History and Achievements of The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6)

By The Sedona Conference®[1]

I. History of The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6)

The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6) was founded in 2005 to bring together some of the world's finest attorneys, privacy and compliance officers, technical consultants, records managers, academics and jurists to facilitate a consensus approach to law and policy issues in the areas of cross-border discovery and data privacy and protection.

The concept of WG6 was conceived at the October 17, 2003 annual meeting of The Sedona Conference® Working Group on Electronic Documents Retention and Production (WG1) in Santa Fe, New Mexico. At that meeting, M. James Daley, Tim Opsitnick, Paul Robertson and Susan Wortzman gave a presentation entitled "The International Dimensions of the Electronic Discovery Dilemma" which highlighted the tension between U.S. style electronic discovery and global data privacy regulations, such as those imposed by the EU Data Protection Directive[2] and others.

After considerable dialogue and discussion, The Sedona Conference® recognized that a separate working group dedicated to this issue could play an important role, given the rapid proliferation of cross-border litigation and regulatory investigations, the increasing

[1] The Sedona Conference® acknowledges the editorial contributions of M. James Daley, Amor Esteban, and Kenneth J. Withers to this essay.

[2] See Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the fee movement of such data, issued 24 October 1995.

interdependence of countries due to commerce and market expansion, and the rapid development of international records retention, e-discovery and e-disclosure rules .

Thereafter, in early 2005, after additional study and dialogue, , The Sedona Conference® established its Working Group on International Electronic Information Management, Discovery and Disclosure (WG6), whose mission is to facilitate a dialogue and help develop a framework and principles for harmonizing cross-border discovery of electronically-stored information (ESI) and data privacy.

On July 14-17, 2005, WG6 held its first international conference in England at Clare College, Cambridge University. There, thought leaders from Europe, Asia and North America converged to identify and illuminate the nature and scope of the challenges faced in harmonizing cross-border discovery with data privacy.

On September 28-30, 2006, WG6 held its second international conference at the Euroforum in El Escorial, Spain, which continued the international dialogue and identified the need for a global framework to assist corporations, counsel and courts in managing these issues.

Building on additional background work, WG6 held its third international conference on December 6-7, 2007 at the Fairmont Hamilton in Bermuda. There, WG6 members outlined the basic contours of a framework document designed to identify the component parts of the cross-border discovery/privacy dilemma.

Considerable work followed by WG6 members in 2008, culminating with the publication in August 2008 of the public comment draft of *The Sedona Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and Discovery (2008).*[3] This work represents the collective input of

[3] THE SEDONA CONFERENCE®, THE SEDONA CONFERENCE® FRAMEWORK FOR ANALYSIS OF CROSS-BORDER DISCOVERY CONFLICTS: A PRACTICAL GUIDE TO NAVIGATING THE COMPETING CURRENTS OF INTERNATIONAL

123 members of WG6 from countries as diverse as Australia, Barbados, Brazil, Canada, China, England & Wales, France, Germany, Japan, Netherlands, Spain, Switzerland, Sweden, the United Kingdom and the United States, among others.

In addition to *The Sedona Framework*, WG6 also published a publically-available wiki entitled *"The Sedona Conference® Overview of International E-Discovery, Data Privacy and Disclosure Requirements"* [4] which provides an overview of the electronic discovery and data privacy landscape in selected countries. Together, these WG6 publications are designed to provide a framework for constructive dialogue about how to harmonize cross-border discovery with data privacy regulations.

On February 11, 2009, the Article 29 Data Protection Working Party (the "WP") issued its "Working Document 1/2009 on pre-trial discovery for cross border civil litigation" (also known as "WP158"). [5] In WP158, the Working Party acknowledged the helpfulness of *The Sedona Framework*, noting that it sets out "relevant factors" that U.S. courts should consider "when determining the scope of cross border discovery obligations."[6]

The fourth WG6 international conference was held June 5-7, 2009 at the Hotel Arts in Barcelona, Spain. This conference brought into sharper focus many of the practical challenges in harmonizing cross-border discovery and data privacy. The EU Article 29 Working Party's Document 158, as well as the WG6 *Framework* document was a major focus of the conference.

DATA PRIVACY & E-DISCOVERY (2008). Hereinafter "*The Sedona Framework*"; and see www.thesedonaconference.org for a free PDF download of this document.

[4] *See* THE SEDONA CONFERENCE® , THE SEDONA CONFERENCE® OVERVIEW OF INTERNATIONAL E-DISCOVERY, DATA PRIVACY AND DISCLOSURE REQUIREMENTS (2009), a free PDF download of which is available at www.thesedonaconference.org, and a web version available at https://www.socialtext.net/wg-6/.

[5] *See* Article 29 Data Protection Working Party, *Working Document 1/2009 on pre-trial discovery for cross border civil litigation*, 00339/09/EN, WP 158, adopted 11 Feb. 2009

[6] *See* www.thesedonaconference.org to obtain a free PDF download of this framework document.

Following the Barcelona conference, on October 30, 2009, WG6 provided its formal response to WP 158, which highlighted areas of common ground, and areas where the need for further dialogue was recognized—such as the feasibility of anonymization of data and use Hague Convention procedures.

Most recently, on September 15-17, 2010, the fifth WG6 international conference was held in Washington, D.C., at the Hyatt Regency hotel. This conference built on a solid foundation of dialogue in prior years, and identified the need for global principles that, when combined with the *WG6 Framework*, might assist corporations, practitioners and courts in unraveling the "Gordian Knot" of cross-border discovery and data privacy.[7]

II. The "Catch 22": Differing Notions of Jurisprudence, Differing Notions of Disclosure and Discovery, and Differing Notions of Privacy

Cultural and legal notions of data privacy and protection differ greatly between the U.S. and most of the rest of the world. The EU and many other countries embrace a global approach to data protection and privacy, based upon the conviction that is a fundamental human right. On the other hand, the U.S. takes a "patchwork quilt" approach to commercial data privacy, with a variety of different federal and state statutes addressing specific types of personal data.

Such U.S. privacy statutes are aimed at protecting personal medical and health information, Health Insurance Portability and Accountability Act (HIPAA),[8] consumer credit information through the Fair Credit Reporting Act (FCRA)[9], financial data through the Gramm-

[7] *See* Moze Cowper & Amor Esteban, *E-Discovery, Privacy, And The Transfer Of Data Across Borders: Proposed Solutions For Cutting The Gordian Knot*, 10 SEDONA CONF. J. 263 (Fall 2009).

[8] Health Insurance Portability and Accountability Act,. Pub. L. No. 104-191, §§ 262, 264; 45 C.F.R. §§ 160-164. PL 104-191, 110 Stat 1936 (August 21, 1996); 45 C.F.R. §§ 160-164

[9] Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq.*

Leach Bliley Act (GLBA)[10], information on employee disabilities through the Americans with Disabilities Act (ADA)[11], data on children through the Children's Online Privacy Protection Act (COPPA)[12], driver's license information through the Driver's Privacy Protection Act (DPPA)[13], and educational records through the Family Education Rights and Privacy Act (FERPA)[14], among others. In litigation, private communications are also protected in the U.S. by privileges which are based upon personal and professional relationships (e.g., attorney-client, priest-penitent, marital, doctor-patient). The conflict involved in global data privacy and protection can only be addressed if these differences are understood.

In addition to differing notions and foundations for data protection and privacy, the U.S. notion of discovery and disclosure of information as part of its common law system of jurisprudence differs greatly from most of the rest of the world. The U.S. justice system suggests that "full and searching" discovery is needed in order to achieve what it calls "the truth, the whole truth, and nothing but the truth." And in the U.S., considerable importance is given to transparency and public access to the records of court proceedings. Indeed, in the United States there is a constitutionally protected right to a "public trial," as well as "freedom of speech" protections that may be in conflict with the constitutional protections of other countries. In contrast to the U.S., civil code jurisdictions in the EU and elsewhere often give greater weight to data privacy and protection considerations than to an individual litigant's need for evidence in the possession or control of an adversary.

---

[10] Financial Services Modernization Act of 1999, Financial Services Modernization Act of 1999, (Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999).

[11] Americans with Disabilities Act, Pub.L. No. 101-336, 42 U.S.C. § 12101, enacted July 26, 1990.

[12] Children's Online Privacy Protection Act, 15 U.S.C. § 6501–6506 (Pub.L. No. 105-277), enacted October 21, 1998.

[13] Drivers Privacy Protection Act, Public Law No. 103-322 codified as amended by Public Law 106-69, 18 U.S.C. § 2721, *et seq*. (October 23, 2000)

[14] The Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g; 34 C.F.R. § 99.1.

These differing legal and cultural notions come to a head in the context of cross-border transfers of personal data for the purpose of litigation or regulatory proceedings. The transfer of data raises numerous issues, most particularly the conflict between the need to gather relevant information from other jurisdictions and the data privacy regulations that seek to prohibit such discovery.

In the face of these sometimes-conflicting priorities, clients, courts and counsel are expected to understand how electronic information is stored and received, how to apply foreign standards and rules procedures for civil discovery, and how to balance them with differing and seemingly irreconcilable notions of data privacy.

This challenge is complicated by significant linguistic differences that create confusion and undermine a common understanding of certain key terms, such as "personal data" and "processing."

a. Different understanding and scope of "personal data"

In the United States, the category of "personal data" protected from processing would ordinarily be limited to something very unique to a person with a high degree of sensitivity, such as social security numbers or medical records. In fact, most U.S. regulations regarding protection of personal data have been grounded in concerns about consumer protection and identity theft, whereas in the EU and elsewhere, regulations codify concerns for what is deemed a fundamental human right. Accordingly, the EU Directive, for example, protects all types of personal data[15] from processing, including e-mails identifying authors or recipients.[16]

[15] See EU Directive, Article 2(a).

[16] See Article 29 Working Party Opinion 4/2007 on the concept of personal data, 20 June 20007 (WP 136).

b. Different definition and scope of "processing"

In the United States, the concept of data processing implies a formal, large-scale handling and labeling of data. The European Union, however, considers virtually any operation conducted on personal data outside the ordinary course of its use by a data subject to constitute "processing" of that data.[17] The EU Directive creates substantive rights to fairness, legality, accuracy, relevance and security that must be observed in any processing or transfer of personal data.

c. Different notions of disclosure and discovery

In the United States and other common law countries, documents and data are discoverable if they are reasonably calculated to lead to admissible evidence. Parties can be severely sanctioned for failing to preserve or produce relevant materials.

Unlike common law pretrial practice, many civil law jurisdictions prohibit disclosure of evidence beyond what is needed for the scope of trial. In these civil code countries (which vastly outnumber common law countries), discovery is very limited. Privacy laws prohibit the processing of personal data, and individuals or organizations can be penalized for such action.

When seeking to resolve discovery disputes, generally, the law of the country where the "data controller" is established will apply to the question of whether the relevant personal data can be legitimately "processed." It is possible that within one company, many sets of laws will apply to data residing in different countries.

[17] See EU Directive, Article 2(b).

d. Different approaches to data privacy and protection

Even when faced with discovery orders from U.S. courts, the trend in litigation has been for other countries to restrict cross-border discovery through the application of blocking statutes and data privacy regulations. And although there is an except in the EU Directive for transfers "which are necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims,[18] the Article 29 Working Party has narrowly interpreted this exception, and, instead, favors the use of the Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters as the preferred procedural framework for such transfers.

Interestingly, in 2004, the European Commission adopted Council Regulation No. 1206/2001 of May 28, 2001 on cooperation between the courts of the Member States in the taking of evidence in civil or commercial matters, which was inspired by The Hague Convention. The purpose of this measure was to harmonize the transmission and execution of such requests between EU Member States. Nevertheless, there remains considerable room for country-specific variation.

i. *European Union Data Protection Directive*

While data protection regulations differ broadly across the globe, the EU Directive provides somewhat of a model as to the kind of processing and transfer restrictions that are included in most of these regulations. As such, it is a useful example to use in evaluation of common privacy principles underlying these regulations.

[18] See EU Directive, Article 26(1)(d).

The European Union Data Protection Directive was published on October 24, 1995. The starting premise under the EU Data Protection Directive is that data processing can only occur under certain circumstances where the interests of the data subject are protected and transfers of personal data are prohibited unless the receiving country provides adequate protection. As a rule of thumb, data transfer is permitted between Member States and prohibited outside of Member States. Each Member State has implemented the data protection directive in different ways—some have given additional layers of protection to personal data.

ii. Blocking Statutes

In addition to the EU Data Protection Directive, several countries have enacted Blocking Statutes. These statutes prohibit the transfer of different types of information across country borders, and were generally enacted with the goal of protecting sovereignty and commercial interests from interference by foreign states. Violation can result in civil or criminal penalties. For example, in January 2008, in the *In Re Christopher X* case, a French lawyer was convicted of violating the French blocking statute[19] for seeking to obtain information from a French resident that related to a lawsuit brought in the United States.

iii. *Exceptions Allowing for Cross-Border Data Transfers*

Litigants might still achieve success in requesting cross-border data transfers if they can fall within one of the following exceptions:[20]

- Consent: given prior to the transfer, unambiguous, specific to the transfer or category of transfers, freely given, and informed.

[19] *In re Advocat "Christopher X,"* Cour de Cassation, Chambre Criminelle (Supreme Court of France), 12 Dec. 2007, 07-83.228.

[20] See EU Directive, Article 26(1)(d).

- Safe Harbor: organizations that regularly send personal information to the United States can join a self-regulatory privacy program or develop its own self-regulatory privacy policy that conforms to the requirements of Safe Harbor, and must annually certify that it is following Safe Harbor requirements. This approach offers advantages and disadvantages.
- Model Contractual Claims: European Commission developed scheme allowing international transfers of personal data where both parties agree to be bound by a set of clauses set to ensure that control over data is secure. This approach also offers advantages and disadvantages.
- Binding Corporate Rules: organizations with complex corporate structures and multiple cross-border data transfers can implement rules that ensure adequacy by adoption of binding codes of conduct by the organization, which must then be approved by DPAs. No company has yet achieved full approval by all relevant DPAs.

iv. The Hague Convention on Taking of Evidence Abroad

The Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters instituted the practice of "letters of request" from one nation to an authority in another nation requesting assistance in obtaining information from within its borders. Such a request may be ignored or denied if restricted by privilege or blocking statutes, or where under Article 23, countries such as France, Germany, Italy and Spain have declared that they will not allow discovery of any information, regardless of relevance, if the information is sought in relation to a foreign proceeding.

A minority of courts have held that parties engaged in cross-border discovery must utilize the procedures of the Hague Convention, through which several countries attempted to

somewhat restrict common-law style pretrial discovery. As noted below, however, United States Courts have generally declined to require use of the Hague Convention as either the exclusive or even primary means of cross-border discovery.[21]

III. The Production in U.S. Litigation of Discovery Subject to Foreign Data Protection Laws: The Sedona Conference's Proposed Approach for Harmonization

a. The Role of Discovery in U.S. Litigation

European views of U.S. litigation emanate in part from the unfamiliarity with the requirement to produce relevant information demanded by an adversary and the broad scope of that requirement; an obligation that is a hallmark of U.S. jurisprudence.[22] Unlike Civil Law countries, the exchange of information between parties to a lawsuit in America is managed primarily by the parties themselves. This exchange of information, or what is known as "discovery," is required by statutes and court rules, as interpreted by the decisions of appellate courts. Meanwhile, trial courts, where the matter is being litigated, are not inclined to become involved in discovery beyond ministerial case administration unless disagreement between the parties requires the court to intervene. In those instances, courts resolve issues such as whether the information sought is relevant to the claims and defenses of the case; whether the burden and

[21] See *Societe Nationale Industrielle Aerospatiale v. United States District Court of the Southern District of Iowa*, 482 U.S. 522 (1987).

[22] United States jurisprudence emanates from a wide variety of sources. There is federal law and a federal judiciary that come into play when the national laws are at issue. Each state has its own set of laws and its own judicial system that may vary considerably from the federal scheme and sometimes conflicts with it. Under certain circumstances, federal law is applied by state courts and state law is applied by federal courts. Accordingly, while there are many parallels that broadly may be generalized when discussing U.S. jurisprudence for purposes of this Chapter, differences may be significant and any specific circumstances must be analyzed uniquely under the appropriate and applicable law.

expense of discovery outweigh its potential benefit; and whether the information sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive.

The concept of party-initiated discovery became part of American legal culture with the enactment of the original Federal Rules of Civil Procedure in 1938. The requirement of an early exchange of all relevant information, it was thought, would permit the parties to evaluate the likelihood of a successful verdict at trial, the potential degree of liability, and the value of a settlement. The theory was that when armed with full knowledge, a litigant is in the best position to obtain justice and the court need not expend resources on trials of undisputed facts. Since 1938, discovery has become a fundamental right of parties to litigation in the United States. The U.S. Supreme Court, for example, long ago determined it essential for the parties to have mutual knowledge of all relevant facts and, towards that goal, stated that "the discovery provisions are to be applied as broadly and liberally as possible."[23]

In order to minimize the potential for dispute, discovery statutes and rules require -- and many judges encourage, prod and sometimes compel -- the parties to meet early in the case to plan how best to address discovery issues that may arise. These "meet and confer" sessions often result in written agreements between the parties. When deemed important, the parties may request that their agreement be entered as a "stipulated order" by the court. Alternatively, particularly if the parties cannot reach full agreement, the court may enter an order at the request of one of the parties or of its own volition. Many times these agreements and court orders are used to protect confidential and personal information exchanged in discovery, as discussed in more detail below.

[23] *Hickman v. Taylor*, 329 U.S. 495, 506-507 (1947).

b. Limitations on the Scope of Discovery in U.S. Litigation

Discovery is not unlimited in U.S. litigation. The Federal Rules of Civil Procedure have been amended several times in order to correct perceived abuses of discovery. One of the most significant changes occurred in 2000 when Rule 26(b)(1) was modified to create a "two-tiered" approach to the scope of relevancy. Prior to the 2000 amendment, the Rule permitted discovery of all information "relevant to the subject matter involved in the pending actions." As the Rule currently reads, a party is only entitled, initially, to information that is relevant to any party's claim or defense in the case, as stated in the pleadings. Any other information relevant to the broader subject matter of the dispute is not properly within the scope of discovery without the prior permission of the court after the requesting party has demonstrated "good cause" for the information sought.

Another significant rule change occurred in 2006 in response to the extraordinary difficulties encountered by the parties as a result of the proliferation of electronic data. This phenomenon is referred to here as electronic discovery or "ediscovery." The 2006 changes to the Federal Rules were extensive and intended to address the potential for excessive costs and burdens associated with electronic discovery, to remedy the lack of uniformity amongst the courts on matters concerning the exchange of electronic data, and to encourage trial judges to more closely manage the discovery issues in the cases before them.[24]

While far from perfect, the 2000 and 2006 efforts to curtail discovery overuse and bridle associated expense demonstrate that discovery – and particularly ediscovery – is not as untamed as might otherwise be thought by many in Europe. And although it is still true that the identification, preservation, collection, processing and production of electronic data in U.S.

[24] Comm. on Rules of Practice & Procedure, Judicial Conference of the U.S., Summary of the Report of the Judicial Conference Committee on Rules of Practice and Procedure 24 (2005).

litigation can be burdensome and unwieldy, especially when measured against comparable litigation in the E.U., these amendments to the Federal Rules (which have been adopted by several of the state courts as well) provide parties and the courts with the tools to better manage or at least argue for the better management of ediscovery.

c. Discovery of Documents and Electronically Stored Information From Sources Outside the United States

In a wide variety of disputes in both state and federal courts in the United States, the information that the parties may seek in discovery is not physically located in the United States. As a general rule, however, the court may compel the party to produce it under the Federal Rules of Civil Procedure (or under the applicable state civil procedure rule), if :

(1) a party is under the jurisdiction of a state or federal court;

(2) the information sought from that party is relevant to the claims or defenses asserted in the litigation;

(3) the information is not exempted from discovery on the basis of a legally-recognized privilege; and,

(4) the information is within the "possession, custody, or control"[25] of the party, regardless of physical location.

A party may respond to a request or to a court order by stating that the information is located in another country, but that does not deprive the court of the power to order that the information be produced, nor does it prevent a court from sanctioning a party for failing to produce it. However, when a party properly asserts that it is prevented from producing the requested information by

[25] Fed. R. Civ. P. 34(a).

the laws of another country, the court is obliged to analyze the situation, determine if the exercise of its power under the circumstances is appropriate, and consider possible alternatives, including the application of the Hague Evidence Convention for the Taking of Evidence Abroad During Civil Commercial Matters (the "Hague Convention").

The leading case on the application of the Hague Convention to U.S. discovery is *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa*[26] *("Aérospatiale")*, in which the United States Supreme Court held that a federal court is not required to apply the Hague Convention to obtain evidence located in a foreign jurisdiction. In *Aérospatiale*, the plaintiffs brought a product liability suit in U.S. federal court in the state of Iowa against a French airplane manufacturer. The French manufacturer objected to the court's application of the Federal Rules of Civil Procedure to govern discovery in the case and argued that discovery should proceed under the Hague Convention because: (1) the evidence sought was located in France; (2) both the U.S. and France were signatories of the Evidence Convention which dictated the exclusive procedures that must be followed for pretrial discovery; and (3) under French law the manufacturer was prohibited from responding to discovery requests that did not comply with the Hague Convention.[27]

The Supreme Court held that application of the Hague Convention was not mandatory, observing that it "does not modify the law of any contracting state, require any contracting state to use its procedures either in requesting evidence or in responding to requests, nor compel any contracting state to change its own evidence gathering procedures."[28]

---

[26] 482 U.S. 522 (1987)
[27] *Id.* at 525-26.
[28] *Id*. at 534.

The Court held further that if the Hague Convention was the exclusive method to obtain discoverable information located in a foreign signatory state, it would be "inconsistent with the overriding interest in the 'just, speedy, and inexpensive determination'" of the American trial court system.[29] Addressing the French statute cited by the manufacturers prohibiting them from responding to discovery requests that did not comply with the Hague Convention, the Court held that the statutes of foreign jurisdictions "do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute" and that any such assertion would be an "extraordinary exercise of legislative jurisdiction" by the foreign sovereign over a U.S. judge.[30]

The Court did not, however, declare that the Hague Convention had no applicability to discovery in U.S. courts. While vigorously asserting the *power* of a U.S. court to order a party to produce evidence from sources abroad, it required U.S. courts to carefully consider, as a matter of international comity under the *Restatement of Foreign Relations Law of the United States,*[31] whether under the circumstances of each case the discovery should be allowed or the Hague Convention presented a viable alternative to the civil procedure rules. It required courts to apply the following five-factor analysis:

> (1) the importance to the litigation of the documents or other information requested;
> (2) the degree of specificity of the request;
> (3) whether the information originated in the United States;
> (4) the availability of alternative means of securing the information; and

---

[29] *Id.* at 542-543, quoting Fed. R. Civ. P. 1.

[30] *Id.* at 544 n.29.

[31] *Restatement of Foreign Relations Law of the United States (Revised)* § 437(1)(c) (Tent.Draft No. 7, 1986) (approved May 14, 1986). The *Restatement* is not a statute or rule, but a document representing the consensus view of the law by leading jurists, law professors, and practitioners who are members if the American Law Institute.

> (5) 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.[32]

In a subsequent case decided just two weeks later, a lower federal court added three more factors to the international comity analysis:

> (1) the competing interest of the nations whose laws are in conflict;
> (2) the hardship of compliance on the party from whom discovery is sought; and
> (3) the importance to the litigation of the information and documents requested.[33]
>
> 1.

Subsequent federal and state decisions resolving conflicts of laws between foreign data protection laws and U.S. discovery have weighed these factors in their respective international comity analysis to determine whether and to what extent the foreign law should prevail or influence the discovery sought.

Applying these factors, for example, the Supreme Court of the state of Texas held that a lower trial court failed to balance the competing interests of the parties, including relevant German law, where Texas discovery rules conflicted with the German Federal Data Protection Act, and information held by the German parent company of the U.S. subsidiary party should not be produced. It was significant to the Texas Supreme Court that ample evidence was presented regarding the importance of the German law, including statements by the data Protection Commissioner for Lower Saxony and the German Federal Ministry of Labor and Social Order.[34]

Aérospatiale and the *Restatement* test have been cited and applied by several state and federal courts in the United States faced with requests for discovery from foreign sources. In recent years, the number of cases involving discovery from foreign sources – and conflicts similar to those faced by the parties and the court in *Aérospatiale* – has increased steadily, as

---

[32] *Id.* at 544 n.28. This five-factor analysis is commonly referred to as the "*Restatement*" test.

[33] *Minpeco, S.A. v. Conticommodity Servs., Inc*., 116 F.R.D 517, 522 (S.D.N.Y. 1987)

[34] *Volkswagen AG, Relator v. Valdez,* 909 S.W.2d 900, 902 (Tex. 1995)

commerce has become more global, digital information is managed on international platforms, and jurisdictions have enacted a variety of new data protection laws. In the majority of these cases, the courts have held that the interests of the United States in compliance with its civil procedure rules has outweighed the interests foreign states, as asserted by the parties objecting to discovery.

One common element to these cases is that the party objecting to the application of U.S. discovery procedures to information from sources outside the U.S. failed to demonstrate to the court's satisfaction that the conflicting foreign law represented a serious impediment to discovery.[35] Another significant factor is that the law outside of the U.S. that is often asserted is in the form of a blocking statute, which are generally disfavored by U.S. courts.[36]

Some American courts have taken a more deferential approach to the competing interests asserted by parties objecting to discovery. In *In re Vitamins Antitrust Litigation*,[37] a trial court in the District of Columbia ordered that discovery proceed under the Federal Rules of Civil Procedures rather than under the Hague Convention, but granted a request to withhold documents protected from discovery by Swiss and German domestic privacy laws. The plaintiffs were then given the chance to determine if the requested information was absolutely essential to their case or if there was a way to frame a protective order to safeguard the producing party from liability in Switzerland and Germany for producing the information. Thus, production of the

---

[35] *See, e.g., Strauss v. Credit Lyonnais, S.A.*, 242 F.R.D. 199 (E.D.N.Y. May 25, 2007) (finding that the parties objecting to the production of French banking records in an international terrorism case faced little likelihood of prosecution under French law).

[36] Blocking Statutes are generally disfavored in the U.S. because they purport to deprive US courts of the authority to make fair adjudications based on the information before them. As noted by the Supreme Court in *Aerospatiale*, blocking statutes, in the context of the international comity analysis, need not be given the same deference by courts of the United States as substantive rules of law at variance with the law of the United States. *Aérospatiale* 482 U.S. at 544, *fn* 29, citing *Restatement of Foreign Relations Law of the United States (Revised)* § 437, Reporters' Note 5, pp. 41,42 (Tent. Draft No. 7, Apr. 10, 1986).

[37] 2001 WL 1049433 (D.D.C. June 20, 2001).

information rested on a balance of the importance of the information to the resolution of the litigation, against the consequences to the producing party of requiring this discovery.

During 2010, several U.S. courts addressed requests for discovery of data from sources outside the U.S. Two cases, both involving private actions under U.S. antitrust laws against international industries, illustrate the different conclusions that U.S. courts can come two when applying the *Aérospatiale* and *Restatement* factors to different sets of facts. In *In Re Air Cargo Shipping Services Litigation*, a trial court on two occasions ordered the discovery of highly relevant transaction and cost records in France[38] and South Africa[39] despite assertions by the defendant corporations that the laws of their home countries prohibited the disclosure of such records for the purpose of U.S. discovery. However, in *In re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation*[40] a different judge in the same court analyzed the plaintiffs' requests for particular documents from Visa and MasterCard's European entities related to an investigation by the European Commission's Directorate-General for Competition into potentially anticompetitive credit card practices. The judge found that the documents in question were not routine documents generated in the course of business, but statements made to the Commission under a guarantee of confidentiality. The court held that while the documents in question were highly relevant to the U.S. litigation, the interests of the foreign entity (in the case, the European Commission as opposed to a sovereign state) in the integrity of its investigative proceedings were "strong and legitimate,"[41] and had been clearly articulated in a statement

[38] 2010 WL 1189341 (E.D.N.Y. Mar. 29, 2010) (finding that the narrow sovereign interests represented by the French blocking statute did not outweigh the international interest in combatting anticompetitive behavior).

[39] 2010 WL 2976220 (E.D.N.Y. July 23, 2010) (finding the likelihood that a South African government-owned business would be prosecuted under the South African blocking statute to be "speculative at best").

[40] 2010 WL 3420517 (E.D.N.Y. Aug. 27, 2010)

[41] *Id.* at *9.

submitted by the Commission's Director-General for Competition.[42] The discovery was therefore denied because of the foreign data protection law.

d. Increasing Awareness of E.U. Data Protection Laws Resulting from Cross-Border Discovery Conflicts

U.S. litigants and courts are generally unfamiliar with E.U. data protection laws and more often than not are surprised both by the expansive application of those protections and the acute restrictions imposed on information that otherwise may be subject to discovery in U.S. litigation. The recent increase in the number of such encounters is attributable to two developments: First, the advent of enterprise-wide information systems and the corresponding ability to distribute information exponentially to world-wide, intra-corporate, collaborative groups, has increased the likelihood that E.U. information – subject to E.U. data protection laws – is relevant for purposes of U.S. litigation. The world has become smaller, in other words, and information is no longer contained within traditional geographic boundaries.

Second, U.S. corporations have become sensitized to a broadening legal requirement to preserve records and data that are relevant to existing or reasonably anticipated U.S. litigation, government investigations and certain audits. This increased awareness comes from a number of recent U.S. court decisions where parties have incurred significant sanctions because of their failure to preserve relevant evidence (a wrong known as "spoliation" of evidence), and because of the 2006 ediscovery amendments to the Federal Rules of Civil Procedure, referenced above,

[42] *Id.* at *4.

that have raised a new and heightened awareness of the duty to undertake reasonable efforts to preserve relevant materials.

The upshot of these developments and the resulting clash of their confluence are easy to see. Data from sources outside the United States have become relevant to American business functions like never before and corporate parties to U.S. litigation are required to identify, preserve, process, and possibly produce documents from locations outside of the United States. Companies involved in U.S. litigation, consequently, will increasingly encounter, and be called upon to resolve, potential conflicts between foreign data protection laws, such as the E.U. Data Privacy Directive (Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data) and U.S. discovery obligations.

IV. Cross Border Solutions: WP158 and The Sedona Conference®

The sheer volume of activity in what is now known variably as "cross-border discovery" and "international ediscovery" has come to the attention of the E.U.'s Article 29 Working Party. In February of 2009, that body issued "Working Document 1/2009 on pre-trial discovery for cross border civil litigation" (hereinafter referred to as WP158).[43] Acknowledging the dilemma that many E.U. corporations and E.U. affiliates of U.S. corporations face, the Working Party in

[43] Working Document 1/2009 on Pre-Trial Discovery for Cross-Border Civil Litigation, 00339/09/EN, WP 158 (Feb. 11, 2009). The paper is found at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp158_en.pdf.

WP158 proposes guidance to aid those multinationals caught between U.S. cross-border discovery obligations and E.U. data protection and privacy laws.[44]

Prior to the publication of WP158, The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6) had identified foreign data protection laws as amongst the most confounding aspects of cross-border discovery and one that was growing in frequency. Determined to clearly explain the legal and political nature of the phenomenon and to provide practical support to lawyers and their clients, WG6 published "The Sedona Framework" for public comment in August of 2008.[45] The Sedona Framework was subsequently recognized by the Article 29 Working Party in WP158 as providing the relevant factors U.S. courts should consider when determining the scope of cross-border discovery obligations.

Since publication of The Sedona Framework for public comment, WG6 has focused its efforts on the identification and development of "best practices" to mitigate the conflict of laws that can arise because of foreign data protection laws, on the one hand, and the discovery rights of parties to U.S. litigation, on the other hand. While the internal deliberations of WG6 are confidential, WG6 works with information and data privacy experts from around the world and has met with members of various data protection authorities. In addition, WG6 has held two International Programmes, open to the public, that have featured discussions of proposed "best practices" in this area: the first in Barcelona in June of 2009 and the second in Washington, D.C. in September 2010. The result of this international effort will be made available for public

[44] For a more complete discussion of WP158, its ramifications relative to U.S. discovery and a proposed solution to cross-border ediscovery conflicts with the E.U. Data Privacy Directive, *see* Moze Cowper & Amor Esteban, E-Discovery, Privacy, and the Transfer of Data Across Borders: Proposed Solutions for Cutting the Gordian Knot, 10 Sedona Conf. J.. 263, 274 (2009).

[45] The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy & e-Discovery (2008) and *see* http://www.thesedonaconference.org/dltForm?did=WG6_Cross_Border for a free PDF download of this document.

comment in 2011 in the form of a publication from The Sedona Conference. The following is a description of the current thinking, as expressed at those open Programmes and in the materials that accompanied them. It is subject to continued evolution throughout 2011.

a. The Sedona Conference International Principles

The writing under development is tentatively entitled: THE SEDONA CONFERENCE® INTERNATIONAL PRINCIPLES ON DATA PROTECTION LAWS IN U.S. LITIGATION: Best Practices, Recommendations & Principles for Addressing the Preservation and Discovery of Protected Data in U.S. Litigation (hereinafter "*International Principles*"). While the focus is the E.U. Data Privacy Directive (Directive 95/46/EC), the *International Principles* will be designed to have broad application whenever U.S. discovery requirements conflict with data protection laws; regardless whether those laws are from E.U. member states, non-E.U. countries or even the United States.

Sedona's *International Principles* will be grounded on the belief that lawyers, parties, judges and data protection authorities, through cooperation, can work their way through the seemingly irreconcilable differences that arise when foreign data protection rights collide with U.S. discovery requirements. Cooperation, in fact, is a hallmark of The Sedona Conference as reflected in its much-heralded *The Sedona Conference® Cooperation Proclamation* published in July 2008.[46] The *Cooperation Proclamation* calls upon adversaries to work collaboratively during the discovery phase of litigation in order to focus on the merits of the case instead of on unnecessary discovery and its attendant costs.

[46] The *Sedona Conference® Cooperation Proclamation* has been cited in more than 20 federal court opinions and is formally endorsed by more than 100 U.S. state and federal judges. It is available without charge at http://www.thesedonaconference.org/content/tsc_cooperation_proclamation.

The strength of cooperation will be the foundation of the *International Principles*, which will seek to identify common ground and consensus-building factors with which to forge practical solutions to the cross-border discovery/data protection conundrum. While it is premature to provide examples here – the exact language is still in development – the *International Principles* will recognize and identify several basic but important values to E.U. and U.S. interests, coupled with a thematic appeal for the mutual respect of cultural differences. A U.S. litigant's right to the discovery of protected information that is relevant and necessary to a claim or defense will be recognized as a legitimate interest. Likewise, E.U. data privacy will be recognized as a fundamental right of European citizens worthy of reasonable protections by litigants and U.S. courts. The compromise between the two can be achieved through reasonable assurances that the interests of the individual will be safeguarded and that transparency, proportionality, data security and similar principles will apply throughout the process and transfer continuum.

Data protection laws, after all, are not antithetical to U.S. preservation and discovery efforts. U.S. courts and parties often provide protections to personal, confidential and sensitive information through the use of confidentiality agreements and protective orders. Courts, in fact, have denied discovery in circumstances where E.U. privacy rights were deemed more important than the discovery sought by litigants.[47] Through its *International Principles*, The Sedona Conference seeks to raise awareness that data protection and discovery can and often does co-exist and that, through its guiding principles and a prototypical approach, the publication can

[47] *See e.g.*, *Salerno v. Lecia*, 1999 LEXIS 7169 (W.D.N.Y. 1999) (production of severance package information and personnel files precluded by Directive 95/46/EC and by the German Act on Data Protection); *Volkswagen AG, Relator v. Valdez*, supra n. 14 (denying request to produce company telephone book protected by German Federal Data Protection Act, BGB1. I, 2954, because production would undermine interests of Germany but no interest of the United States would be undermined if it was not produced, particularly where alternative methods of discovery of same information were available).

facilitate international recognition that a party should be able to achieve both compliance with foreign data protection laws and meet its U.S. preservation and production obligations.

b. The Three-Stage Approach for Harmonization

It is currently proposed that a three-stage approach advanced at The Sedona Conference International Programmes be reflected in the *International Principles*. That approach envisions an order from the U.S. court that extends special protections to data covered by foreign data protection laws; a separate order that schedules or phases discovery, and a protocol that seeks to maximize compliance with the foreign data protection law. Depending on the circumstances of the case, the parties and the court may find that some or all of these steps should be applied.

Protective Order. The first stage of the proposed three-stage approach is the Protective Order. The Protective Order is intended to be negotiated and agreed to by the parties, but it may be submitted to the court unilaterally if cooperation is not forthcoming. Having the court enter the order would be an important factor that signifies to foreign data protection authorities that the foreign data protection laws are respected and that the confidentiality and security of the protected information is maintained under the auspices and authority of the U.S. court.

Confidentiality can be achieved at three levels. First, all protected data would be marked appropriately and distribution limited to only those persons who have a need to see the data and who agree to be bound to the terms of the Protective Order. Second, the producing party may retain the right to redact protected information that it considers irrelevant, and a process for challenging those determinations is provided. Third, the Protective Order would permit the producing party to petition the court to address specific foreign data protection requirements that may not be covered in the more general terms of the proposed stipulated order.

Data security can be achieved through a requirement that the recipient of protected information maintain it in a password protected environment and take similar additional steps as the parties may agree or as the court may order.

Scheduling Order. The second stage of the proposed approach anticipates the use of a scheduling order whereby the parties agree on, or the court orders, deadlines and sequencing for the completion of discovery. The primary purpose of the scheduling order would be to ensure sufficient time to "legitimize" the processing and transfer of protected foreign data. Legitimization is the third stage of the proposed methodology and is discussed below. Scheduling also serves to demonstrate respect for foreign data protection laws and to maintain confidentiality and security. Scheduling contemplates that information that is not subject to data protection laws would be identified, collected, processed and produced first, thereby minimizing the likelihood that the same or similar information will be required from sources subject to foreign data protection laws.

Generally speaking, discovery pursuant to the scheduling order would proceed chronologically as follows:

1. Data from U.S. sources that are not subject to U.S. data protection laws;
2. Data from U.S. sources that are subject to U.S. data protection laws (*i.e.*, Gramm–Leach–Bliley Act);[48]
3. Data from foreign sources that are not subject to foreign data protection laws; and then,
4. Data from foreign sources that are subject to foreign data protection laws (and, therefore, that have to undergo legitimization).

[48] Also known as the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (1999).

In the development of the schedule, the law of each implicated country would be considered separately, recognizing that different timetables may apply.

Legitimization Plan. In this third prong, the party responding to foreign discovery would develop a plan setting forth the methodology by which it contemplates preserving, processing, transferring and producing protected information. The legitimization plan should be tailored to each applicable data protection law and should seek to comply with as many requirements as possible. For example, in the E.U., and for processing to be lawful under Article 7(f) of the Data Privacy Directive, legitimization would require that the "legitimate interests" of the controller or third party would not reflexively be overridden by the interests for fundamental rights and freedoms of the data subject. This test seeks to balance proportionality, relevancy to the litigation and the consequences to the data subject. Moreover, if the balancing test tipped in favor of the data controller, adequate safeguards would need to be put in place. Accordingly, a legitimization plan under Article 7(f) should address each of these various factors, identifying how each step will be accomplished, and the producing party should document the endeavor in the event of a challenge from data protection authorities or others.

Consent to disclose protected information from the data subject would be another factor to consider in the legitimization planning, recognizing, however, that in many jurisdictions consent is not considered voluntary when requested of an employee. Establishing a transparency plan for employees whose protected information may be subject to U.S. discovery would also be recommended. Such a plan would include consideration to giving data holders general advance notice of the possibility that their protected data will be processed for litigation, the identity of any recipients of that data, the purposes for which the data is processed, the

categories of data at issue and the existence of the data subject's right to object to the preservation or production.

Another important aspect of the Legitimization Plan would be the separation and segregation of relevant data that is subject to the data protection laws from relevant data which is not protected. Before undertaking that process, the proposed *International Principles* would likely suggest that negotiations or a motion to the court may help to narrow the definition of what is "relevant," and the more narrow the scope of foreign data required for discovery purposes, the better. Once "relevancy" is defined, data that does not fall within the definition would be filtered out of further processing. Foreign data that is relevant but not subject to any data protection law could be produced without further legitimization-related processing and pursuant to the scheduling order. Relevant data that is protected by the foreign law would then be separated from the rest and be ready for additional treatment.

Consideration would then be given as to whether protected, relevant data may exist in a non-protected form. For example, if protected data is a duplicate of or substantially identical to information maintained geographically within the United States, it may be possible to produce the U.S. information in substitution for the protected data by means of a stipulation or a court order, if necessary.

Any remaining, relevant and protected foreign data can then be processed in the usual way. Consideration should be given to processing this data within the geographical boundaries of the host country; a approach that is supported by certain data protection authorities. Other similar processing considerations, depending on the law of the hosting nation, include the use of

a neutral to oversee the processing of protected information and the employment of anonymization and pseudo-anonymization.[49]

The transfer of protected data to the United States and its production to the requesting party also requires legitimization. In the first instance, the proposed *International Principles* will likely suggest the development of a transfer plan that would include, for example, selection of an appropriate transfer mechanism (*e.g.*, Binding Corporate Rules, Model Contracts or Safe Harbor). Before producing the information to the requesting party, further consideration would also be given to instituting appropriate data protection measures, including, for example, the use of Model Contracts .

Conclusion

The Sedona Conference's forthcoming *International Principles* and the proposed three-stage approach seek to strike a balance between the rights of data subjects, the public policies underlying data protection laws and the preservation obligation and discovery rights of parties to U.S. litigation. They strive to achieve reasonableness, proportionality and respect for the fundamental rights and freedoms of the individual. The proposed method is driven by cooperation between the various stakeholders or it may be invoked by the court if intervention is necessary. In either event, the outcome should satisfy data protection laws by demonstrating compliance or, at a minimum, the effort to comply with data protection laws within the constraints of also meeting U.S. discovery requirements. For more information and the posting

[49] It should be noted that anonymization and pseudo-anonymization is not likely to be accepted by the requesting party or the U.S. court, except in perhaps certain very narrow circumstances, because, without identification of the individual and the connection that person may have had to the events at issue, the information itself likely is rendered meaningless and therefore useless for U.S. discovery purposes.

of the *International Principles* for public comment when completed, please visit the work of WG6 at the website of The Sedona Conference, http://www.thesedonaconference.org.