A NEW APPROACH TO CROSS-BORDER DISCOVERY: THE SEDONA CONFERENCE'S *INTERNATIONAL PRINCIPLES*

By: Tripp Haston and Lindsey Boney

This article originally appeared in the February 2012 International Committee Newsletter.

Of all issues in modern litigation, discovery of electronically stored information (ESI) remains one of momentous and ever-growing significance. Collection, processing and production of ESI can be time-consuming, and its cost crushing. It is no surprise, then, that the scope of e-discovery is often a central point of contention between parties. But those challenges grow exponentially when international entities are involved. It is then that parties and American courts must contend not only with liberal American discovery rules but also with data privacy laws like those implemented in the European Union. In view of these unique challenges, the Sedona Conference—an organization "dedicated to the advancement of law and policy in the areas of antitrust law, complex litigation and intellectual property rights"[1]—has proposed a framework to help American courts and their multinational litigants successfully navigate these often conflicting obligations.

Tripp Haston is a partner with Bradley Arant Boult Cummings LLP where he serves as Co-Chair of its Life Sciences Industry Team.

Lindsey Boney is an associate with Bradley Arant Boult Cummings LLP where he practices in the general litigation group, with a particular focus on pharmaceutical litigation.

This article proceeds in three parts. First, we offer a brief overview of EU data protection laws and how they can conflict with U.S. discovery rules. Second, we briefly survey how U.S. courts have applied data privacy laws. Finally, we provide a glimpse of the Sedona Conference's new, innovative suggestions for the complexities of cross-border discovery—the *International Principles*.[2] Published in December 2011, the *International Principles* advocate cooperation between parties not only to avoid any potential conflicts but also to resolve them when they arise and propose a number of specific suggestions for cross-border discovery.

[1] The Sedona Conference: Frequently Asked Questions, http://www.thesedonaconference.org/content/faq (last visited January 27, 2012).

[2] WORKING GROUP 6, THE SEDONA CONFERENCE, INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION: BEST PRACTICES, RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING THE PRESERVATION OF DISCOVERY OF PROTECTED DATA IN U.S. LITIGATION (European Union ed. 2011).

I. The Conflict

EU Data Protection Laws

Three sources of international law, in particular, can create conflicts when a company with an EU-presence must respond to discovery in American litigation.

First, the EU Data Protection Directive has led many countries to enact data privacy laws.[3] Directive 95/46/EC cements data privacy as a fundamental human right. In relevant part, it requires EU-member States to protect their citizens' "right to privacy with respect to the processing of personal data." Data privacy laws do that by specifically restricting the ways in which personal information can be stored, used, and disseminated.

Even applying the Directive—and the data privacy laws that it has spawned—can be challenging for U.S. courts because terms like "personal data" and "processing" do not have common meanings between the EU and U.S. legal systems. "Personal data," for example, as used in the Directive, references more than a social security number, national identification number or medical records. Instead, it much more broadly includes "any information relating to an identified or identifiable natural person."[4] And the term "processing" includes not only common functions like formatting conversions, de-duplication, filtering, and indexing, but also any collection or manipulation of data, including the storage of data as required in a routine litigation hold.[5]

As a practical matter, the Directive prohibits the transfer of a broad range of data. No personal data may be transferred to a non-EU State unless that country "ensures an adequate level of protection" for the data.[6] There are some exceptions. Data that is "necessary or legally required on important public interest grounds" may be transferred, as can any data that a party needs "for the establishment, exercise or defence of legal claims."[7] But still, local laws may preclude transfer, and even though there are some "safe harbor" principles that the EU and the U.S. have developed, those safe harbors are limited in scope and often fail to facilitate discovery.

Second, although the Hague Convention on the Taking of Evidence provides a procedure to facilitate the discovery of information sought in transnational litigation, its application is fraught with problems. Fifty-four countries, including the United States, have agreed that judicial authorities in the contracting states "may … request the competent authority of another Contracting State … to obtain evidence, or to perform some other judicial act."[8] But the Convention contains an important opt-out: a State can "declare that it will not execute letters of request issued for

---

[3] Directive 95/46 of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) (EC).

[4] *Id.* art. 2(a).

[5] *Id.* art. 2(b); *see also* Data Protection Working Party, Working Document 1/2009 art. 29 (describing this tension).

[6] Directive 95/46, art. 25.

[7] *Id.* art. 26(1)(d).

[8] *Id.* art. 1.

the purpose of obtaining pre-trial discovery of documents."[9]

Third, numerous EU-member States employ "blocking statutes" to require parties to use the procedure established by the Hague Convention, or otherwise to restrict the production of documents within their borders. That process can be complicated. Switzerland, for example, requires that parties use its local courts to facilitate document production for litigation abroad.[10] Other EU-member States—including Germany, Spain, and Belgium—have adopted similar laws.[11] And France has even authorized criminal sanctions against private parties that conduct discovery within its borders for litigation abroad.[12]

U.S. Discovery Rules

In stark contrast to these discovery limits are the liberal discovery rules that are, in many ways, the hallmark of the modern American legal system. The Federal Rules of Civil Procedure—and the many state-based rules of procedure patterned on them—give a requesting party the basis to obtain a broad range of another party's data.[13] Although some limitations exist, in practice, U.S. discovery often requires the production of mountains of data, even though that data may, at times, bear only tangential relevance to the case. The Federal Rules are expansive in this regard. Litigants need not establish that the requested information will be admissible evidence; discoverability expands to anything "reasonably calculated to lead to the discovery of admissible evidence."[14] These burdens extend beyond production. Parties to U.S. litigation are required to preserve any potentially responsive data from the moment they reasonably anticipate litigation.[15] With these liberal discovery rules, U.S. litigation subjects a tremendous amount of data to possible management or production.

In today's world of multinational companies doing business (and, as a result, litigating) across the globe, the U.S. and EU laws are bound to conflict. And it is still an open question whether conflicts may arise simply by a party's data cache in the cloud or stored on servers housed overseas, or by outsourcing document review to a foreign-based company. In any event, multinational companies must be cognizant of the two systems' discovery obligations and endeavor to comply with both. Unfortunately, the current approach by many U.S. courts frustrates such compliance.

---

[9] *Id.* art. 23.

[10] Swiss Penal Code Art. 271, 273.

[11] *See generally* WORKING GROUP 6, THE SEDONA CONFERENCE, FRAMEWORK FOR ANALYSIS OF CROSS-BORDER DISCOVERY CONFLICTS 17–22 (2008) (discussing blocking statutes worldwide); Carla L. Reyes, *The U.S. Discovery–E.U. Privacy Directive Conflict: Constructing a Three-Tiered Compliance Strategy*, 19 DUKE J. COMP. & INT'L L. 357 (2009).

[12] French Penal Law No. 80-538.

[13] Fed. R. Civ. P. 26(b)(1) ("Parties may obtain discovery regarding any nonprivileged matter that is *relevant to* any party's claim or defense . . . ." (emphasis added)).

[14] *Id.*

[15] *See* INTERNATIONAL PRINCIPLES, *supra* note 2, at 2.

II. The Current Approach:

Aerospatiale

In light of these liberal discovery rules, American courts have not always given deference to EU data protection laws. The Supreme Court has provided some guidance for American courts to apply other nations' discovery laws, but interpretive problems remain.[16]

Aerospatiale involved a product-liability action brought by the plaintiff against two French-government-owned corporations in an Iowa federal court. Both sides exchanged initial discovery under the Federal Rules. When the plaintiffs served additional requests, however, the defendants moved for a protective order on two bases. First, they raised a procedural objection that the plaintiffs had not complied with the procedures established by the Hague Convention before serving the requests. Second, and more significantly, the defendants argued that any response would violate France's blocking statute. The magistrate judge ultimately compelled production of the requested discovery, a decision that the Eighth Circuit upheld.[17]

The Supreme Court also affirmed in relevant part, holding that although the procedures of the Hague Convention apply to discovery demands made of foreign companies, they are but "one method of seeking evidence that a court may elect to employ."[18] The Court held that the Convention procedures are neither a mandatory nor a required first step before resort to the procedure provided in the Federal Rules of Civil Procedure because they set only the "minimum standards" for cross-border discovery.[19] As for the French blocking statute, the Court held that "such statutes 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."[20] In powerful language, the Court exhorted other courts not "to adhere blindly to the directives of such a statute" because to hold otherwise would lead to the "incongruous" result that "nationals of such a country [would hold] a preferred status in our courts."[21]

Predictably, other American courts heeded the Court's admonition. As noted above however, because of the complex interplay between these various laws, interpretive problems remain.[22] It is in

---

[16] *See* Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for the S. Dist. of Iowa, 482 U.S. 522 (1987).

[17] *Id.* at 524–530.

[18] *Id.* at 541.

[19] *Id.* at 537 n.23.

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

[21] *Id.*

[22] *Compare* In re Perrier Bottled Water Litig., 138 F.R.D. 348 (D. Conn. 1991), Linde v. Arab Bank, PLC, 2009 WL 1456573 (E.D.N.Y. 2009), Old Ladder Litig. Co. v. Investcorp Bank, 2008 WL 2224292 (S.D.N.Y. 2008), and Volkswagen, A.G. v. Valdez, 909 S.W.2d 900 (Tex. 1995) *with* United States v. First Nat'l City Bank, 396 F.2d 897, 903 (2d Cir. 1968), In re Global Power Equip. Grp., 418 B.R. 833 (Bankr. D. Del. 2009), Strauss v. Credit Lyonnais, S.A., 249 F.R.D. 429, 442–443 (E.D.N.Y. 2008). For a more detailed discussion of these cases and other problems with cross-border discovery, *see generally* Tripp Haston &

this context that the Sedona Conference drafted its *International Principles* to help parties—and courts—manage cross-border discovery.

III. New Proposed Solution: *The International Principles*

Overview

Confronted with the complexities and conflicts of cross-border litigation, Working Group 6 of the Sedona Conference drafted the *International Principles* to provide a framework for addressing these problems. The *Principles* were written by an international group of attorneys who specialize in cross-border discovery and data protection. Although they were designed to apply broadly to cross-border discovery issues between the U.S. and any foreign country, consistent with the discussion above, the commentary accompanying the first edition focuses on issues specific to cross-border discovery between the U.S. and the EU.[23]

Underlying all six principles is the theme of cooperation between parties. Everywhere possible, the *Principles* exhort, the requesting party and the responding party should seek to reach agreements that provide relevant information while respecting EU laws. The *International Principles* contains a three-stage approach for avoiding and minimizing conflicts: (1) a stipulation or court order extending special protections to data covered by data protection laws; (2) a phased discovery process, memorialized in the scheduling order, that allows time for implementation of data protection measures and for determining whether the necessary information can be gathered from sources not subject to data protection laws; and (3) a legitimization plan that describes "the methodology by which it contemplates preserving, processing, transferring, and producing Protected Data."[24]

The Principles in Brief

Principle 1

With regard to data that is subject to preservation, disclosure, or discovery, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.

In keeping with the overarching idea of cooperation and collaboration, Principle One is based on two core tenets of U.S. law—comity and good faith. First, comity—which, as recognized by the Supreme Court in *Aerospatiale*, is essential to maintaining an international legal system—requires courts and parties to afford due respect the laws of other countries. Second, as reflected in the FRCP, good faith requires that parties advance data protection laws only when

---

Lindsey Boney, *The Unique Challenge of Serving Two Masters: European Data Privacy Laws & United States Discovery Obligations*, Int'l Who's Who of Prod. Liab. Def. Lawyers (2011).

[23] INTERNATIONAL PRINCIPLES, *supra* note 2, at vi.

[24] *Id.* at 17–18. The drafters included, as an appendix to the *Principles*, a model protective order and a model legitimization plan.

they truly are in conflict with U.S. discovery requirements.[25]

Principle 2

Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.

Principle Two echoes the Supreme Court's call in *Aerospatiale* for balancing certain considerations when deciding whether to order foreign discovery over the objections of the foreign sovereign. Both *Aerospatiale* and the drafters of the *International Principles* state that courts should consider the requested information's importance to the litigation, "the degree of specificity of the request, and the availability of alternative means of securing the information."[26] These factors are among several that the Restatement (Third) of Foreign Relations Law § 442(1)(c) states should be considered by a domestic court determining whether its interests outweigh those of a foreign country. The *International Principles* suggests that parties should use these same factors to guide their actions, and if those actions are challenged, courts should then use the factors in evaluating those actions.[27]

Principle 3

Preservation or discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.

In the commentary to Principle Three, the drafters set out a number of ways that parties can limit the scope of discovery to help minimize conflicts with EU data protection laws. One of these suggestions encourages phased discovery. Parties should agree to a scheduling order that organizes discovery such that the first data produced is the data least likely to be subject to data protection laws. In this chronological process, the last data to be produced would be the data most likely protected by EU data protection laws.[28]

Principle 4

Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.

The elements of the three-stage approach described above should be used to fulfill Principle Four: a protective order, a scheduling order for phased discovery, and legitimization plan. The most difficult of these to craft will be the "legitimization plan." Such legitimization plans "should be tailored to each applicable Data Protection Law and should seek to comply with those requirements, as well as with the U.S.

[25] *Id.* at 7–8.
[26] *Id.* at 11 (citing *Aerospatiale*, 482 U.S. at 544 n.28).
[27] *Id.*
[28] *Id.* at 15.

preservation and discovery obligations."[29] Appendix C to the *International Principles* is a helpful guide with instructions for establishing a data protection and transfer protocol that can be used in conjunction with a "legitimization plan."[30] Depending on the case, any or all of the three elements may help parties meet both U.S. and EU obligations. [31]

Principle 5

A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.

Principle Five reflects another practical tool developed by the drafters—namely, a protocol designed to help data controllers comply with data protection laws. These data controllers are encouraged to document their compliance with the protocol, which will provide evidence of good faith, reasonable efforts to safeguard data subject to privacy laws.[32]

Principle 6

Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

Principle Six addresses the issues created by data retention policies. Because ESI is relatively inexpensive to store, it is easy for an organization to become a hoarder of electronic data. Retaining electronic data for longer than business or legal reasons require, though, can further complicate compliance with EU privacy laws. To minimize such complications, organizations should enact policies to prevent data retention for any longer than their business needs (or the law) would require. Retained data, of course, should be protected with appropriate safeguards to prevent compromise of the data's integrity and confidentiality.[33]

IV. Conclusion

Cross-border discovery—in whatever form—creates enormous pitfalls. It is a problem that U.S. courts and litigants will continue to face. The Sedona Conference's new *International Principles* present a useful set of principles to aid parties in navigating these rough waters. Parties and courts should heed their admonition to cooperate to make cross-border discovery more efficient, fair, and effective.

* * *

[29] *Id.* at 18.
[30] *Id.*
[31] *Id.*
[32] *Id.* at 19.
[33] *Id.* at 22.