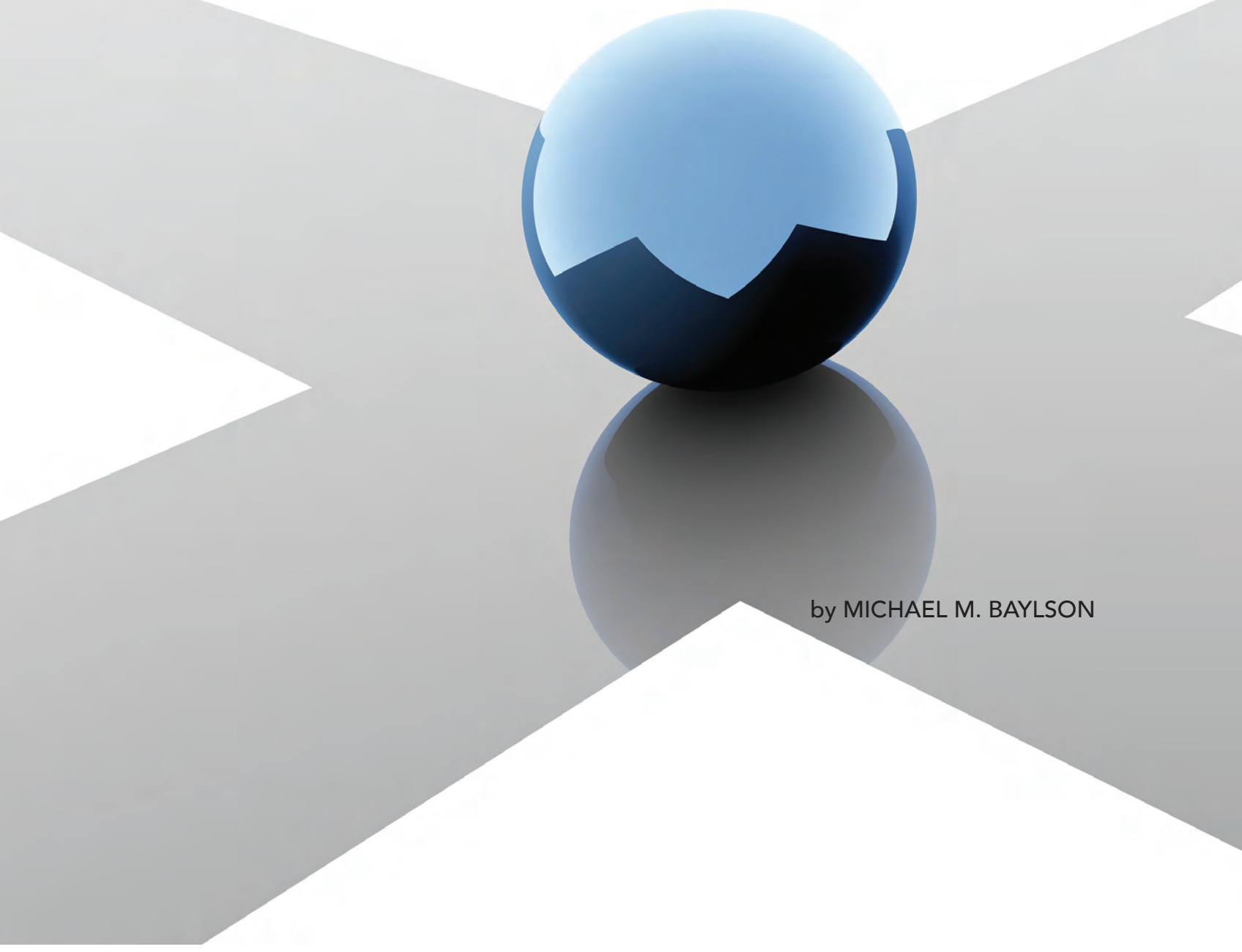
CROSS-BORDER DISCOVERY *at a crossroads*



by MICHAEL M. BAYLSON

Along with explosive globalization, including the ease with which parties can conduct business abroad, there has been a concomitant need for international legal systems to consider exchange of information across sovereign borders. How should a U.S. court analyze conflicting interests in a cross-border discovery dispute?

In its 1987 decision in *Aerospatiale*,[1] the Supreme Court of the United States held that the Hague Convention,[2] entered into by the United States and numerous foreign countries, was not the exclusive means by which the parties to litigation in a U.S. court could conduct discovery overseas.

The intervening 29 years have not only led to a significant growth in the global economy, but also to the revolutionary ability of digital technology to collect huge amounts of data, often without regard to sovereign borders. Along with the expected increase in international litigation, we have experienced more disputes over cross-border discovery.

THE ISSUES

Securing discovery from an overseas source is not easy – indeed, it can be painfully difficult.

Why?

There are several reasons, and the details can vary significantly depending on the country.

No nation in the world allows pretrial discovery in the same manner as the United States. Indeed, most foreign countries have an innate hostility towards the entire concept of pretrial exchange of documents and taking depositions. Most European countries empower quasi-judicial "data-protection officers" to regulate the production of information out of the host country, with very limited rights of appeal. Sovereign nations in different parts of the world have enacted laws ("blocking statutes") forbidding production of personal data, considered part of a "natural right of privacy," to specifically prohibit "exporting" information about one of their citizens, whether an individual or corporation.[3]

Experience has shown that it is appropriate, indeed necessary, to divide the quest for information from foreign sources into three separate categories:

First, transactional data, such as names, account numbers, and other identifying information, necessarily used by banks and

> ONE CLEAR INDICATION OF COMITY IS THE FACT THAT OUR CONGRESS HAS ENACTED STATUTES THAT SPECIFICALLY EMPOWER A DISTRICT COURT JUDGE TO ASSIST A FOREIGN PARTY SEEKING INFORMATION FROM WITHIN THE UNITED STATES.

credit card companies, in the cross-border purchase and sale of goods — independent of litigation.

Second, exchange of data in civil litigation. Following *Aerospatiale*, U.S.-based lawyers have frequently used a variety of litigation techniques when seeking overseas discovery. After many district court opinions, various strategies and techniques to achieve some pretrial factual discovery have allowed parties in U.S.-based litigation to get limited information from an overseas source.

Third, in criminal or national security investigations, different rules may apply, particularly when the basis of the request is related to terrorism, genocide, or some other internationally condemned activity.

A U.S. judge faced with a cross-border discovery dispute need not feel despair. The judge should promptly ascertain the reality of the situation — i.e., the relative simplicity or complexity of the issues, the "landscape" of the foreign country in terms of its own policies, and considerations of relevance, necessity, and proportionality (discussed below) — and enter a procedural order requiring each party to state its goals and contentions, and to promptly initiate any foreign discovery requested.

THE HAGUE CONVENTION

The Hague Convention remains the most frequently used method of requesting discovery, particularly for third-party discovery. As a treaty, it is well recognized and often applied. Of necessity, it is limited to signatory countries. While most European Union states (plus Russia and China) are signatories to the Hague Convention, a large number of developing countries (with which the United States has large-scale commercial transactions), and even some countries with highly developed economies (like Japan) have not signed the Hague Convention.

Proceedings under the Hague Convention can vary significantly according to the country where the information is located. Although the initiation of a request under the Hague Convention is fairly simple and will be administered promptly with assistance, if needed, by our U.S. Departments of State and Justice, the speed with which the request is treated in the overseas country can vary significantly.

For example, the Hague Convention has a specific provision protecting against privileged information. The scope of the "privilege," however, may be broader or more limited than in the United States. Collateral proceedings in the overseas country may be necessary for a foreign court to adjudicate a claim of privilege that is recognized in the foreign country, but perhaps not in the United States.

COMITY

Aerospatiale noted the importance of comity among the factors that a trial judge should consider in determining what orders should realistically be entered in a U.S. court. The touchstone is often determining what respect or obedience those orders will have when considered in a foreign country. The Supreme Court borrowed § 437(1)(c) from the Restatement of Foreign Relations Law of the United States,[4] which lists the following factors:

- The importance to the litigation of the documents or other information requested;
- The degree of specificity of the request;
- Whether the information originated in the U.S.;
- The availability of alternate means of securing the information; and
- The extent to which noncompliance with the request would undermine important interests of the U.S., or compliance with the request would undermine important interests of the state where the information is located.[5]

These factors, and particularly the last, form the basis of "comity," i.e., respect that one tribunal in one country should pay to a tribunal of another country. This has been termed "a balancing of competing interests, taking into account the extent to which the discovery sought serves important interests of the foreign state versus the policies to which providing the discovery would undermine the important interests of the foreign state."[6]

Resistance to our discovery rules increased after the recent revelations by Edward Snowden of massive data gathering by the U.S. government, some of which was directed specifically to leaders of foreign countries. In particular, European data administrators and courts sharpened their opposition to providing discovery for use in U.S. courts. Their fear, well deserved in their view, is that private information will not remain private once it reaches U.S. shores.

Judges may find it difficult to ascertain U.S. policy on the topic of international discovery. Our government has split various functions relating to oversight over cross-border transactions in international litigation among several different cabinet-level agencies, including the Departments of State, Justice, and Commerce as well as the Federal Trade Commission. Neither these cabinet-level departments nor the White House has seen fit to issue a policy statement. In January 2017, the new administration should direct one of these agencies to develop and issue a coherent statement of principles that a U.S.-based judge (or overseas judge) could follow as accurately expressing the policies of the United States in this area.

However, one clear indication of comity is the fact that our Congress has enacted statutes that specifically empower a district court judge to assist a foreign party seeking information from within the United States.

28 U.S.C. § 1781 authorizes the use of a letter rogatory, allowed by specific agree-

ment between countries. Such a letter takes the form of interrogatories or document requests sent by one party to a foreign party. Once again, because the concept of reciprocity is essential, the U.S.-based attorney and judge should verify that the practice of letters rogatory is recognized in the host country.[7]

28 U.S.C. § 1782 authorizes a district court with jurisdiction to provide "assistance to foreign and international tribunals and to the litigants before those tribunals in pending fact discovery."[8]

28 U.S.C. § 1783 pertains to the issuance of a U.S. subpoena to a U.S. citizen or resident located in a foreign country.[9]

Also, Federal Rule of Civil Procedure 28(b) authorizes and specifies certain rules for the taking of depositions in a foreign country.

These important — but seldom used — rules and statutes strongly show that our Congress has expressed a favorable view of pretrial discovery when relevant and necessary in international litigation. Mutuality should follow. U.S. judges should consider citing these provisions when contemplating and ordering overseas discovery. We can hope that other countries will respect comity and adopt these same principles as well.

Research has not found similar legislation in any other country in the world.

WHAT CAN A U.S. JUDGE DO WHEN A PARTY SEEKS INFORMATION HELD IN FOREIGN COUNTRIES?

A number of steps can be taken when a party seeks information held in a foreign country. It is important to separately approach intraparty and third-party discovery.

First, at the initial Rule 16 conference, require counsel for all parties to be prepared and candid in describing any likelihood of international discovery.

Second, set a prompt deadline for the parties themselves to initiate any foreign discovery and to periodically report to the court on how it is progressing, along with prompt identification of any barriers.

Third, given the wide disparity of foreign laws, require counsel — keeping in mind any language translation requirements — to report on the likelihood of getting the information from the foreign country and the status of their efforts.

Fourth, as to intraparty discovery:

- Most cases that involve this type of discovery usually have a high-dollar value or high exposure. Thus, legal fees, however substantial, are an expected "cost of doing business." U.S. counsel may be required to retain overseas counsel in the host country to facilitate the request, negotiate with data-protection authorities, or seek waivers or other accommodations to allow for the flow of information.
- Depositions may take place in the foreign country if conducted pursuant to the Federal Rules of Civil Procedure as allowed by Rule 28(b). Documents that are subpoenaed can be brought to the deposition or produced a day or two ahead of time for preparation and then used at the deposition, but originals are left in the host country with only one copy, as an exhibit, retained by the court reporter and taken back to the United States.
- There is a high likelihood that Electronically Stored Information ("ESI"), if allowed to be transferred over international borders, can include a great deal of private information, the transfer of which would breach a country's privacy laws. In these cases, as retrogressive as this may sound, a party can legitimately accept "hard copy" documents, with redactions made in the copy of the document to be used in the United States (or at a deposition) to eliminate any names, birthdates, or other personal identifiers that are not needed for the litigation. Thus, discovery of these redacted documents could be allowed, whereas discovery of the ESI containing all of the information would not be allowed.
- There are cases requiring a foreign corporation with substantial U.S.-based operations to produce documents held in a foreign country under the theory that the company has "control" over its records, and a U.S.-based judge can require a foreign corporation to produce them in U.S. litigation. However, the recent Second Circuit decision in *Microsoft v. United States,* although arising out of the issuance of a search warrant in the Southern District of New York for ESI that was located in a Microsoft digital server in Ireland, quashed the search warrant and rejected the government's expansive definition of "control."[10] The impact of this decision in civil cases will be developed in further litigation and possibly by a Supreme Court ruling. The issue, at least in civil actions, is whether "control" in the digital age warrants worldwide compliance with requests for digital documents that are otherwise subject to discovery rules, assuming they can be intelligently searched and then transferred to a U.S.-based computer.
- Protestations about possible criminal prosecutions in the foreign country for producing information for use in U.S. litigation frequently received a hostile reaction from U.S. judges.[11]
- Sanctions can follow a party's failure to produce information. When litigation is in the United States, a U.S. judge has the ability to impose sanctions on a party for failure to produce discovery within its "control." Thus, if the plaintiff has control over data located overseas and fails to produce it, the court retains the possible sanction of preclusion, or even dismissal, for failure to produce discovery within its control.[12]

This same principle can be applied by the court's power over a U.S.-based defendant that refuses to produce discovery within its "control" in overseas operations. The key issue, of course, is what constitutes "control."

THE SEDONA CONFERENCE® INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION

The Sedona Conference, a nonprofit think tank based in Phoenix, Ariz., has contributed greatly to discussions on many litigation topics and is best known for its work on developing principles for electronic discovery. However, Sedona also has taken the leading role in developing principles for cross-border discovery. Although those

principles are subject to possible revision because of recent developments summarized below, they deserve repeating and consideration not only by federal judges, but also by data administrators and courts around the world:

- 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.
- 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.
- 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.
- 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.
- 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.
- 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.[13]

Note that the word "necessary," which connotes a narrower view of information subject to discovery, may require a U.S. judge to ascertain a party's precise burden of proof and any specific evidence located within a foreign country.

RECENT DEVELOPMENTS IN THE EUROPEAN UNION

Background: Competing Concepts of the Right to Privacy

For over 20 years, the United States and the European Union have struggled to find a proper framework for protecting data and privacy interests in the face of cross-border commerce. For Europeans, these concerns are fundamental rights on par with free expression and equal treatment under the law as enshrined in Article 8 of the European Convention on Human Rights and Articles 7 and 8 of the E.U. Charter of Fundamental Rights. In Europe, the processing of personal data is prohibited unless authorized by law.[14] E.U. member states tend to favor "omnibus" laws for privacy protection.[15] Most of these provisions apply to mass transfers of data pursuant to commercial transactions, rather than litigation. However, as a pretrial matter, the E.U. attitudes on transactional data "spill over" to private litigation.

The Safe Harbor (2000-2015)

In 1995, the European Parliament and the Council of the European Union issued a Directive, Article 25 of which permits the transfer of personal data to countries outside the E.U. only if the country in question ensures "an adequate level of [data] protection."[16] Although the E.U. never made an official finding as to the adequacy of U.S. privacy protections, general consensus held that the United States was falling short.

Following negotiations from 1998-2000, the U.S. Commerce Department and the E.U. announced the adoption of the so-called Safe Harbor Privacy Principles in an effort to address concerns about data transfer to the United States. The European Commission approved Safe Harbor in 2000, holding that any U.S. company that complied with Safe Harbor and its related FAQs issued by the U.S. Commerce Department in July 2000 was providing "an adequate level of protection as set out in Directive 95/46/EC."[17]

For the ensuing 15 years, Safe Harbor provided a framework for many companies for exchange of information between the U.S. and the E.U. As of 2015, some 4,500 businesses were using it. Safe Harbor allowed companies to self-certify that they were in compliance with seven basic data-privacy principles, such as giving individuals choice over the sharing of their data with third parties and establishing safeguards for protecting information.

Snowden and *Schrems* — the Demise of Safe Harbor

Several developments impacted the data-privacy landscape after the adoption of Safe Harbor. Most notably, in 2013 Edward Snowden released classified data from the U.S. National Security Agency disclosing the existence of massive, covert U.S. surveillance programs and bulk collection of data. In addition, American-based social media companies such as Myspace, Facebook, Twitter, Instagram, and Snapchat — none of which existed at the time Safe Harbor was adopted — began to collect and share information from users from around the globe on an unprecedented scale. These events raised significant concerns from many citizens in both the U.S. and the E.U. about the importance of privacy protection. Consequently, proposals to revise Safe Harbor began receiving attention.

As those discussions were ongoing, in October 2015 the European Court of Justice struck down Safe Harbor. The court's ruling in *Schrems v. Data Protection Commissioner*, Case C-362/14, stemmed from the plaintiff's use of Snowden's revelations as a basis to challenge Facebook's Irish subsidiary's transfer of data from Ireland to servers in the United States for processing. The court held that the U.S. government's improper elevation of purported national security concerns over the Safe Harbor protections, coupled with a lack of meaningful remedies for E.U. citizens to challenge U.S. data collection, required finding the Safe Harbor was invalid. The court remanded *Schrems* to the High Court of Ireland to determine whether that court should suspend transfer of data to the United States for failure to provide sufficient protection.

The Privacy Shield: A New Way Forward?

As a result of *Schrems*, in February 2016 the U.S. Department of Commerce and E.U. authorities announced a new "E.U.-U.S. Privacy Shield" framework. The Privacy

ALTHOUGH THE ADOPTION OF THE PRIVACY SHIELD BY THE EUROPEAN COMMISSION SHOULD EASE THE CONTINUED FLOW OF DATA RELATED TO TRANSACTIONS, THE OPPOSITION OF POWERFUL DATA ADMINISTRATORS MAY CREATE PROBLEMS FOR CONTINUING TRANSFER OF DATA IN PRIVATE LITIGATION.

Shield creates legal remedies for E.U. citizens alleging privacy violations, increases oversight of U.S. companies from the Commerce Department and Federal Trade Commission, and establishes new requirements such as mandatory disclosures and referrals to Privacy Shield-related materials for participating businesses. On July 12, 2016, the European Commission formally adopted the Privacy Shield; however, its success is not guaranteed.

European Data Administrators

An important but little-known group of European officials dealing with data regulations is known as the Article 29 Working Party. These government employees are charged with the duty, sometimes subject to limited judicial review, of determining what discovery to allow in a particular case. Some of these officials are receptive to transfer of data to the United States, and they often use a type of balancing interest similar to that set forth in *Aerospatiale*. Some are receptive of negotiation and advocacy by lawyers or even the judge in a particular case.

Assuming it is warranted by the merits and importance of the case, retaining local counsel to conduct the negotiation with the data administrator would be essential.

In April 2016, the Article 29 Working Party issued a statement and corresponding opinion on the viability of the proposed Privacy Shield. The group criticized the Privacy Shield for its overall lack of clarity, opined that the proposed redress mechanisms might be too difficult for E.U. residents to use, and raised the specter of continued mass-data collection by the U.S. government. Other privacy advocates similarly believe the Privacy Shield does not go far enough in protecting personal data. Although the adoption of the Privacy Shield by the European Commission should ease the continued flow of data related to transactions, the opposition of powerful data administrators may create problems for continuing transfer of data in private litigation.

General Data Protection Regulation – Effective May 2018

The European Union also has adopted a lengthy and very complex set of regulations for cross-border discovery, which is scheduled to go into effect in May 2018. Titled "General Data Protection Regulation (GDPR)," it will become law in all states of the European Union and includes onerous dictates about transferring data out of a host country. One of the most severe provisions is Article 48, which basically prevents any kind of data transfer unless pursuant to the Hague Convention or any other type of treaty (generically referred to as a mutual legal assistance treaty or MLAT). The recent exit of Great Britain from the E.U. may show that traditional standards apply to requests for discovery from Britain.

Practical Suggestions for Overseas Discovery

- "Routine" requests for pretrial discovery, such as interrogatories, document requests, requests for admissions, and depositions — frequently sought from overseas corporations doing business in the United States — face the most difficulties. Corporate defendants quite legitimately assert that the laws of their host country bar production of this information. Generally speaking, the majority of U.S. judges who have dealt with an objection of this nature have overruled it, concluding that the corporation's business activities in the United States justifiably subject it to U.S.-based pretrial discovery.[18] The failure to produce the discovery may lead to a sanction and possibly a default. Therefore, carefully tailored decision making is recommended. A judicial opinion will have more weight than a mere "request" by counsel.
- Notwithstanding the hostility of many foreign countries to pretrial discovery as practiced in the United States, there are precedents allowing for document production and sworn testimony, particularly for use in a trial context, outside of the Hague procedures. Thus, although a party that seeks pretrial discovery may find a shut door, very often when trial is approaching a specific request for certain documents necessary for use at trial, or testimony from an individual who cannot be required to come to the United States, may be allowed.

  If one or more parties shows that "necessary" evidence is located overseas, a U.S. judge faced with an approaching trial date should frame a court order focused on the specific evidence the judge finds "necessary" and should explain, in sufficient detail, the efforts a party has made to secure the information. A written judicial opinion articulating reasons why the discovery requested is "necessary" will give important weight to the request. An explanation also should be given showing that the request is "proportional" to the overall needs of the case.[19]
- Emphasize the benefits rather than the burdens of electronic discovery. For all of the complaints, expense, and burdens some judges attribute to ESI, the fact remains that ESI has dramatically increased productivity and prompted many successes in the

"FOR ALL OF THE COMPLAINTS, EXPENSE, AND BURDENS SOME JUDGES ATTRIBUTE TO ESI, THE FACT REMAINS THAT ESI HAS DRAMATICALLY INCREASED PRODUCTIVITY AND PROMPTED MANY SUCCESSES IN THE SEARCH FOR TRUTH, WHICH (ONE HOPES) IS THE PURPOSE OF DISCOVERY.

search for truth, which (one hopes) is the purpose of discovery. By intelligent adoption of search terms and other devices (often suggested by one of many private vendors with expertise in fashioning protocols for electronic discovery), lawyers have been more successful, sometimes at a high cost, in finding facts that help them and their clients in proving or denying allegations made in pleadings. Computer-assisted technology has opened new frontiers in the search for underlying facts, associating names with documents, and finding communications (however old, cryptic, or disguised), as well as funding the careers of lawyers with expertise in electronic discovery. Many large law firms, in fact, have components devoted exclusively to electronic discovery in litigation or transactional work, almost as a "staff" component.

- If the court needs to make a determination about foreign law, Rule 44.1 provides the approach that district court judges must use. A number of precedents are available to guide the court in the application of Rule 44.1.[20]
- Conferences on cross-border discovery have shown that many foreign data administrators, and foreign judges, have misunderstandings about U.S. discovery. Some do not understand that although parties may make very broad requests, the judge will enter an order granting or denying certain discovery requests if there is a disagreement among the parties. As noted above, a judicial order stating why the foreign discovery is "necessary" will go a long way in persuading a foreign judge or data administrator to provide the information, particularly when accompanied by an explanatory memorandum or opinion.[21] After notice to the parties, a U.S. judge can individually (but acting in official capacity) contact a data administrator or foreign judge and, perhaps in a conference call with counsel, urge that the sought-out discovery be provided, emphasizing that it is needed for specific issues at a forthcoming trial. Various counsel handling these issues in a foreign context have verified that this is established practice in many countries, and several E.U. data administrators have confirmed their participation in these discussions and that such discussions are entirely proper.

  Some overseas data administrators and judicial officers may have an initially negative reaction to any and all U.S. discovery requests, based on past exposure to what they considered overbroad pretrial U.S. discovery requests. To remedy this "reputational handicap," some thoughtful judicial outreach will be helpful. This outreach should explain the recent tightening of discovery with the Rule 26 amendments in 2015, particularly endorsing the "proportionality" requirement.

  Specifically, a pretrial order (and supporting opinion) for overseas discovery should emphasize that the assigned judge, after review of the parties' contentions, has found that the requested discovery is both "relevant" and also "necessary" for the trial of the case. Adding a citation to the 2015 Rule 26 amendments — and explaining that these amendments were designed to curtail overly broad and unduly expensive discovery — may be persuasive.

Protective Orders

The concept of "privacy" is highly valued, particularly in a litigation context. The customary protective order that most U.S. trial judges approve when there is significant proprietary or other confidential information involved in litigation is not as accepted overseas as paving the road to discovery. Data-protection administrators, who may negotiate the terms of any U.S.-based discovery requests, may be willing to allow production of the information if it will be accessed only by the lawyers or clients involved in the U.S. litigation but will not be otherwise available.

Some courts have adopted different rules when national security interests are at stake.[22]

A recent handbook published in 2015 on these topics by the Federal Judicial Center, available to judges as well as the public, is valuable. Titled "Discovery in International Civil Litigation – a Guide for Judges," the handbook reviews numerous judicial decisions in the United States, as well as the laws of many commercially important countries, in providing information to be used in U.S.-based litigation.[23] This handbook includes detailed case citations of opinions and orders on the topic of overseas discovery. The appendices describe discovery practice in selected jurisdictions, summarize the Hague Convention on taking evidence abroad in civil or commercial matters, provide sample letters rogatory, and contain a sample Rule 16 pretrial order addressing international discovery issues, prepared by the author of this article.

A Case Study – *Wultz v. Bank of China*

In Tel Aviv, Israel, a suicide bomber killed a Florida teenager and injured the teenager's father. The bomber belonged to the Palestinian Islamic Jihad ("PIJ"), an organization the U.S. government has labeled

as a Foreign Terrorist Organization and a Specially Designated Global Terrorist. The PIJ is therefore subject to stringent economic sanctions. The teenager's family sued the Bank of China ("BOC"), arguing that BOC aided and abetted terrorism because it failed to observe its statutory duties and facilitated dozens of wire transfers for PIJ, totaling millions of dollars.

Wultz shows how complicated cross-border discovery issues can become and resulted in many detailed opinions and orders resolving cross-border discovery disputes. This summary looks at five of those opinions, highlighting issues that can be raised in international litigation and how a judge's determined case management can result in a fair resolution of the cross-border issues after sequential discovery requests and motions to compel.

In *Wultz's* first discovery dispute, plaintiffs moved to compel production of documents by a Letter of Request pursuant to the Hague Convention. However, over 13 months passed after the Letter of Request was granted, and China's Ministry of Justice had yet to grant BOC permission to disclose the relevant documents.[24] Plaintiffs were seeking imposition of a "unilateral" resolution of the discovery dispute, while BOC's opposition argued that a "bilateral" resolution, according to the Hague Convention, was proper. Plaintiffs' motion implicated one of the central concerns in cross-border discovery, namely to what extent a U.S. court can employ its expansive discovery rules in obtaining discovery from a foreign entity.

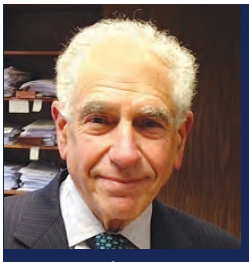
Judge Shira Scheindlin began her analysis by referencing *Aerospatiale's* holding that the Hague Convention did *not* provide the only means of obtaining foreign discovery. She acknowledged the important role of comity, as the dispute raised concerns of foreign sovereignty. She considered, in turn, the five *Aerospatiale* factors, and two additional factors dictated by the Second Circuit Court of Appeals. The most important factor requires balancing conflicting national interests. Judge Scheindlin weighed not only the United States' interest in combatting terrorism by identifying and stopping its funding and China's national interest in enforcing its bank secrecy laws, but she also weighed the interests of both countries "in the bilateral resolution of cross-border legal enforcement issues."[25] After narrowing certain requests and weighing these factors, Judge Scheindlin compelled BOC's production of specific documents, but did *not* order production of "confidential regulatory documents *created by the Chinese government* whose production is clearly prohibited under Chinese law."[26]

A subsequent dispute concerned BOC's withholding of certain documents identified in a privilege log.[27] Judge Scheindlin was again compelled to complete a choice-of-law analysis, except this time with respect to privilege claims involving foreign documents. According to Second Circuit precedent, a district court must use the "touch base" analysis to determine "which country 'has the predominant or the most direct and compelling interest in whether those communications should remain confidential.'"[28] The "touch base" test is met where communications relate to U.S. legal proceedings or advice on U.S. law. Based on this test, the court found that documents created after Jan. 28, 2008 — the date of plaintiffs' demand letter — were governed by U.S. privilege law, while documents created before that date or afterwards, but not relating to the demand letter, were governed by Chinese privilege law. Accordingly, Judge Scheindlin ordered BOC to produce items on its privilege log governed by Chinese privilege law (which recognizes only a duty of confidentiality), as well as documents governed by U.S. law, as the attorney-client privilege did not apply.

In another dispute that may require judicial resolution in this increasingly globalized economy, Judge Scheindlin considered whether to compel production of investigative files and U.S. regulatory communications from both BOC and the U.S. Office of the Comptroller of the Currency (the "OCC").[29] The court noted that to compel agency compliance with discovery requests, plaintiffs must first exhaust their administrative remedies. The OCC, as with other federal banking regulators, developed administrative regulations governing the release of nonpublic information pursuant to what is known as the "Housekeeping Statute," 5 U.S.C. § 301. These regulations, upheld by the Supreme Court in *United States ex rel. Touhy v. Ragen,*[30] are colloquially referred to as *Touhy* regulations. While plaintiffs partially complied with administrative procedures by submitting a request to the OCC for the production of documents, plaintiffs also moved to compel production of documents not described in the request. Accordingly, plaintiffs had not exhausted their administrative remedies with respect to these documents, and Judge Scheindlin denied plaintiffs' motion to compel production from the OCC.

In yet more installments, nonparties Bank Hapaolim (an Israeli bank),[31] and the State of Israel[32] moved to quash subpoenas issued to them. BOC served a subpoena on Hapaolim pursuant to Federal Rule of Civil Procedure 30(b)(6) to obtain testimony of a corporate designee. Hapaolim challenged the subpoena as violating Rule 45's territorial limits on nonparty depositions, and on grounds of international comity. Judge Scheindlin rejected these arguments and denied Hapaolim's motion to quash. She found that although all individuals with relevant knowledge were at the bank's branch located in Israel, it would not be unduly burdensome to produce a witness for the U.S. deposition in light of digital communications, including the bank's ability to prepare New York branch employees via video conference with employees of Hapaolim's Israel branch. Furthermore, concerns of international comity favored disclosure because the U.S. interest in combating terrorism outweighed Israel's interest in enforcing its bank secrecy laws.

Similarly, Israel moved to quash a subpoena, served on it by BOC, which sought the deposition of a former Israeli national security officer.[33] Israel's motion



MICHAEL M. BAYLSON is a U.S. District Court judge for the Eastern District of Pennsylvania.

He thanks his current law clerks, Ilana D. Cohen, Stephen Henrick, and Selby Brown for their assistance with research on this article.

implicated the Foreign Sovereign Immunities Act ("FSIA"), 28 U.S.C. § 1602 *et seq.*, which the Supreme Court held governed sovereign immunity for states but not for foreign officials.[34] Rather, claims for sovereign immunity by foreign officials are determined by common law. Noting the dearth of case law, Judge Scheindlin nonetheless found that the former officer was immune from being questioned about information regarding acts taken or knowledge obtained in his official capacity.

Wultz remains a valuable resource when a judge must confront and weigh international comity and sovereignty against not only national interest but also personal tragedy.

CONCLUSION

In facing these difficult issues, trial judges can take comfort in that there are abundant resources to consult, and the judge has wide (and wise) discretion in deciding these disputes. Nonetheless, the ultimate decision will likely be novel and necessarily a venture into unknown territory, legal and perhaps geographic.

---

1 *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for S. Dist. of Iowa*, 482 U.S. 522, 538 (1987) (hereinafter *Aerospatiale*).

2 *See Convention on the Taking of Evidence Abroad in Civil or Commercial Matters*, Mar. 18, 1970, 847 U.N.T.S. 231, *available at* https://assets.hcch.net/docs/dfed98c0-6749-42d2-a9be-3d41597734f1.pdf.

3 *Aerospatiale*, 482 U.S. at 565; *see also In re Perrier Bottled Water Litig.*, 138 F.R.D. 348, 352 n.3 (D. Conn. 1991) (discussing French blocking statute).

4 Restatement of Foreign Relations Law of the U.S. (revised) (tentative draft no. 7, 1986) (approved May 14, 1986) (subsequently adopted as Restatement (Third) of Foreign Relations Law of the U.S., § 442(1)(c)).

5 *See Linde v. Arab Bank, PLC*, 706 F.3d 92, 111 (2d Cir. 2013) ("In general, the careful application of Restatement § 442 will faithfully adhere to the principals of international comity."); *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1474–75 (9th Cir. 1992) (applying the factors enunciated in the Restatement (Third) of Foreign Relations law in its analysis of discovery noncompliance).

6 *In re Activision Blizzard, Inc.*, 86 A.3d 531, 547 (Del. Ch. 2014).

7 *See United States v. Staples*, 256 F.2d 290, 292 (9th Cir. 1958) ("This Court, like all courts of the United States, has inherent power to issue Letters Rogatory."); *see also Lantheus Med. Imaging, Inc. v. Zurich Am. Ins. Co.*, 841 F. Supp. 2d 769, 777 (S.D.N.Y. 2012) (quoting 22 C.F.R. § 92.54) ("Both the issuance and enforcement of letters rogatory by U.S. and foreign courts 'rest entirely upon the comity of courts toward each other, and customarily embody a promise of reciprocity.'").

8 *See Intel Corp. v. Advanced Micro Devices, Inc.,* 542 U.S. 241, 255–56, (2004) (noting that § 1782 "authorizes, but does not require, a federal district court to provide assistance to a complainant in a European Commission proceeding" and delineating factors to guide courts in exercising their discretion); *Akebia Therapeutics, Inc. v. FibroGen, Inc.*, 793 F.3d 1108, 1111 (9th Cir. 2015) (*stayed pending further order*, 136 S.Ct. 1) (applying § 1782 to allow discovery for foreign "administrative and quasi-judicial proceedings"); *In re Gianoli Aldunate*, 3 F.3d 54, 59 (2d Cir. 1993) (holding § 1782 does not require that the discovery requested be discoverable under the laws of a foreign jurisdiction).

9 *Estate of Ungar v. Palestinian Auth.,* 412 F. Supp. 2d 328, 332 (S.D.N.Y. 2006); *see also Klesch & Co. v. Liberty Media Corp.,* 217 F.R.D. 517, 523 (D. Colo. 2003).

10 *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, No. 14-2985, 2016 WL 3770056 at *2 (2d Cir. July 14, 2016); *but see In re Uranium Antitrust Litig.*, 480 F. Supp. 1138, 1148 (N.D. Ill. 1979) (concluding that a district court can compel production of documents located abroad if "the particular defendant is within the personal jurisdiction of this court and has control over the requested documents").

11 *See Societe Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers, 357 U.S. 197, 205 (1958) (hereinafter Participations*), ("[T]o hold broadly that petitioner's failure to produce the . . . records because of fear of punishment under the laws of its sovereign precludes a court from finding that petitioner had 'control' over them, and thereby from ordering their production, would undermine congressional policies.").

12 *See generally Linde v. Arab Bank, PLC.*, No. 04-2799, 2009 WL 8691096 (E.D.N.Y. June 1, 2009).

13 The Sedona Conference Internatinal Principles on Discovery, Disclosure, & Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery of Protected Data in U.S. Litigation iv (Amor A. Esteban et al. eds., European Union ed. 2011).

14 Martin A. Weiss & Kristin Archick, Cong. Research Serv., *U.S.–EU Data Privacy: From Safe Harbor to Privacy Shield* (May 19, 2016), available at https://www.fas.org/sgp/crs/misc/R44257.pdf.

15 *See Paul M. Schwartz, The EU–U.S. Privacy Collision: A Turn to Institutions and Procedures,* 126 Harv. L. Rev. 1966, 1975 (2013).

16 Council Directive 95/46/EC, art. 25, 1995 O.J. (L 281) 45.

17 Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7–47.

18 *See, e.g., Linde v. Arab Bank, PLC,* 269 F.R.D. 186, 197 (E.D.N.Y. 2010) ("Defendant continues to assert that foreign bank secrecy laws require it to refrain from producing a range of documents . . . . This court has already rejected defendant's rationale for withholding the documents.").

19 The 2015 amendments to Federal Rule of Civil Procedure 26(b)(1), relocated from Rule 26(b)(2)(c)(iii), require parties and the court to consider proportionality.

20 *See Faggionato v. Lerner*, 500 F. Supp. 2d 237, 244 (S.D.N.Y. 2007) ("In acting under Rule 44.1, a court may reject even uncontradicted expert testimony and reach its own decisions on the basis of independent examination of foreign legal authorities").

21 Experience has shown that the more narrowly tailored the request, and the more significance the request will have at a trial, the better the chances of persuading the foreign judge or data administrator that the information should be provided.

22 *See, e.g.,* the *Wultz* case discussed in part 9, *infra*.

23 Timothy P. Harkness, Rahim Moloo, Patrick Oh & Charline Yim, Fed. Judicial Ctr., Discovery in International Civil Litigation: A Guide for Judges (2015).

24 *Wultz v. Bank of China, Ltd.*, 910 F. Supp. 2d 548, 551 (S.D.N.Y. 2012).

25 *Id.* at 559.

26 *Id.* at 556.

27 *Wultz v. Bank of China, Ltd.,* 942 F. Supp. 2d 452, 472–73 (S.D.N.Y. 2013).

28 *Wultz v. Bank of China, Ltd.,* 979 F. Supp. 2d 479, 486 (S.D.N.Y. 2013).

29 *Wultz v. Bank of China, Ltd.,* 61 F. Supp. 3d 272 (S.D.N.Y. 2013).

30 340 U.S. 462 (1951).

31 *Wultz v. Bank of China Ltd.,* 298 F.R.D. 91 (S.D.N.Y. 2014).

32 *Id.* at 486.

33 *Wultz v. Bank of China Ltd.,* 32 F. Supp. 3d 486, 489 (S.D.N.Y. 2014).

34 *Samantar v. Yousuf,* 560 U.S. 320 (2010).