



**CROSS-BORDER E-DISCOVERY:
NAVIGATING FOREIGN DATA PRIVACY
LAWS AND BLOCKING STATUTES
IN U.S. LITIGATION**

E-DISCOVERY WORKING GROUP

REISSUED FEBRUARY 2020

I. INTRODUCTION

These guidelines, published by the *E-Discovery Working Group* of the New York City Bar Association, address (a) the conflict that New York practitioners face when documents within the scope of a client's discovery obligations reside in a foreign jurisdiction that prohibits transferring those same documents to the United States and (b) strategies and workflows that will minimize, if not completely overcome, that conflict.

Over the last ten years, the need to navigate foreign laws during the domestic discovery process has arisen with increasing frequency as businesses continue to cross borders and foreign data privacy and other blocking statutes proliferate at unprecedented rates. Even disputes that appear on their face to be entirely domestic – *e.g.*, New York parties in a New York court applying New York law to New York conduct – can trigger transnational discovery obligations when potentially relevant documents happen to reside abroad. The circumstances triggering this conflict of laws are varied: a domestic entity might outsource its Information Technology or Human Resources functions to foreign service providers; a New York business might maintain its electronically stored information on a “cloud” platform that resides on physical servers located abroad; a party's foreign parent, affiliate or subsidiary company might possess potentially relevant documents.

Notwithstanding the complexity and increasing frequency with which this issue arises, there is little in the way of authoritative guidance on how practitioners can analyze and navigate this conflict of laws. Accordingly, the *E-Discovery Working Group* offers these *Guidelines* to the New York bar.¹

II. COMMON CIRCUMSTANCES TRIGGERING CROSS-BORDER DISCOVERY IN NEW YORK

Practitioners in New York should consider early in their representation whether foreign documents or information may be within the scope of their clients' domestic discovery obligations. While the circumstances that can trigger cross-border discovery obligations are too varied to set forth in a comprehensive matter, it is worth calling attention to the two most common scenarios: (a) when the New York court exercises jurisdiction over a foreign party (or a U.S. party with foreign offices, operations or agents) and (b) when a domestic party has a foreign parent, subsidiary or affiliate that possesses information potentially relevant to the underlying claims or defenses.

This paper does not purport to present a comprehensive analysis of either of these scenarios (each of which are sufficiently complex to warrant their own independent studies). Rather, it is the Working Group's goal to provide a high-level overview of the applicable legal principles to facilitate practitioners undertaking a preliminary assessment of whether cross-border discovery concerns are likely to arise in their engagements.

¹ This report is meant to be informational only. It is not intended to be - and should not be relied upon as - legal advice regarding a particular situation, nor should it substitute for the advice of a lawyer.

a. Personal Jurisdiction over Foreign Parties under New York Law

As a general matter, courts “may exercise two types of personal jurisdiction over a corporate defendant properly served with process. . . . specific (also called ‘case-linked’) jurisdiction and general (or ‘all-purpose’) jurisdiction.” *Brown v. Lockheed Martin Corp.*, 814 F.3d 619, 624 (2d Cir. 2016). See New York Civil Practice Law & Rules (“CPLR”) §§301, 302.

Within the last decade, the Supreme Court has limited the scope of both general and specific personal jurisdiction over foreign parties. In *Goodyear Dunlop Tires Operations, S.A. v. Brown*, 564 U.S. 915, 919 (2011), the Court explained that “[s]pecific jurisdiction . . . depends on an affiliatio[n] between the forum and the underlying controversy, principally, activity or an occurrence that takes place in the forum State and is therefore subject to the State’s regulation.” *Id.* (citation and quotation marks omitted). In that case, Goodyear, an Ohio corporation, was sued in North Carolina state court over an allegedly defective tire manufactured in Turkey that caused a bus accident in France. *Id.* at 920. The Court concluded that, “[b]ecause the episode-in-suit, the bus accident, occurred in France, and the tire alleged to have caused the accident was manufactured and sold abroad, North Carolina courts lacked specific jurisdiction to adjudicate the controversy.” *Id.* at 919.

Further, in *Daimler AG v. Bauman*, the Supreme Court concluded that Daimler’s contacts in California were insufficient to support general personal jurisdiction in that state because “Daimler’s slim contacts with the State[,]” given that the company and its named entities were not incorporated in California or had a principal place of business there, “hardly render it at home there.” 571 U.S. 117, 136 (2014)..

Courts in New York have routinely applied the Supreme Court’s guidance from *Goodyear* and *Daimler* concerning the scope of personal jurisdiction over foreign entities. See e.g., *Brown*, 814 F.3d at 623; *Lopez v. Shopify, Inc.*, 16 Civ. 9761 (VEC) (AJP), 2017 WL 2229868, at *7 (S.D.N.Y. May 23, 2017).

b. Domestic Parties with Foreign Parents, Subsidiaries or Affiliates

The other common circumstance that practitioners should assess when determining whether foreign documents potentially are within the scope of their client’s discovery obligations is whether the client has a foreign parent, subsidiary or affiliate that possesses information relevant to the underlying claims or defenses.

In New York, CPLR Article 31 governs the production and disclosure of documents. CPLR 3111 applies to production of documents for use at a deposition, while CPLR 3120 applies to the service of a document demand or subpoena duces tecum. Under both sections, New York law allows a party to discover books, papers, documents, and “other things” that are “in the possession, custody, or control of” either the person being examined or the recipient of the subpoena duces tecum. Likewise, under Rules 34 and 45 of the Federal Rules of Civil Procedure, parties and non-parties receiving a subpoena must produce documents and information in their “possession, custody, or control.” Unfortunately, neither the CPLR nor the Federal Rules define “possession, custody, or control” and as such, litigants are required to rely upon inconsistent

caselaw. Indeed, the interpretation and application of “possession, custody, or control” in the intra-corporate context is an issue of significant debate.

Practitioners should be aware, however, that New York courts have in certain situations construed ‘control’ broadly “as the legal right, authority, or practical ability to obtain the materials sought upon demand.” *S.E.C. v. Credit Bancorp, Ltd.*, 194 F.R.D. 469, 471 (S.D.N.Y. 2000); *see also Shcherbakovskiy v. Da Capo Al Fine, Ltd.*, 490 F.3d 130, 138 (2d Cir. 2007) (“[I]f a party has access and the practical ability to possess documents not available to the party seeking them, production may be required.”).

Under such a standard, determining whether a party has sufficient “control” over the documents of a foreign entity is a pragmatic and fact-intensive inquiry. “In deciding whether a subpoenaed domestic corporation can be compelled to produce documents held by a foreign affiliate, a court must consider the nature of the relationship between the corporation and its affiliate.” *Zenith Elecs. LLC v. Vizio, Inc.*, Misc. No. M8–85, 2009 WL 3094889, at *1 (S.D.N.Y. Sept. 25, 2009) (citations and quotation marks omitted). Courts may look to whether “the degree of ownership and control exercised by the parent over its subsidiary, a showing that the two entities operated as one, demonstrated access to documents in the ordinary course of business, and an agency relationship.” *Dietrich v. Bauer*, No. 95 Civ. 7051(RWS), 2000 WL 1171132, at *3 (S.D.N.Y. Aug. 16, 2000) (citation omitted); *cf.*, *Linde v. Arab Bank, PLC*, 262 F.R.D. 136, 141-42 (E.D.N.Y. 2009) (holding there was inadequate control between a nonparty foreign bank and its indirect, wholly-owned domestic subsidiary to compel the disclosure of documents because the domestic subsidiary did not have access to its foreign parent’s documents in the regular course of business, the two companies had different computer systems, and the two entities did not share with each other confidential information relating to customers and transactions).

Recognizing that the case law concerning “control” in the intra-corporate context “is unclear and, at times, inconsistent . . . resulting in a lack of reliable legal—and practical—guidance[.]” the Sedona Conference, one of the leading think tanks on U.S. discovery issues, published *The Sedona Conference Commentary on Rule 34 and Rule 45 “Possession, Custody, or Control.”* 17 Sedona Conf. J. 467, 475 (2016) (the “Sedona Commentary”).

The Sedona Commentary advocates “abolishing use of the common-law ‘Practical Ability Test’” because it leads to the “inequitable” result of a party being required to preserve and produce documents that the party does “not have the *actual ability* to obtain[.]” *Id.* at 476 (emphasis in original). More specifically, in the intra-corporate context, the Sedona Commentary argues that the “Practical Ability” test carries a panoply of unfair consequences:

1. “[T]he Practical Ability Standard [] require[s] parties with cross-border obligations to produce Documents and ESI from related entities with foreign operations, even when such production causes the entity to violate foreign data privacy laws.” *Id.* at 500.
2. “[T]he Practical Ability Standard . . . obligate[s] sister corporations to obtain documents from each other when each has ties to a common parent corporation, notwithstanding the fact that the entities may lack a sufficient relationship to warrant the imposition.” *Id.* at 507.

3. “[T]he Practical Ability Standard . . . find[s] that employers have Rule 34 ‘control’ over documents in the possession of former employees.” *Id.* at 511

Thus, the Sedona Commentary advocates narrowing the definition of “control” to require either actual possession or the legal right to obtain and produce” the requested discovery. *Id.* at 477.

III. THE RULES GOVERNING CROSS-BORDER DISCOVERY

When documents potentially within the scope of discovery are identified abroad, counsel should next consider what rules will govern their disclosure. The following summarizes the panoply of potentially-applicable legal regimes to guide the practitioner’s analysis of what laws may be impacted by the discovery of foreign data in U.S. courts (and how to navigate any resulting conflict of laws). Once again, this section does not purport to present a comprehensive analysis of the potentially-applicable legal regimes, but rather a basic overview to guide a more detailed, case-specific analysis.

a. The CPLR

Provisions in the CPLR explicitly addressing cross-border discovery are limited. CPLR 313 governs service of process to persons domiciled in the state or subject to the jurisdiction of the state courts. It provides that such persons may be served with the summons outside of the state in the same manner as service is made within the state by any person authorized to make service within the state. The defendant must be domiciled in New York or must have participated in acts or transactions that render him or her subject to personal jurisdiction under CPLR Sections 301 (jurisdiction over persons, property, or status) or 302 (personal jurisdiction by acts of nondomiciliaries). In a case involving the efforts of the plaintiff to obtain the proceeds of an allegedly illegal international money transfer scheme engaged in by a defendant who was operating out of Brazil, the New York Court of Appeals found service of process pursuant to CPLR Section 313 to be sufficient where “no treaties or international agreements supplant New York’s service requirements.” *Morgenthau v. Avion Resources Ltd*, 11 N.Y.3d 383, 385 (2008). The Court further found that “principles of international comity do not mandate a different result.” *Id.* Beyond these provisions, the CPLR offers little guidance on cross-border discovery.

b. The Federal Rules of Civil Procedure

The Federal Rules provide that parties may obtain discovery regarding any non-privileged matter that is “relevant to any party’s claim or defense and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties’ relative access to relevant information, the parties’ resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.” Fed. R. Civ. P. 26(b)(1). This broad dictate is severely at odds with the laws of most foreign countries, where privacy is considered an absolute right and the American practice of pre-trial discovery is viewed generally with skepticism. Nonetheless, under Rule 34,

litigants are compelled to produce discoverable materials within their “possession, custody or control.”

Rule 4(f) establishes the protocol for effective service beyond the borders of the United States. It directs litigants to select “any internationally agreed means of service that is reasonably calculated to give notice,” such as the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, *opened for signature* March 18, 1970, 23 U.S.T. 2555 (the “Hague Convention”). The rule provides for a number of alternative methods where “there is no internationally agreed means, or if an international agreement allows but does not specify other means, by a method that is reasonably calculated to give notice.”

c. Federal Statutes

Federal legislation addressing varying aspects of cross-border litigation are available to parties under the right circumstances. Most relevant to this discussion is 28 U.S.C. § 1781, which authorizes the State Department “to receive a letter rogatory issued, or request made, by a tribunal in the United States, to transmit it to the foreign or international tribunal, officer, or agency to whom it is addressed, and to receive and return it after execution.” In this instance, reciprocity is key. The U.S.-based attorney and judge will need to verify that the practice of letters rogatory is recognized in the host country.

d. Treaties

The Hague Convention is often cited as the go-to treaty for relief in international discovery disputes. The Hague Convention is intended to enable litigants to enlist the aid of the laws and procedures of the Convention’s signatory nations to obtain evidence for use in civil or commercial matters. Evidence is generally obtained pursuant to a letter of request that is transmitted through a Central Authority in the receiving country. The Convention provides that signatories “shall organize the Central Authority in accordance with its own law,” so the powers exercised by the Central Authority in each of the signatory nations may differ.

Although the Convention generally operates as intended, litigants should be aware of its limitations. It is binding only on the nations that have ratified it, and its provisions are not uniformly applied throughout those signatory states. Some signatories either prohibit or curtail the use of letters of request for purposes of obtaining pre-trial discovery, which means that in addition to being required to identify the documents they wish to obtain with some particularity, litigants must be able to establish that these documents will actually be used as evidence at trial. The Hague Convention applies only to civil or commercial matters and only where the address of the person to be served is known. Finally, the procedures required under the Hague Convention can be time-consuming, inefficient and limited in scope, all of which can be significant concerns for litigants with short deadlines or aggressive procedural calendars.

In *Societe Nationale Industrielle Aerospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522 (1987) (“*Aerospatiale*”), which involved a lawsuit against French aircraft manufacturers, defendants argued that the American plaintiffs were required to go through the procedures established by the Hague Convention to obtain discovery of the defendants’ foreign

documents. The Supreme Court disagreed, finding that under the circumstances of that case, the Hague Convention's procedures regarding foreign service did not deny a United States court of the authority to order a party subject to its jurisdiction to produce evidence (even though in that case, the act of production was alleged to have violated a foreign blocking statute). *Id.* at 542-44. In that case, the Court determined that the Convention was neither a required first resort nor the exclusive method to obtain evidence located outside the United States. In its opinion, the Supreme Court stressed the prominent role that international comity should play in the District Court's regulation of international discovery.² The Court referenced a five-factor balancing test³ that, in essence, mirrors the framework set forth in the Restatement (Second) of Foreign Relations Law and which the Court noted is "relevant to any comity analysis." *Id.* at 544 n.28.

Like the Hague Convention, the Inter-American Convention on Letters Rogatory and Additional Protocol ("IACAP")⁴ facilitates obtaining foreign discovery from signatory countries. Although the application of IACAP is limited to civil and commercial matters, countries may choose to apply it to criminal and administrative matters. Signatories to IACAP may or may not also be members of the Hague Convention. Brazil, for example, is not a signatory to the Hague Convention, so the Convention is not implicated in connection with service on Brazilian nationals. However, both the United States and Brazil are signatories to IACAP.

e. Contracts or Agreements between the Parties

Parties can (and are encouraged to) negotiate a discovery and confidentiality agreement that will resolve various issues related to discovery in pending litigation and that can be adopted by a court order. While such agreements may not entirely resolve the conflict of law presented by foreign blocking statutes, as described in Section VII below, certain provisions relating to the use, security and redaction of foreign documents can be very helpful in navigating the conflict.

IV. FOREIGN LAWS RESTRICTING DISCOVERY OF DOCUMENTS LOCATED ABROAD

The American Bar Association ("ABA") has emphasized the increasingly global nature of litigation, noting that "the daily interfaces essential to cross-border commerce and dialogue, including through electronic information transfers, call for recognition of the exigencies of other legal systems, and where warranted, application of their privacy and data protection laws." Resolution 103, Adopted by the House of Delegates, American Bar Association (Feb. 6, 2012). The ABA has thus urged consideration and respect for the data protection and privacy laws of "any

² Edmund M. O'Toole and David N. Cinotti, *E-Discovery in Cross-Border Litigation: Taking International Comity Seriously* by, Int'l Dispute Resolution News (Fall 2010).

³ (1) the requested document's or information's importance to the litigation; (2) the degree of specificity in the request; (3) whether the information was created in the United States; (4) whether the information could be obtained by alternative means; and (5) the extent to which compliance or noncompliance would subvert important interests of the United States or the nation where the information was located.

⁴ Inter-American Convention on Letters Rogatory, Jan. 30, 1975, and Additional Protocol to the Inter-American Convention on Letters Rogatory, May 8, 1979, S. Treaty Doc. No. 98-27.

applicable foreign sovereign, and the interests of any person who is subject to or benefits from such laws, with regard to data sought in discovery in civil litigation.” *Id.*

Data privacy laws have, in one form or another, been enacted in over eighty nations worldwide. Such laws seek to protect a person’s personal information from disclosure or misuse. The nature and scope of the afforded protection varies widely as do the penalties for unauthorized disclosure.

The most stringent of these laws is arguably that found in the European Union. For many years, data privacy in Europe was governed by the Data Protection Directive 95/46/EC, a set of data privacy guidelines that each Member State of the EU was required to implement through national legislation. The EU General Data Protection Regulation (“GDPR”) (effective May 25, 2018), replaced Data Protection Directive 95/46/EC and its accompanying implementing statutes. The GDPR is an attempt to harmonize differences found within the various national implementing statutes, as well as to simplify and enhance enforcement procedures.

For the purposes of these guidelines, one of the most important aspects of the GDPR is the prohibition against transferring “personal data” – that is, data that relates to a living individual who can be identified from that data – outside the European Economic Area unless the destination country provides an “adequate level of protection.” GDPR, Articles 44-45(1). While the U.S. is not considered to provide an “adequate level of protection,” at the time of publication of these guidelines, the U.S. and the E.U. have in place a Privacy Shield arrangement. Pursuant to the Privacy Shield, transfers of personal data to the U.S. are permissible if the U.S. entity receiving the personal data self-certifies that it will treat the data confidentially and securely in accordance with the Privacy Shield requirements. One of those requirements, however, is that there will be no “onward transfer” of the personal data to a third party in the U.S. This requirement thus effectively prohibits document “productions” in a litigation or governmental investigation. In turn, in the context of e-discovery, the Privacy Shield is not a valid basis upon which to overcome the prohibition against cross-border transfers of personal data contained in Article 44.

Article 49 of the GDPR, however, contains additional “derogations” from Article 44, which do apply in the context of U.S. e-discovery. Specifically, Article 49(1)(e) permits such transfers when “necessary for the establishment, exercise or defence of legal claims[.]” The European Data Protection Board, which is the EU regulatory body in charge of the application of the GDPR, has affirmed that the exception in Article 49(1)(e) applies specifically to pre-trial discovery proceedings, but has cautioned that due attention be paid to the qualifier “necessary” within the text. Specifically, this qualifier means that Article 49(1)(e) does not permit the wholesale transfer of EU personal data to the U.S. for discovery purposes, but first requires “data minimization” to ensure that “only a set of personal data that is actually necessary is transferred and disclosed.”

Outside of privacy laws, many foreign countries have additional “blocking statutes” restricting the extraterritorial transfer of documents. France, for example, has a broad blocking statute. Article 1 of the French statute prohibits communicating to foreign public officials “documents or information of an economic, commercial, industrial, financial or technical nature and the communication of which is against the sovereignty, security, or essential economic interest

of France, or its public policy.” French Penal Law Code no. 80-538. The compliance with a foreign discovery order, in most instances, is thus a punishable crime in France.

When a U.S. litigant is faced with a data privacy or other blocking statute, transferring potentially responsive documents to the U.S. can be problematic and, in some cases, criminal. As noted above, the United States Supreme Court addressed the French blocking statute in *Aerospatiale*. There, the defendants, French aircraft manufacturers, argued that they had no obligation to produce documents in response to plaintiffs’ requests because the French blocking statute required that service be executed through the Hague Evidence Convention, which plaintiffs had not utilized. The defendants argued that complying with the non-Hague requests would constitute a violation of the French blocking statutes and would expose defendants to criminal liability in France.

The Supreme Court held that in the circumstances of that case, the French blocking statute did “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.” *Aerospatiale*, 482 U.S. at 544 n.29.

In *Motorola Credit Corp. v. Uzar*, 73 F. Supp. 3d 397, 404 (S.D.N.Y. 2014), the court contrasted the Swiss Bank Secrecy Act with the French blocking statute:

In contrast with the French situation, Switzerland’s bank secrecy regime constitutes, not just a seriously enforced national interest, but an element of that nation’s national identity.... Switzerland’s recent cooperation with U.S. authorities in pursuing such tax evasion suggests that ...Switzerland regards bank secrecy as a positive social value and benefit, to be used but not abused. In such circumstances, a balancing of interests strongly favors denying the release of subpoenaed information from bank branches located in Switzerland, and the *Aerospatiale* factors do not overcome this conclusion. Accordingly, the Court quashes the subpoenas to the extent they seek documents located in Switzerland.

Further, some nations, most notably China, have broadly-applicable “state secrets” acts. The *Law of the Peoples Republic of China on Guarding State Secrets* broadly prohibits the exportation or dissemination of data that the Chinese government would consider to include matters bearing on state security and state secrets without first obtaining governmental review and clearance. Violation of this somewhat vague and ambiguous requirement subjects the individual to criminal prosecution.

V. REPRESENTATIVE CASE LAW REGARDING BLOCKING STATUTES

As discussed above, the concept of “comity” between nations figures prominently in requests for evidentiary documents between U.S. courts and foreign sources of information. *Aerospitale* adopted the following five-factor test from the Restatement of Foreign Relations Law of the United States § 437(1)(c) (revised and approved on May 14, 1986):

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
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.

Many American courts have addressed this issue in a wide variety of contexts. This paper does not purport to be an extensive survey of the resulting case law, but offers the following examples of how some courts have analyzed the particular facts presented in order to resolve the issues raised by “blocking” statutes and similar laws restricting the transfer of documents to the U.S. for discovery.

In *A.G. Volkswagen v. Valdez*, 897 S.W.2d 458 (Tx. 1995), a mandamus proceeding after the Texas trial court ordered production of evidence pertaining to a personal injury case, Plaintiff sought to protect its corporate employee records from discovery on the ground that it would violate the German Federal Data Protection Act. Following *Aeropostiale*, the court in *Volkswagen* applied the Restatement’s five-part “balancing test” to determine that the interests of the parties obtaining the requested material outweighed that of Germany in prohibiting its disclosure. *Id.* at 464-65. As a result, the trial court was found to have acted within its discretion in ordering production. *Id.*

In *Salerno v. Lecia, Inc.*, No. 97-CV-973S(H), 1999 WL 299306 (W.D.N.Y. Mar. 23, 1999), an employment discrimination suit before U.S. District Court for the Western District of New York, plaintiff sought personnel documents of European employees. Defendant argued that the information sought could not be disclosed to third parties in the United States without consent of the European data subjects or assurance that identical levels of privacy protections would apply in the U.S. According to defendant’s European counsel, United States safeguards were considered inadequate compared with European law and thus, production in the U.S. would have marked legal consequences for defendants in Europe. The court agreed with the need to comply with these European privacy laws, and held that the document requests were overly burdensome, given the great number of Defendant’s non-party corporate divisions across many countries. The court further deemed the employee information sought to have little relevance to Plaintiff’s claims. Plaintiff’s motion to compel was thus denied.

In *Las Vegas Sands Corp., v. Eighth Judicial District Court of the State of Nevada*, Index No. 10-A-627691(Dist. Ct. Clark Co., March 6, 2015), another employment dispute, one of the defendants, a Chinese corporation, maintained that it was unable to disclose requested documents residing in Macau due to the Macau Personal Data Protection Act. The court applied the Restatement five-factor test and determined that in the circumstances presented, the need for the documents outweighed the interests of the foreign statute. Specifically, the court noted that the defendant “cannot dispute the relevancy of the unproduced documents” and that the foreign state’s interests in preventing the discovery appeared minimal in light of the fact that prior violations had resulted in relatively small fines. *Id.* at 30-33.

VI. PRIVILEGE LAW AND CROSS-BORDER E-DISCOVERY

Significant privilege issues also arise in the context of cross-border e-discovery. Other jurisdictions' privilege law may not mirror that of the U.S., which may lead to the unwarranted withholding of documents incorrectly believed to be privileged. In addition, it is necessary to plan carefully in order to best protect foreign entities' communications from being compromised in the context of U.S. litigation where the protections afforded by the attorney client privilege and the work product doctrine may not be available or may not be as broad in the relevant foreign jurisdiction as they are in the U.S..

One issue that arises is the application of the attorney client privilege to in-house counsel in the European Union. In *Akzo Nobel Chemicals, Ltd. v. European Commission*, Case C-550/07 P (Sep. 14, 2010), the Court of Justice of the European Commission determined that in the context of investigations by the European Competition Commission, attorney-client or legal professional privilege does not attach to communications between in-house counsel and their employers. While it is unclear to what extent this decision will be followed within individual E.U. countries and outside of the context of antitrust investigations, the *Akzo Nobel Chemicals* determination underscores the necessity of being mindful of key differences between U.S. and foreign application of the attorney client privilege.

Another privilege issue that arises is the question of which jurisdiction's privilege law applies. Federal courts in New York have applied a "touch base" test pursuant to which the court "must apply the law of the country that has the predominant or the most direct and compelling interest in whether ... communications should remain confidential to disputes involving foreign attorney-client communications, unless that foreign policy is contrary to the public policy of [the] forum." *Veleron Holding B.V. v. BNP Paribas, SA*, 12-CV-5966 (CM) (RLE), 2014 U.S. Dist. LEXIS 117509, at * 11 (S.D.N.Y. Aug. 22, 2014) (citations omitted) (determining that, under facts presented, touch base analysis favored application of Russian and Dutch law neither of which provided for attorney client privilege in these circumstances). *See also Wultz v. Bank of China*, 979 F. Supp. 2d 479, 485 (S.D.N.Y. 2013) (applying Chinese law, which does not recognize the attorney client privilege or work product doctrine and rejecting privilege claim over certain Chinese documents).

VII. BEST PRACTICES AND GUIDELINES TO NAVIGATE FOREIGN LAWS DURING DOMESTIC DISCOVERY

In this final Section, the Working Group addresses strategies and workflows that practitioners can take to minimize, if not completely overcome, the conflict that occurs when documents within the scope of a client's discovery obligations reside in a foreign jurisdiction that prohibits transferring them to the United States.

a. Plan Early, Plan Often

To the extent counsel believes that documents that reside abroad may be within the scope of their clients' discovery obligations, it should inquire with the client's IT department whether any corporate data sources that may contain potentially responsive materials reside on foreign

servers (*e.g.*, if the client utilizes “cloud” platforms, counsel should assess the physical location of the underlying servers). Likewise, counsel should review the client’s organizational structure to assess whether any corporate divisions, affiliates, parents or subsidiaries that exist abroad may possess relevant documents.

To the extent that potentially relevant documents reside in a jurisdiction with data privacy laws or other blocking statutes restricting the transfer of those documents to the United States for discovery and production purposes, it is imperative that counsel identify and raise that issue as early as possible in the proceedings.

b. Be Transparent and Cooperative; Address Cross-Border Discovery Issues in Discovery Meet-and-Confers and the Resulting Confidentiality Order and/or Discovery Stipulation

If potentially relevant foreign documents are identified, counsel should address the impact of any applicable foreign blocking statutes or data privacy laws promptly so that measures to navigate the conflict of laws can be explored and addressed in the governing confidentiality order and/or discovery stipulation. In the *Las Vegas Sands* case, discussed in Section V, *supra*, counsel’s failure to promptly identify and proactively address these issues resulted in substantial sanctions. In that decision, the court went out of its way to chastise counsel for failing to raise the Macau data privacy laws and their impact on discovery during the parties’ discovery meet-and-confers or in the resulting joint stipulation on discovery.

Amongst other measures that can be embodied in the confidentiality order and/or discovery stipulation are the following.

1. A rolling production schedule to provide the time necessary to review and redact foreign documents abroad, seek permission from foreign data subjects to transmit the data to the U.S. for production or, failing that, seek such consent from relevant foreign regulators.
2. Confidentiality and information security provisions, including permission to file documents with personal information under seal and provisions governing how the receiving party will utilize and protect personal data. Such measures will prove invaluable when seeking the approval of foreign data subjects and/or foreign regulators to transfer the relevant documents to the U.S.
3. Agreements on the use of redactions to anonymize or pseudonymize personal data to mitigate the impact of foreign privacy laws.

c. Choose a Service Provider with Foreign Infrastructure and Services

In the context of cross-border e-discovery, look for service providers with infrastructure (*i.e.*, data centers and project management teams) in the jurisdiction where the data is located. While the GDPR, for example, prohibits the transfer of personal data from an EU member state to the U.S., it does not prohibit such transfer to another EU member state or to any other foreign country that provides an “adequate level of protection.” Likewise, as discussed in more detail above, under Article 49(1)(e) of the GDPR, if the relevant data set is “minimized” abroad, it can then be transferred to the U.S. for document production. Thus, service providers that offer data

processing and hosting facilities within the jurisdiction where the data resides (or for the E.U., another jurisdiction offering an adequate level of protection) can offer immediate solutions.

Even better, some service providers can travel to the client's foreign offices or data centers and establish a temporary, on-premises e-discovery environment to collect, process, review and redact documents in-country.

Lastly, look for a vendor with data privacy consulting expertise. In the complex and nuanced intersection of U.S. and foreign legal obligations, your service provider should be your partner and trusted advisor, not merely a resource to execute tasks on command.

d. Use Emerging Technology

Finally, take advantage of cutting edge technology that can be introduced into the discovery workflow to effect a streamlined, cost-efficient process. For example, "regular expression scripting" software empowers you to automate searches for certain types of personal information within the data set. Once identified, such data can be set aside for a separate privacy review, redaction or approval from data subjects or foreign regulators. Meanwhile, the remainder of the data set that does not contain personal data can be transferred immediately to the U.S. for a traditional discovery workflow and rolling production.

Emerging technologies can also facilitate the automated redaction of certain types of personal information. This results in a far more efficient and reliable privacy review. Through redaction, the data set can be anonymized of personal information rendering it outside the scope of foreign privacy law altogether.

VIII. CONCLUSION

Businesses continue to transcend national borders at unprecedented rates. As a result, it is increasingly rare to represent a purely "domestic" corporate client. At the same time, foreign data privacy laws and other blocking statutes that prohibit the wholesale transfer of foreign documents to the United States are proliferating on a global basis. The result is a "catch-22" pitting domestic discovery obligations against foreign data transfer restrictions. Only through proper foresight and planning can the savvy practitioner mitigate, if not entirely overcome, this conflict of laws.

E-Discovery Working Group
Daniel S. Meyers, Chair

Reissued February 2020