these communications outside of the United States.[38] While the Supreme Court was set to address this issue, the CLOUD Act was enacted, and the government obtained a new warrant pursuant to the amended SCA.[39] The Supreme Court ruled that the passage of the CLOUD Act rendered the case moot because the new warrant applied to information located outside of the United States.[40]

Matter of Leopold

In *Matter of Leopold*, petitioners sought to obtain electronic communications in closed criminal investigations by unsealing federal government surveillance applications and related orders under the SCA and the Pen Register Act (PRA).[41] In relevant part, petitioners moved for reconsideration of the court's conclusion that the First Amendment does not afford a right of access to judicial records relating to SCA warrants.[42] Petitioners argued that the CLOUD Act reflected Congress's intent that SCA warrants equate to traditional search warrants, which do not apply to information stored abroad, as opposed to subpoenas, which do.[43] According to petitioners, if Congress intended for SCA warrants to be akin to subpoenas, the passage of the CLOUD Act would have been superfluous.[44] In denying petitioners' motion for reconsideration, Chief Judge Beryl Howell rejected this argument, concluding that the CLOUD Act's enactment, if anything, reflected Congress's intent to clarify that SCA warrants are functionally equivalent to subpoenas.[45]

III. RECENT RELIANCE ON RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW

The American Law Institute addressed the potential conflict of national laws and interests in its 1987 Restatement (Third) of Foreign Relations Law of the United States. Section 442(1)(c) of the Restatement establishes five factors by which courts should determine whether to issue an order compelling production of foreign-held documents. Those factors include:

- The importance to the investigation or litigation of the documents or information;
- The degree of specificity of the request;
- Whether the information originated in the United States;
- The availability of alternative means of securing the information; and
- The extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.[46]

A leading case with a thorough discussion of factors affecting cross-border discovery is *In re Xarelto (Rivaroxaban) Products Liability Litigation*.[47] In the Eastern District of Louisiana, Judge Eldon Fallon held the Restatement's five-factor approach is one of "numerous mechanisms" courts have devised to comply with *Aerospatiale*, which requires courts to undergo a comity analysis before compelling the production of foreign-held information, but "declined to articulate the factors" that courts should take into account.[48] Judge Fallon stated that a "majority of the lower courts" have adopted the restatement's five-factor approach, based on the Supreme Court's "favorable reference to the Third Restatement in a footnote in [*Aerospatiale*]."[49]

Judge Fallon's Decision in *Xarelto*

In *Xarelto*, Judge Fallon engaged in a robust analysis of principles governing international discovery to determine whether the plaintiff, in complex litigation alleging a pharmaceutical company was liable for failing to warn consumers of alleged defects in a drug it sold, could compel production of personnel files[50] of two employee-deponents located in Germany.[51] Defendants argued that the files did not fall within the scope of Rule 26(b) because the privacy interests of the deponent-employees outweighed plaintiff's interest in discovery.[52] Defendants also objected on the ground that the files contained "personal data," and production of such data would constitute a violation of the German ▸

Data Protection Act — referred to as a "blocking statute."[53]

Before embarking on a comity analysis, Judge Fallon first determined that the applicable German law conflicted with the Federal Rules of Civil Procedure, as employee-deponents' overriding privacy interests outweighed any exceptions in the law that would allow for disclosure.[54] Judge Fallon then applied the Restatement's five-factor comity analysis, even though the Fifth Circuit previously had espoused a three-factor approach.[55] Determining that he would better understand the privacy interests at stake if he could review the documents *in camera*, Judge Fallon limited the analysis to whether the United States' interest in reviewing the documents *in camera* outweighed Germany's interest in protecting the employee-deponents from *in camera* review.[56]

Judge Fallon found that all but the third of the five factors weighed in favor of *in camera* review.[57] More interesting for immediate purposes[58] was how Judge Fallon chose to weigh each factor — guidance for which is lacking in the Restatement. For example, although Judge Fallon found that the third factor — whether the information originated in the United States — weighed in favor of Germany's protective interest, the court ultimately concluded that this factor was of "limited weight" because defendants willingly entered into business in the United States and "significantly benefited from availing [themselves] of [U.S.] markets."[59]

Although Judge Fallon found that the third factor — whether the information originated in the United States — weighed in favor of Germany's protective interest, the court ultimately concluded that this factor was of "limited weight" because defendants willingly entered into business in the United States.

Judge Fallon additionally found that the fifth factor — the balancing of national interests — carried the most weight.[60] This factor, Judge Fallon explained, is most important when it involves national security and state secrecy concerns, which were not at issue in *Xarelto*.[61] Rather, Germany's strong interest in protecting its employees' data was evidenced by a "right [in the German Constitution] to informational self-determination," particularly in the context of the employer-employee relationship; by an amendment to the German Data Protection Act strengthening employee rights; and by an amicus brief submitted by Germany in a similar case, in which Germany urged the court to defer to its privacy laws regarding the disclosure of employee personal data.[62] In light of the quantity and character of plaintiff's requests, the court's willingness to review the documents *in camera*, an existing protective order in the case, the availability for redactions, and the eventual protection of Federal Rules of Evidence 401 and 403 (should the documents be produced after *in camera* review), Judge Fallon ordered the documents be produced for in camera review.[63]

Additional Decisions Addressing the Restatement

Recent decisions that have cited the Restatement favorably when examining an international discovery dispute include the following:

- In *NIKE, Inc. v. Wu*,[64] Chief Judge Colleen McMahon affirmed an order from Magistrate Judge Debra Freeman denying a motion to quash and granting a motion to compel discovery from six nonparty Chinese banks.[65] Both Chief Judge McMahon and Magistrate Judge Freeman followed the Restatement factors, as well as two additional factors considered by the Second Circuit — "hardship of the party facing conflicting legal obligations" and "whether that party has demonstrated good faith in addressing its discovery obligations" — to determine that the information could be subpoenaed without first giving the banks the opportunity to produce it under The Hague convention.66
- In *Salt River Project Agricultural Improvement and Power District v. Trench France SAS*,[67] Judge David Campbell relied on the Restatement factors, as well as two additional factors considered by the Ninth Circuit — "the extent

and the nature of the hardship that inconsistent enforcement would impose" on the foreign state and "the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state" — to determine whether The Hague procedures governing international discovery should apply to the case, and whether the court should appoint a commissioner to oversee discovery in France.[68]

- In *Henry Zoch II v. Daimler, A.G.*,[69] Judge Amos Mazzant granted plaintiff's motion to compel discovery from a German defendant. Finding that four out of the five Restatement factors favored the plaintiff, Judge Mazzant concluded that the balance of interests leaned towards production.[70]
- In *Burrow v. Forjas Taurus S.A.*,[71] Magistrate Judge Edwin Torres granted the plaintiff's motion to compel discovery from the Brazilian defendant. The defendant argued that in Brazil, discovery is "carried out by, and is the responsibility of, the courts, rather than the advocates of the parties," and that therefore discovery should be conducted by a Brazilian judge pursuant to letters rogatory.[72] Judge Torres analyzed the Restatement factors, finding that they ultimately favored the plaintiff.[73]
- In *Connex R.R. LLC v. AXA Corp. Sols. Assurance*,[74] Magistrate Judge Rozella Oliver ruled on the plaintiff railroad's motion to compel production from a French corporation. After reviewing each discovery request and determining that some were valid, Judge Oliver determined that the Restatement factors weighed in favor of the court permitting discovery under the Federal Rules of Civil Procedure, rather than The Hague Convention, despite the existence of a French blocking statute.[75]
- In *Ney v. Owens-Illinois, Inc.*,[76] Magistrate Judge Thomas Rueter denied the plaintiff's motion for sanctions but granted its motion to compel in a limited form because all Restatement factors favored production.[77]
- In *Catalano v. BMW of North America, LLC*,[78] Judge Katherine Forrest granted in part the plaintiff's motion to compel the defendant, a German corporation, to respond to its discovery requests. Judge Forrest stated that the court "conducts a comity analysis to determine whether it *should* order discovery under the Federal Rules and, if so, what the proper scope of such discovery should be."[79] Judge Forrest also reviewed the Restatement factors, ultimately ordering discovery in a limited form through the Federal Rules rather than The Hague process.[80]
- In *Leibovitch v. Islamic Republic of Iran*,[81] Judge Ruben Castillo relied on a comity analysis premised on the Restatement's five factors to deny plaintiffs' motion to compel foreign discovery.[82]
- In *Laydon v. Mizuho Bank, Ltd.*,[83] Magistrate Judge Henry Pitman applied the Restatement's five-factor test and an additional two factors proscribed by the Second Circuit — "the hardship of compliance on the party or witness from whom discovery is sought" and "the good faith of the party resisting discovery" — to deny a motion to compel international discovery production on comity grounds.[84]

IV. GENERAL DATA PROTECTION REGULATION (GDPR)

For years, litigants and judges have grappled with the complexities of cross-border discovery pursuant to data protection regimes in Europe.[85] The GDPR, which took effect on May 25, 2018, is considered the most important change in European data privacy regulation. Designed to harmonize data privacy laws across Europe, its requirements apply to each member state of the European Union (EU). In general, the GDPR addresses how businesses and organizations must handle the personal data of individuals in the EU and provides such individuals with rights and control over their personal information. This article addresses only the transfer of personal information, as defined by GDPR.[86]

"Personal data" is defined very broadly by the GDPR. Any information relating to a natural person who can be identified, *directly or indirectly*, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person, is considered "personal data."[87] Even an individual's email address or location data, if it can identify a person, is therefore governed by the GDPR. Violations of the GDPR may subject businesses to significant administrative penalties of up to €20 million or four percent of a business's annual worldwide revenue, whichever is greater.

The transfer of personal data outside the EU is governed by Article 48 of the GDPR. The European Commission makes clear that the mere fact that a foreign court issued an order for the transfer of information outside ▸

the EU does not make the transfer lawful under the GDPR. In the European Commission's view, any domestic law that creates transfer obligations should be applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity.[88]

Article 48 of the GDPR allows for a transfer in response to third-country authorities if in accord with Articles 44 through 50, which govern the transfer of personal data to third countries or international organizations.

Article 48 expressly addresses situations in which a foreign tribunal or administrative body orders a transfer that is not otherwise permitted by the GDPR. It makes international agreements, such as mutual legal assistance treaties (MLATs), the preferred option for transfers. Alternatively, transfer of personal data from the EU may be completed using an approved transfer mechanism under Article 46, such as the EU-U.S. Privacy Shield, standard data-protection clauses, or binding corporate rules, as described in Article 47. Only when none of these transfer mechanisms is applicable is a transfer of personal data allowable under certain conditions identified in Article 49.

The European Data Protection Board (EDPB) recently adopted guidelines interpreting Article 49.[89] Those guidelines are instructive in laying the foundation for cross-border transfer under the following conditions.

Transfer for the Establishment, Exercise, or Defense of Legal Claims

Under Article 49(1)(e), personal data may be transferred if it is "occasional and necessary in relation to a contract or a legal claim, regardless of whether in a judicial procedure or whether in an administrative or any out-of-court procedure, including procedures before regulatory bodies." Transfer under this derogation could address criminal or administrative investigations where the transfer of data may be necessary to defend oneself. It is also possible that data transfers in connection with pretrial discovery may fall within this derogation.[90]

It is important to note, however, that the data transfer may only take place when it is necessary for the establishment, exercise, or defense of the legal claim in question, requiring a close and substantial connection between the data in question and the specific establishment, exercise, or defense of the legal position. Only personal data that is actually necessary can be transferred and disclosed. The need for personal data must also be relevant and limited to what is necessary in relation to the purposes for which the data is processed. An assessment also should be made as to whether anonymized or pseudonymized data would be sufficient.[91]

> The European Commission makes clear that the mere fact that a foreign court issued an order for the transfer of information outside the EU does not make the transfer lawful under the GDPR.

Transfer for Important Reasons of Public Interest

Article 49(1)(d) addresses the public interest derogation, which applies when data transfers are allowed for important public interest purposes. Such purposes include the spirit of reciprocity for international cooperation, as made clear by EU law, the law of the relevant member state, or an international agreement or convention where the EU or the member states are a party to that agreement or convention.[92]

Transfer Based on Consent

Transfers may also be based on consent under Article 49(1)(a), but reliance on consent is difficult for a number of reasons. First, consent must be obtained from the individual(s) whose personal data may be transferred. Consent cannot be obtained from the entity holding the data. Second, consent must be explicit, informed, and voluntary, which may be a subjective determination made on a case-by-case basis. For example, consent from an employee may be viewed as coerced because employees cannot freely refuse an employer's request. Finally, under the GDPR, consent can be withdrawn by the individual at any time.

Limited Transfer for Compelling Legitimate Interests of the Data Transferring Party

Reliance on Article 49(1)(2) for a limited transfer of individual data in a case of compelling, legitimate interests of the data transferring party is considered by the EDPB to be a derogation of last resort.[93] It only applies where

no other transfer mechanism can be used and under a number of very specific, expressly enumerated conditions, where transfer is necessary for the purposes of compelling, legitimate interests. The following criteria must be met:

- [T]he transfer is not repetitive and concerns only a limited number of data subjects;
- the transfer is necessary for compelling, legitimate interests of the data transferring entity that are not overridden by the interests or rights and freedoms of the data subject;
- the transferring entity has assessed all the circumstances surrounding the data transfer and has provided suitable safeguards;
- the relevant data protection authority has been informed of the transfer; and
- the data subjects have been informed of the intended data transfer.[94]

The ramifications of the *Vitamin C* case, as applied to the GDPR, are yet to be developed by U.S. courts. If a judge determines under Rule 44.1 that the GDPR is applicable, attorneys and judges in the United States will be faced with determining how the GDPR should apply to disputes in the United States.

Attorneys who practice in this area will be looking for interpretations and practical application as cross-border and transfer disputes arise. Further guidelines will be promulgated, and administrative law and court decisions will follow. In the interim, the following guidelines may be helpful where the transfer of personal data protected by the GDPR is appropriate:

- Retain qualified counsel in the country in which the data is located.
- Limit requests for personal data to what is necessary for introduction at trial, rather than merely pretrial discovery, as is common in the United States.
- Anonymize personal data where appropriate and if not appropriate, attempt to pseudonymize personal data.
- Consider processing and hosting personal data in the EU.
- Determine if personal data can be transferred under one of the safeguard mechanisms (EU-US privacy shield, standard data protection clauses, or binding corporate rules).
- Identify relevant public interest factors that make the discovery appropriate and in the public interest, as opposed to merely serving the interests of one party or another.

V. WORK PRODUCT OF THE SEDONA CONFERENCE, THE FEDERAL JUDICIAL CENTER, AND THE ELECTRONIC DISCOVERY REFERENCE MODEL ("EDRM")

Judges facing these issues in civil litigation need to consider the impact of the *Vitamin C* decision and Rule 44.1, as foreign law deserves to be considered. In doing so, judges, whether state or federal, can find a great deal of authority in the Federal Judicial Center's handbook *Discovery in International Civil Litigation – A Guide for Judges*, published in 2015, as well as the cases reviewed above and cases decided after the preparation of this article.

In addition, the ongoing excellent work product of two independent organizations should be considered. First, as mentioned in the earlier *Judicature* article, the Sedona Conference, a highly regarded "think tank" that sponsors discussions on legal issues and whose mission is "to move the law forward in reasoned and just ways," has developed general "principles" for lawyers and judges to deal with cross-border disputes. Because of the GDPR, Sedona's Working Group 6 has initiated a revision of its principles for U.S. judges and lawyers, as well as overseas data-protection authorities, to use in resolving cross-border and data-transfer disputes. Sedona has developed a "transitional" statement of more specific principles, largely because of the anticipated impact of the GDPR,[95] entitled *International Litigation Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*.[96] These principles, which Sedona anticipates completing during calendar year 2020, discuss in greater detail, with case citations, appropriate approaches towards trying to resolve disputes. The Sedona Principles advocate a "[t]hree-[s]tage [a]pproach for [h]armonization of U.S. [d]iscovery and [d]ata [p]rotection [l]aws" as follows:

- [A] stipulation by the parties or an order from the U.S. court to extend special protections to data covered by Data Protection Laws;
- a scheduling order by the U.S. court that phases discovery to permit time to implement data protection processes and to determine whether the same or substantially similar information is available from non-protected sources; and
- implementation of a legitimization plan by the parties to maximize simultaneous compliance with the foreign data protection law and the U.S. discovery obligation.[97]

Another group, EDRM, part of the Bolch Judicial Institute at Duke Law School (which also publishes *Judicature*), describes itself as "an international professional e-discovery organization," and is developing "best practices" guidance for conducting data transfers between the EU and the United States. ▸

EDRM, along with many law firms with international practices, published a very detailed description of the GDPR entitled "Decoding GDPR" (available on its website EDRM.com and published in the Spring 2018 edition of *Judicature*), which clarifies terms used in the GDPR that have caused confusion.

VI. CONCLUSION

When facing disputes where the information sought includes personal information under the GDPR or is located in a foreign country with restrictions on data transfer, U.S. federal and state judges will have to determine what law to follow in the absence of an agreement by the parties. If the judge chooses to follow U.S. law, the resolution may follow traditional U.S.-based discovery principles but runs the risk that businesses forced to comply with the court's order would be in violation of the GDPR or another country's laws and potentially subject to significant administrative penalties. Moreover, if the judge chooses to follow the GDPR or other foreign law and orders production of documents containing the personal information of EU residents, compliance may be possible, but only after the detailed requirements of the GDPR are satisfied — often with substantial time and expense. As discussed in the prior article, use of The Hague Convention procedures may be preferable or necessary.

Internationally acceptable principles, as Sedona is developing, that are designed to promote the proverbial "search for the truth" with appropriate safeguards for the protection of individual privacy, are needed.

SANDRA JESKIE is a partner in the Philadelphia and San Diego offices of Duane Morris LLP.

MICHAEL M. BAYLSON is a senior judge of the U.S. District Court for the Eastern District of Pennsylvania. The authors appreciate the substantial assistance of Judge Baylson's law clerks, Samantha Weiss, Elizabeth Coyne, and Martha Guarnieri, in the preparation of this article.

1 138 S. Ct. 1865 (2018).

2 *Id.* at 1867

3 *Id.*

4 *Id.* at 1871.

5 *In re Vitamin C Antitrust Litigation*, 837 F.3d 175 (2d Cir. 2016), *vacated*, 138 S. Ct. 1865 (2018).

6 *Aerospatiale v. United States,* 482 U.S. 522 (1987).

7 A law review article by Professor Geoffrey Sant conducted a statistical analysis of whether there was a pro-forum bias in courts applying *Aerospatiale*, as predicted by the dissenting justices. *See* Geoffrey Sant, *Court-Ordered Law Breaking U.S. Courts Increasingly Order the Violation of Foreign Law*, 81 Brook. L. Rev. 181, 182 (2015). Professor Sant analyzed the opinions of every trial court to apply *Aerospatiale* and found that its factors were "overwhelmingly resolved in favor of violating foreign law." *Id.* at 191.

8 *In re Vitamin C,* 138 S. Ct. at 1869.

9 *Id.* at 1873–74.

10 For example, in *Peterson Energia Inversora S.A.U. v. Argentine Republic*, 895 F.3d 194 (2d Cir. 2018), *petition for cert. filed,* 2018 WL 5802394 (Nov. 2018) (No. 18-581), a shareholder brought suit against Argentina and an Argentinian corporation when Argentina expropriated 51% of the company shares. Argentina regained control of 51% of the company allegedly under the expropriation law and canceled a previously scheduled dividend payment promised during the IPO. *Id.* at 199–203. After determining that his court had jurisdiction over the dispute, Judge Chin on the Second Circuit analyzed Argentina's law in the context of the dispute. *Id.* at 207. Argentina produced an expert witness who opined that the corporation's bylaws could not "validly restrict, limit, or in any way affect the exercise of sovereign powers of the National Government in general and regarding expropriations in particular." *Id.* at 208. The Court cited *Vitamin C* and found that "even according respectful consideration to Argentina's views, we do not find that the expert's interpretation supports Argentina's argument." *Id.* at 208. Ultimately, the Second Circuit affirmed the district court's denial of the motion to dismiss under the FSIA and denied the appeal under the Act of State Doctrine.

Similarly, in *In re: Chinese-Manufactured Drywall Products Liability Litigation*, 2018 WL 4816135 at *7 (E.D. La. 2018), Judge Fallon denied an interlocutory appeal of an order granting one defendant Chinese drywall manufacturer's motion to dismiss pursuant to the FSIA. The judge noted that *Vitamin C* "is inapplicable to this case, as the Court did not simply accept a representation from the Chinese Government as dispositive; rather, it concluded that the [plaintiffs] had failed to present evidence demonstrating that [this defendant] was entitled to immunity under the FSIA." *Id.* In *A.O.A. v. Ira L. Rennert*, 2018 WL 5013854 at *19–23 (E.D. Mo. 2018), Judge Perry declined to grant Peruvian Defendant's 12(b)(6) motion on the basis of "international comity" in an action by Peruvian children who lived near a smelting and refining complex.

11 739 F. App'x 674, 678–79 (2d Cir. 2018).

12 *Id.*

13 *See* Stephen P. Mulligan, Cong. Research Serv., LSB10125, Law Enforcement Access to Overseas Data Under the CLOUD Act 1 (2018) (hereinafter "Cong. Research Serv."); 164 Cong. Rec. S595-07 (daily ed. Feb. 5, 2018) (statement of Sen. Hatch); *The Center for Strategic and International Studies [CSIS] Holds a Discussion on the Clarifying Lawful Overseas Use of Data Act*, 2018 WL 2416500 at 2, 6 (May 24, 2018) (statements of Sujit Raman, Assoc. Deputy Att'y Gen. and James Andrew Lewis, Sr. Vice Pres. CSIS) (hereinafter "CSIS Discussion").

14 Cong. Research Serv. at 1; 164 Cong. Rec. S595-07.

15 164 Cong. Rec. S595-07; CSIS Discussion at 7.

16 Pub. L. No. 115-141.

17 CSIS Discussion at 6, 8 ("As a whole[,] the CLOUD Act addresses both the conflicts that may arise when the United States seeks data abroad and wh[en] our foreign allies seek data located in the United States for law enforcement purposes."); Cong. Research Serv. at 1. A very helpful article published by the law firm that represented Microsoft in *United States v. Microsoft;* Richard Loeb et al., *The CLOUD Act, Explained: Cyber, Privacy & Data Innovation Alert*, Orrick, Herrington & Sutcliff LLP (Apr. 6, 2018), https://www.orrick.com/Insights/2018/04/The-CLOUD-Act-Explained.

18 18 U.S.C. § 2701 *et seq.* Sections 2701–03 were amended by the Cybersecurity and Infrastructure Security Agency Act of 2018, Pub. L. No. 115-278, 132 Stat. 4168 (2018), which was enacted on Nov. 16, 2018. The enactment of the Cybersecurity and Infrastructure Security Agency Act does not affect the substance of this article.

19 Cong. Research Serv. at 1. The CLOUD Act expanded only the geographic reach of the SCA, not the entities or data subject to warrants under the SCA. *See* Loeb et al., *supra* note 17.

20 *See* Cong. Research Serv. at 2; *see also* CSIS Discussion at 8.

21 CSIS Discussion at 6.

[22] Cong. Research Serv. at 2; CSIS Discussion at 7–8.

[23] CSIS Discussion at 8.

[24] Cong. Research Serv. at 2; CSIS Discussion at 8.

[25] Cong. Research Serv. at 2; 164 Cong. Rec. S595-07.

[26] Cong. Research Serv. at 2.

[27] *Id.* at 1.

[28] *See* Brief for E-Discovery Institute et al. as Amici Curiae Supporting Neither Party, 21–30, *United States v. Microsoft,* 138 S. Ct. 1186 (2018) (No. 17-2).

[29] Cong. Research Serv. at 2.

[30] *Id.*

[31] *Id.*

[32] 164 Cong. Rec. S595-07.

[33] *Id.*

[34] 138 S. Ct. 1186 (2018) (per curiam).

[35] 2018 WL 3941947 (D.D.C. Aug. 16, 2018), *appeal filed*, 18-5276 (D.C. Cir. Sept. 19, 2018).

[36] 138 S. Ct. at 1188.

[37] *Id.*

[38] *Id.*

[39] *See* Cong. Research Serv. at 1.

[40] *Id.* at 1188.

[41] 2018 WL 3941947 at *1.

[42] *Id.* at *2–3.

[43] *Id.* at *4–6.

[44] *Id.* at *6.

[45] *Id.*

[46] Restatement (Third) of Foreign Relations Law § 442(1)(c) (West Oct. 2018 update).

[47] 2016 WL 3923873 (E.D. La. July 21, 2016).

[48] *Id.* at *7 (explaining that different circuits have adopted three-, four-, or even seven-factor tests).

[49] *Id.*; *see Aerospatiale*, 482 U.S. at 544 n.28 (citing Restatement Section 437, a predecessor to Section 442).

[50] Personnel files are those files "maintained by the Human Resources department of an employer and are likely to contain confidential employer evaluations which the employee may have never seen. The personnel file may also include sensitive information such as salary, physical or mental health data, alimony and child support garnishment, tax records, and drug test results." *Id.* at *2 (internal citations omitted).

[51] 2016 WL 3923873 at *2.

[52] The court disposed of this first argument in an earlier decision that "appropriately tailored the scale of production by balancing the relevancy and importance of the material against employee privacy interests." *Id.* At the time of that decision, Judge Fallon declined to rule on the German law issue because the parties had not sufficiently briefed whether a "blocking statute" could trump the Federal Rules of Civil Procedure. *Id.* Defendants later revived the argument, which is the subject of the decision discussed here. *Id.*

[53] *Id.*

[54] *Id.* at *8–13. Noting that the German law allowed the data to be transferred with the free decision of the data holder, Judge Fallon explained that a "good faith request" from defendants for the information would be appropriate, considering the sophisticated, high level of the employee-deponents and their capacity to meaningfully provide consent. *Id.* at *11–12.

[55] *Id.* at *7, *14 (noting that "[d]istrict courts in the Fifth Circuit have consistently implemented this command by applying the five factors of the Third Restatement," despite the Fifth Circuit's command that they need only consider scrutiny of the facts of each particular case, sovereign interests, and the likelihood that resorting to foreign discovery procedures would prove effective) (citing *In re Anschuetz & Co., GmbH*, 838 F.2d 1362, 1364 (5th Cir. 1988)).

[56] 2016 WL 3923873 at *14.

[57] *Id.* at *14–19.

[58] Also of potential interest, Judge Fallon explained that the first factor — the importance of the requested discovery — is subject to various formulations. While some circuits articulate an "exceedingly high" bar, others apply an "absolutely essential" standard, and still others apply a "critical or compelling" standard. *Id.* at *14–15. In the absence of guidance from the Fifth Circuit, Judge Fallon applied the "critical or compelling" standard. *Id.*

[59] *Id.* at *16.

[60] *Id.* at *17 (citing *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1476 (9th Cir. 1992)).

[61] 2016 WL 3923873 at *17.

[62] *Id.* at *13, *17.

[63] *Id.* at *17–19. The judge did not seriously consider defendants' contention that they faced civil and criminal penalties under the German law if they produced the documents because defendants had failed to meet their burden of showing that Germany enforced the law against parties that revealed documents pursuant to a U.S. court order. *Id.* at *18.

[64] 2018 WL 6056259 at *11–15 (S.D.N.Y. Nov. 19, 2018).

[65] *Id.* at *1.

[66] *Id.* at *11–12 (citations omitted).

[67] 303 F. Supp. 3d 1004 (D. Ariz. 2018).

[68] *Id.* at 1007.

[69] 2017 WL 5177959 (E.D. Tex. Nov. 8, 2017).

[70] *Id.* at *4–6.

[71] 2017 WL 2620067 (S.D. Fla. June 16, 2017).

[72] *Id.* at *3.

[73] *Id.* at *7.

[74] 2017 WL 3433542 at *3 (C.D. Cal. Feb. 22, 2017).

[75] *Id.* at *15.

[76] 2016 WL 7116015 at *1 (E.D. Pa. Dec. 6, 2016).

[77] *Id.* at *5.

[78] 2016 WL 3406125 at *7 (S.D.N.Y. June 16, 2016).

[79] *Id.* at *7.

[80] *Id.* at *7–9.

[81] 188 F. Supp. 3d 734 (N.D. Ill. 2016).

[82] *Id.* at 757.

[83] 183 F. Supp. 3d 409 (S.D.N.Y. 2016).

[84] *Id.* at 419–20.

[85] By way of background, the member states of the EU have, for many years, imposed restrictions on data transfers, usually enforced by a multinational entity known as the "Article 29 Working Party," which has been replaced by another entity, pursuant to the GDPR, called the "European Data Protection Board" (EDPB).

[86] National law may also contain so-called "blocking statutes" that prohibit or restrict the transfer of personal data to foreign courts and vary from country to country; they are not addressed by this article. Under the GDPR, the term "cross-border" refers exclusively to data transfers within the EU.

[87] Commission Regulation 2016/679, 2016 O.J. (L'119) 1(EU), art. 4(1).

[88] The European Commission, acting on behalf of the EU, filed an amicus brief in the *Microsoft* case. Although it did not take any specific position on the interpretation of the dispute between the United States Department of Justice and Microsoft, it urged that if the Supreme Court were intending to create any type of cross-border discovery obligations, they should be "applied and interpreted in a manner that is mindful of the restrictions of international law and considerations of international comity." Brief of the European Commission on Behalf of the European Union as *Amicus Curiae* in Support of Neither Party at 14, *United States v. Microsoft Corp.*, 138 S. Ct. 1186 (Dec. 13, 2017) (No. 17-2). The EU also asked the Supreme Court to "consider EU domestic law as it pertains to searches of data stored in the European Union." *Id.*

[89] *See* Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679, Adopted 25 May 2018 (hereinafter "EDPB Article 49 Guidelines").

[90] EDPB Article 49 Guidelines at 11.

[91] *Id.*

[92] *Id.* at 11.

[93] *Id.* at 14.

[94] Art. 49(1)(2).

[95] In a separate but related publication, Sedona also proposed *International Principles for Addressing Data Protection in Cross-Border, Government and Internal Investigations: Principles, Commentary and Best Practices*, dated May 2018 and published at 19 Sedona Conf. J. 557 (2018), which advocates a set of principles to protect individual rights and privacy, yet allow appropriate government investigations to proceed under standards that could be accepted on an international basis.

[96] The Sedona Conference Working Group on International Electronic Information Management, Discovery, and Disclosure (WG6), *International Litigation Principles on Discovery, Disclosure & Data Protection in Civil Litigation* (Transitional Edition) (Jan. 2017).

[97] *Id.* at 6–7.