BNA, INC.

PRIVACY & SECURITY LAW

BNA Employee-Owned Since 1947

REPORT

The rising tide of globalization has meant that, more frequently than ever before, multinational corporations must navigate between U.S. litigation discovery demands seeking the production of documents and information located in the European Union and EU data protection requirements. The authors examine the arguments available in U.S. litigation for resolving conflicting laws, and suggest an approach they say lawyers and business people can take to try to navigate through the rocky shoals of U.S. discovery obligations (the proverbial ''rock'') and EU data protection authorities (the proverbial ''hard place''). Notwithstanding conflicting obligations, there are means today to navigate this legal morass, according to the authors, who suggest a way forward.

Mind the Gap: U.S. Discovery Demands versus EU Data Protection

By Karin Retzer and Michael Miller

I. THE SOURCES OF THE CONFLICTING OBLIGATIONS

Complying with U.S. discovery demands can involve enormous effort and expense, even in the best of circumstances. But the discovery process can become even more difficult when compliance with U.S. discovery demands raises potentially conflicting legal obligations in non-U.S. jurisdictions. One way in which these conflicting demands might arise is when EU data protection laws prohibit the discovery of the requested information. On the one hand, U.S. courts can seek to compel litigants and third-party witnesses to produce documents and other information, and impose serious sanctions for failure to do so. On the other hand, data protection authorities in EU Member States[1] can view the production of those documents and other information, whether court ordered or not, as itself vio-

lating EU data protection rules, and can impose penalties for taking the steps necessary to comply with those U.S. discovery orders. Below we discuss these conflicting demands, and suggest a constructive way to reconcile them. A useful place to start this discussion is at the roots of the conflicting demands imposed by the different legal regimes.

A. Different Approaches to Data Protection

One of the roots of the conflict that can arise in U.S.-EU cross-border discovery is the substantially different notions of ''personal data'' adopted under U.S. and EU law, and the different protections accorded such data. The EU takes an omnibus approach—protecting all personal information, while the United States operates on a harms-based approach—protecting only that information that is particularly sensitive or which, if inappropriately used or disclosed, can cause substantial harm to individuals. It is critical to understand these differences in any dialogue on cross-border discovery.

The EU Member States[2] generally embrace a broad view of ''personal data.'' The 1995 Data Protection Directive[3] (''Directive''), as implemented by the Member States, protects individuals against the unauthorized processing of personal data, which is defined as any information relating to an identified or identifiable individual. This includes e-mails or documents created in the workplace such as work related e-mails, memoranda, and reports. The concept of ''processing'' is broadly defined as ''*any operation or set of operations,*'' whether manual or automated, including, but not limited to, ''*collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.*''[4]

In the European Union, regulators view any processing of personal data with suspicion. Processing personal data is prohibited unless there is a specific statutory authorization, or consent from the individuals concerned. Individuals must also receive detailed notice regarding the personal data that are processed. Personal data may only be collected for a specific, explicit purpose, and may not be further processed in a manner incompatible with that original purpose. Surprisingly to many U.S. lawyers and business people, all of these rules apply equally to documents or information created in the context of employment. These rules were not created to block U.S. discovery or to influence U.S. policy decisions. Instead, they represent EU-based policy choices, and are of equally restrictive effect in the European Union itself.

The United States, by contrast, takes a more narrow, sector-by-sector approach. Unless there is applicable legislation that prevents such actions, an organization remains free to collect, use, transfer, and retain personal data as it deems necessary. Unlike the rules in the European Union, processing of personal information in the United States is permitted unless explicitly prohibited. The concepts of ''personal data'' and ''processing'' are also quite different. In the United States, the term ''personal information'' is generally restricted to specific types of information that are considered particularly sensitive, such as personal medical information, Social Security numbers, information relating to children, and financial information. The focus is on protecting only certain types of personal information. Other information (such as information created in the context of employment including e-mails and other documents) is not generally covered by U.S. data protection rules. Thus, courts in the United States—unless educated by the lawyers in the case—may have a hard time weighing discovery demands against EU notions of personal data privacy if for no other reason than that EU notions of personal data privacy are truly foreign to them.

B. Different Approaches to Gathering Evidence

The other major root of the conflict stems from the varied approaches to litigation discovery in the United States and European Union. EU jurisdictions (especially civil law jurisdictions such as those in Continental Europe, but also to some extent common law jurisdictions like the United Kingdom) generally limit disclosure of evidence to what is offered by the parties as evidence in support of the case, and impose limited affirmative disclosure obligations. In these jurisdictions, the ability of one party to a litigation to require the other party to produce broad categories of documents and information is very limited; the ability to require a *non-party* to disclose such documents and information even more so. Because EU authorities often, as a practical matter, can view U.S. discovery obligations as unnecessary and unreasonable, they have a hard time weighing them against EU privacy laws.

The U.S. Federal Rules of Civil Procedure (''FRCP''), by contrast, impose on litigating parties (and nonparties when subpoenaed) broad and substantial obligations to retain, search for, and produce documents and information requested by the other party.[5] U.S. discovery gives parties the right to seek discovery relating

[1] The 27 Member States of the European Union are: Austria, Belgium, Bulgaria, Cyprus, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and the United Kingdom (collectively, the ''Member States'').

[2] The EEA member states Iceland, Liechtenstein, and Norway are bound to implement most EU legislation—including the 1995 Data Protection Directive—under Article 7 of the European Economic Area (EEA) Agreement.

[3] Directive 95/46/EC of October 24, 1995 on the protection of individuals with regard to processing of personal data and on free movement of such data [1995] OJ L 281/31. Article 2 of the Directive defines ''personal data'' as ''*any information relating to an identified or identifiable natural person (''data subject''); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*''.

[4] Article 2(b) of the Directive.

[5] State procedural laws, which apply to cases brought in the courts of an individual U.S. state rather than in a federal court, are similar. A comparable set of laws extends this obligation to preserve and produce evidence to U.S.-based administrative and regulatory proceedings. For example, the U.S. Securities and Exchange Commission (''SEC'') holds the authority to investigate U.S. companies for compliance with federal securities laws, and the agency may invoke its broad subpoena power to compel the prompt production of records in accordance with its investigation. Failure to preserve or produce in-

  PVLR ISSN 1538-3423

to: (1) any matter, not privileged, that is *relevant* to the claim or defense of any party; and (2) all information ''reasonably calculated to lead to the discovery of admissible evidence.''[6] U.S. courts apply these standards liberally, and generally resolve any doubt in favor of permitting discovery. As one federal district court put it, in language that is typical of the mindset of U.S. judges (especially judges at the trial-court level), this broad construction ''is consonant with American civil process which puts a premium on disclosure of facts to ascertain the truth as the means of resolving disputes.''[7] This is why major U.S. litigation can involve the production of millions of pages of documents. It is also why an entity might find itself subject to a discovery demand that an EU data protection authority is likely to view as irrelevant to the underlying litigation (and thus, from the EU perspective, excessive and unnecessarily in breach of EU data protection laws).

Two particular aspects of U.S. discovery rules increase the potential conflict between U.S. discovery demands and EU data protection laws. The first is that the physical location of a document is not dispositive or even particularly relevant. Rule 34 of the Federal Rules of Civil Procedure provides that discovery may be had of documents that are in the ''possession, custody or control'' of a party. The notion of '' '[c]ontrol' has been construed broadly by the courts as the legal right, authority, or practical ability to obtain the materials sought upon demand.''[8] So, if an entity subject to U.S. jurisdiction has possession, custody, or control of documents or information physically located in the EU, those documents are just as much subject to U.S. discovery obligations as documents actually physically located in the United States.

The second aspect giving rise to potential conflict relates to the role of foreign parents, subsidiaries, or affiliates of U.S. entities. The test in these circumstances focuses on the U.S. entity's control of the foreign affiliate's documents. Where the U.S. entity is the parent corporation, ''the determination of control turns upon whether the intracorporate relationship establishes some legal right, authority, or ability to obtain the requested documents on demand. Evidence considered by the courts include the degree of ownership and control exercised by the party over the subsidiary, a showing that the two entities operated as one, demonstrated access to documents in the ordinary course of business, and an agency relationship.''[9] Even where the U.S. entity is not the parent corporation, U.S. courts can require the production of documents and information from parent companies or affiliates located abroad. Again, the test focuses on the concept of ''control'' over those foreign-based documents and information. The factors used to evaluate control in these situations ''include (a) commonality of ownership, (b) exchange or intermingling of directors, officers or employees of the two corporations, (c) exchange of documents between the corporations in the ordinary course of business, (d) any benefit or involvement by the non-party corporation in the transaction, and (e) involvement of the non-party corporation in the litigation.''[10]

The U.S. entity that is subject to the discovery request cannot simply ignore the request for ''foreign'' documents. Sanctions for failing to comply with discovery in United States litigation are severe, and include monetary sanctions, evidentiary sanctions such as an adverse inference, or termination of the proceedings in favor of the requesting party. There has been an increase in ''adverse inference'' sanctions imposed by the courts recently, which means that the courts informed the jury of the fact that the company lost or failed to produce certain relevant documents, and directed jurors to assume that whatever documents were lost contained evidence harmful to the company.

II. RESPONSES TO BROAD DISCOVERY—THE BACKGROUND TO THE CURRENT DEBATE

EU data protection laws are not the first instances of non-U.S. jurisdictions adopting laws that can affect the U.S. discovery process. Many of the prior examples of these sorts of laws began in significant part as a way to deal with what was perceived in non-U.S. jurisdictions as overwhelming U.S. discovery processes or interventionist U.S. antitrust and other litigation.[11] As we argue below, however, EU data protection laws are different, in that they were adopted to achieve EU public policy objectives separate and apart from any concern over U.S. discovery or the extraterritorial application of substantive U.S. law. U.S. courts' perception of the initial motivation for these kinds of statutes, however, continues to color the legal standard that courts will apply to conflicts between U.S. discovery obligations and EU data protection laws.

---

formation may result in prosecution for criminal obstruction of justice.

[6] Fed. R. Civ. P. 26(b)(1)

[7] *Uniden Am. Corp. v. Ericsson Inc.*, 181 F.R.D. 302, 306 (M.D.N.C. 1998)

[8] *SEC v. Credit Bancorp*, 194 F.R.D. 469 (S.D.N.Y. 2000).

[9] *Camden Iron & Metal Inc. v. Marubeni Am. Corp.*, 138 F.R.D. 438, 442 (D.N.J. 1991); *see also In re Uranium Antitrust Litigation*, 480 F. Supp. 1138, 1152 (N.D. Ill. 1979) (corporate parent held responsible for producing documents of wholly owned subsidiaries); *Am. Rock Salt Co. v. Norfolk S. Corp.,* 228 F.R.D. 426, 458-59 (W.D.N.Y. 2005) (defendants had ''both legal and practical control'' over the documents because: (1) defendants had access to the subsidiary's records in the ordinary course of business; (2) the defendant had a 58 percent ownership interest, and 50 percent stock interest, in the subsidiary; and (3) the subsidiary's website stated that the corporate entity ''operates as an agent for its owners''); *Twentieth Century Fox Film Corp. v. Marvel Enters.*, 2002 U.S. Dist. LEXIS 14682, at *12 (S.D.N.Y. Aug. 8, 2002) (defendant had sufficient control over entity it ''owns and operates'' to compel production); *Dietrich v. Bauer,* 198 F.R.D. 397, 401 (S.D.N.Y. 2001) ''[i]t is not always clear whether the decisions arising in the parent-subsidiary context are premised on a strict 'legal right' standard or . . . on a somewhat more flexible 'pragmatic approach.' ''. *See generally*, C. Wright & A. Miller, 8 Federal Practice & Procedure 2d § 2210 (2006); *Strom v. Am. Honda Motor Co.*, 423 N.E.2d 1137, 1141-1145 (Mass. 1996) (reviewing the federal case law).

[10] *Uniden Am. Corp. v. Ericsson Inc.*, 181 F.R.D. at 306. In *Uniden*, the court concluded that the defendant had sufficient control over its sister corporation to compel overseas documents in the possession of the sister corporation.

[11] *See, e.g., Westinghouse Electric Corp. v. Rio Algom Ltd.,* 480 F. Supp. 1138 (N.D. Ill. 1979) (describing blocking statutes in Canada, Australia, and South Africa as having been enacted ''for the express purpose of frustrating the jurisdiction of the United States courts over the activities of the alleged international uranium cartel'').

A. The International Response: Blocking Statutes

One method that has been used to thwart the efforts of U.S. litigators and courts to obtain evidence under the FRCP is by enacting ''blocking statutes'' that penalize foreign citizens for complying with extraterritorial discovery requests.

For example, the French blocking statute, codified as Law No. 80538 of 16 July 1980, currently prohibits any French resident or national, as well as French legal entities and their employees, legal officers, or representatives, from disclosing, in any form, economic, commercial and technical documents and information to foreign legal entities and natural persons, except where the Hague Convention requires such disclosure.[12] This legislation also provides for potential criminal sanctions including imprisonment for compliance with discovery requests issued outside of the Hague Convention. A French witness in receipt of a discovery request issued pursuant to the FRCP (as opposed to the Convention) must inform French authorities and will usually contest its applicability on the ground that compliance will cause the witness to violate French law. The French witness will therefore ask the court to require the U.S. litigants to utilize the Convention. U.S. courts have been very reluctant to accept such requests. The trend has been to refuse to order application of the Convention and instead permit U.S. litigants to seek to obtain foreign evidence using the FRCP, notwithstanding the consequences under the blocking statute if the French witness complies with the discovery request. In justifying their position, some U.S. courts have stated that the French blocking statute is ''overly broad and vague and need not be given the same deference as a substantive rule of law.'' Other U.S. courts have ruled, more moderately, that the ''protection of United States Citizens from harmful foreign products and compensation for injuries caused by such products [i.e., aircrafts],'' was stronger than France's interest in protecting its citizens ''from intrusive foreign discovery procedures.'' The bottom line is that U.S. litigators have perceived that U.S. courts will order discovery without regard to the French blocking statute, and this has led many litigants to ignore these blocking statutes altogether.[13]

The conflicts created by the coexistence of broad U.S. discovery and the more restrictive procedures in most EU countries contributed to the ratification of the Hague Evidence Convention. The Convention is a multilateral agreement that currently stands between over 40 nations; it seeks to facilitate a uniform procedure for obtaining evidence located abroad. The Convention generally provides two general methods for obtaining evidence:

- The U.S. court issues letters of request, which are sent to the ''Central Authority'' of the jurisdiction where the discovery is located. The Central Authority is then responsible for transmitting the request to the appropriate judicial body in that jurisdiction for a response. A letter of request should typically be in the language of the Central Authority or accompanied by a translation. Execution of a letter of request is then subject to the local laws of the particular jurisdiction. Execution of a valid letter of request (*i.e.*, one that complies with the Convention) may only be refused in instances where the judiciary considers that its sovereignty or security would be prejudiced by execution of the letter.

- Alternatively, where the parties consent, the Convention provides for evidence gathering abroad by U.S. diplomatic officers or consular agents and appointed commissioners. These methods of gathering (oral) evidence are limited in three key respects: First, unlike letters of request, U.S. diplomatic officers, consular agents, and appointed commissioners cannot compel the production of evidence. Second, these methods cannot be used to obtain documents located abroad and can be used only to take deposition testimony. Third, contracting states have the prerogative to declare that U.S. diplomatic officers, consular agents, and appointed commissioners must first obtain permission from the foreign state prior to the deposition.

Many Convention signatory countries have rejected the prototypical ''no holds barred,'' ''no stone unturned'' form of pre-trial discovery common in U.S. litigation. In particular, Article 23 of the Convention provides that contracting states are permitted ''at the time of signature, ratification or accession'' to declare that they will not execute letters of request issued in order to obtain pre-trial discovery of documents. So far, over 30 of the contracting nations to the Convention, including China, Mexico, France, and the United Kingdom, have filed limited reservations under Article 23 prohibiting some degree of pre-trial document discovery. Some nations, such as Argentina, Australia, Denmark, Germany, Italy, Luxembourg, Monaco, Poland, Portugal, South Africa, Spain, and Sweden, have filed reservations under Article 23 that essentially prohibit all pre-trial document discovery.

---

[12] A translation of the French blocking statute reads as follows: *Article 1. Except when international treaties or agreements provide otherwise, no natural person of French nationality or habitually residing on French territory, nor any officer, representative, agent or employee of any legal entity having therein its principal office or establishment, may in writing, orally or in any other form, transmit, no matter where, to foreign public authorities documents or information of an economic, commercial, industrial, financial or technical nature, the communication of which would threaten the sovereignty, security, or essential economic interests of France or public order, as defined by government authorities to the extent deemed necessary.*

Article 1bis. Except when international treaties or agreements and laws and regulations in force provide otherwise, no person may request, seek to obtain or transmit, in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature, intended for the establishment of evidence in connection with pending or prospective foreign judicial or administrative proceedings.

[13] In fact, however, the statute cannot simply be ignored. In 2010 the French Supreme Court confirmed a Paris Court of Appeal Decision which ordered a French attorney to pay to a French witness €10,000 in damages for violation of Article 1bis of the blocking statute. The California Insurance Commissioner brought the suit against French insurance company MAAF regarding the takeover of U.S. insurance company Executive Life. The U.S. lawyer handling the case tried to obtain information from a former member of the MAAF board about how the board made decisions. The information was provided by a French attorney. The French court ruled, in rather broad terms, that the French attorney was liable under the blocking statute because the information sought and produced was of an economic nature and intended to establish evidence.

  PVLR ISSN 1538-3423

B. Balancing Tests Applied in the U.S. Courts

U.S. courts have frequently confronted the conflict between discovery obligations and blocking statutes. However, there is no single test that is consistently used in all U.S. courts. The issue appears to be addressed largely on a case-by-case, court-by-court basis; this is most striking from an EU perspective.

Discovery disputes do reach the appellate or U.S. Supreme Court level, but such appellate cases represent only the tip the iceberg: individual judges deal with many work-a-day discovery cases, and issue decisions at the trial level that tend to be more sympathetic to parties seeking to take the discovery. Even when cases get to the Supreme Court or appellate levels, it is up to the lower courts to apply the often ambiguous standards that are created. We find generally that these trial-level courts are more likely to impose a broader application of their own discovery authority, due to their focus on day-to-day case management issues, as opposed to the wider theoretical issues of comity and international relations.[14]

No single standard governs foreign discovery in U.S. courts. However, many U.S. federal courts of appeal recognize a five-factor balancing test of the exercise of their enforcement jurisdiction, derived largely from the Restatement (Third) of Foreign Relations law of the United States. Under that test, courts consider the following five factors:

- The importance of the requested documents or other information to the litigation;
- The degree of specificity of the request;
- Whether the information originated in the U.S.;
- The availability of alternative means of securing the information; and
- The extent to which noncompliance with the request would undermine important interests of the state where the information is located.[15]

Some courts (including those in the U.S. Court of Appeals for the Second Circuit) add two additional factors:[16]

- The good faith of the party resisting discovery; and
- The hardship of compliance on the party from whom discovery is sought.

U.S. courts applying these balancing tests have shown a propensity to prioritize discovery over foreign law. For example, in a case addressing potential violations of Malaysian law resulting from compliance with discovery demands, the court concluded:

> [T]he documents are vital to the litigation, the requests are direct and specific, the documents are not easily obtained through alternative means, the interest of the United States outweighs that of Malaysia under the circumstances, and the likelihood that [the New York branch] would face civil or criminal penalties is speculative. Although [it] has acted in good faith, and the documents are located abroad, this is insufficient to overcome those factors weighing in favor of disclosure.[17]

U.S. courts tend to be less deferential to foreign authority in assessing potential hardship to the complying party because U.S. courts come to the question assuming that international blocking statutes are motivated by an express desire to block U.S. discovery in order to protect non-U.S. companies or to defeat substantive U.S. laws (for example, U.S. antitrust laws).[18] Litigants and U.S. courts point to the indisputable trade protection or bank secrecy rationales that characterize many blocking statutes, and openly doubt the *bona fides* of such laws.

There are, of course, cases that find in favor of the party opposing discovery.[19] Most recently, in *SEC v. Stanford International Bank Ltd.*, a Swiss non-party bank located in the United States was served with a subpoena seeking banking records located in Switzerland, the production of which, it argued, would ''subject it and its employees to criminal, civil, and administrative penalties under Swiss law.[20] The non-party resisted the subpoena, arguing under *Aerospatiale* that the party seeking the discovery should first be required to proceed through the Hague Convention rather than requiring production by enforcing the U.S. subpoena. The district court agreed, after applying the seven-factor test described above. Although the court acknowledged that the requested documents were ''vital'' to the litigation, it found that three factors favored the non-party bank—the defense was not raised in bad faith, the documents were not located in the United States, and the non-party bank had a ''potentially well-founded fear'' that it could be prosecuted in Switzerland if it complied with the discovery request. Significantly, however, the district court declined to find that the U.S. interest in full discovery outweighed Switzerland's interest in its banking privacy laws, concluding that the very act of balancing was itself ''political,'' and ''especially inapposite in this case, where the legislative authorities of both nations essentially have spoken by adopting the Convention.''[21] Refusing to read *Aerospatiale* as giving litigation parties a ''green light to generally 'discard[] the treaty as an unnecessary hassle,' '' it found that the ''comity'' factor required the requesting party to go

---

[14] *Columbia Pictures Indus. v. Bunnell*, 2007 U.S. Dist. LEXIS 46364, at *49-50 (C.D. Cal. June 19, 2007) *(''[I]t is well-settled that foreign blocking statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce (let alone preserve) evidence even though the act of production may violate that statute.''*) (Citing *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1474 (9th Cir. 1992); *Rich v. KIS Cal., Inc.*, 121 F.R.D. 245, 257 (M.D.N.C. 1988) (''[i]n general, broad blocking statutes, including those which purport to impose criminal sanctions, which have such extraordinary extraterritorial effect, do not warrant much deference'').

[15] RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES 442(1) (C) (1987).

[16] *See First Am. Corp. v. Price Waterhouse LLP*, 154 F.3d 16, 22 (2d Cir. 1998); *Minpeco, S.A. v. ContiCommodity Servs. Inc.*, 116 F.R.D. 517, 523 (S.D.N.Y. 1987).

[17] *Gucci Am., Inc. v. Curveal Fashion*, No. 09 Civ. 8458, 2010 WL 808639 (S.D.N.Y. Mar. 8, 2010).

[18] Indeed, in *In re Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct.*, 482 U.S. 522 (1987), the U.S. Supreme Court specifically stated that the lower courts must give greater deference to the substantive law of foreign nations than to procedural rules such as the French ''blocking statute.''

[19] Civil Action No. 3:09-CV-0298-N, 2011 WL 1378470 (N.D-.Tex. Apr. 6, 2011).

[20] *Id.* at *2.

[21] *Id.* at *9.

through the Hague Convention ''*at least in the first instance*.''[22]

Cases like *Stanford* are rare, and are unlikely to stem the tide of more numerous cases that compel discovery even in the face of foreign prosecution. And, notably, the court in *Stanford* does not make at all clear what might happen if resort to the Hague Convention ''in the first instance'' does not lead to the necessary discovery from the Swiss Bank.

III. GUIDANCE FROM EU AUTHORITIES ON BALANCING EU DATA PROTECTION AND U.S. DISCOVERY OBLIGATIONS

The Article 29 Working Party (''Working Party''), the consortium of EU Member State data protection authorities, provides useful non-binding guidance on the challenges that arise from discovery obligations, in its 2009 Working Paper[23] on pre-trial discovery for cross-border civil litigation (''Paper''). Unfortunately, the Paper does not cover document production in U.S. criminal and regulatory investigations.

Although the Paper does not formally address document preservation in anticipation of proceedings before U.S. courts, or in response to requests known as ''freezing'' or ''data retention order'' it does stress that EU organizations have no permission to retain data *''at random for an unlimited period of time because of the possibility of litigation in the US.''* The mere or unsubstantiated possibility of an action being brought before U.S. courts is not sufficient. Rather, data may only be retained if relevant and to be used in specific or imminent proceedings, where ''reasonably anticipated.''

Under the Directive, personal data may only be processed where authorized by law. The Paper covers three legal bases that can be used to authorize the processing (*i.e.*, disclosure or transfer) of personal data in cross-border discovery:

- *Consent*: The Working Party considers that *''it is unlikely that in most cases consent would provide a good basis for processing''*. The use of consent is not reliable, nor particularly workable. To legitimize data processing using this basis, organizations must obtain the ''specific'' and ''informed'' consent of all individuals who might potentially be concerned by, or relevant to the discovery. Individuals may subsequently withdraw their consent at any time, and consent is only deemed valid in cases where there is a ''real opportunity'' to withhold or withdraw consent without suffering any penalty. In earlier guidance, the Working Party has taken the position that a current employee cannot freely provide consent because of the prejudice that might arise should he/she refuse consent. This suggests that the use of employee consent to legitimize data processing exists only in theory. While obtaining the freely given consent of third parties, such as customers or suppliers, may be more realistic than for employees, the right to withdraw consent substantially lowers the utility of consent as a legal basis for complying with U.S. discovery requirements, even in the case of non-employees.

- *Legal Necessity*: An organization may establish the legitimacy of data processing where *''necessary for compliance with a legal obligation.''* Regulators and courts interpret this quite narrowly to only cover situations where there is an EU statutory requirement: the Directive does not consider an extraterritorial legal dispute to be a legal obligation. The Working Party has also opined that *''an obligation imposed by a foreign legal statute or regulation . . . may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate.''*

- *Balance of Interest*: The balance of interest exception may cover discovery—or compliance with foreign requests. This is because organizations' interest in complying with U.S. statutory requirements (*i.e.*, U.S. discovery requests) is usually legitimate. The Paper stresses that the proportionality and relevance of the data, and possible consequences for the individuals concerned must be taken into account. Adequate safeguards must be adopted to protect the rights of the individual. The organization supplying the data should also ''anonymize'' or at least aggregate the data and, where possible, apply filtering techniques to exclude or cull irrelevant data. These tasks should be assigned to a ''trusted'' third party within the European Union.

In addition to a legitimate legal basis, an adequacy mechanism must be in place where records are transferred to the United States (or to another country outside the EEA). Generally, the only acceptable mechanism is if the recipient country meets the Directive's ''adequacy'' requirements for data transfers. Adequacy is determined by a global assessment of safeguards and suitability to protect personal data, based on the various provisions of the Directive. Under this standard, the United States has not been deemed to have an adequate data protection scheme. For legal transfer of data to the United States, three mechanisms exist, and are described below. However, while these mechanisms can be useful to facilitate document review, none of them legitimizes the onward transfer of data from the requesting organization to other parties, witnesses, or the arbitrators. This limits their utility in U.S. discovery proceedings.

- *Safe Harbor Provisions*: The Safe Harbor program established by the European Commission and the U.S. government allows U.S.-based organizations to self-certify that they will abide by the Safe Harbor principles of notice, choice, onward transfer, security, data integrity, access, and enforcement. Thus, Safe Harbor legitimizes transfers between an organization established in the EEA or Switzerland and a U.S. organization.

- *Model Clauses*: Concluding a transfer agreement including the EU model contractual language furnishes organizations located in the United States (or another country not considered ''adequate'') with the necessary safeguards to engage in data transfers. However, because model contracts must reflect the Directive's provisions, they do not address the aforementioned conflicts over data transfers for U.S.-based discovery efforts. Crucially, model clauses impose even stricter limitations for subsequent use in U.S. discovery proceedings. For example, it will not generally be permissible to share the information with other parties or U.S. courts. In addition, U.S. courts are very unlikely to execute transfer agreements in order to receive information.

[22] *Id.* at *3, 13 (emphasis added).

[23] Article 29 Working Party, *''Working Document 1/2009 on pre-trial discovery for cross-border civil litigation,''* WP 158, Adopted on 11 February, 2009. Available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf.

  PVLR ISSN 1538-3423

- *Binding Corporate Rules*: Multinational companies that wish to transfer data between international offices may look to binding corporate rules (''BCRs'') as mechanisms by which data may be transferred outside of EU countries. BCRs are internal data protection rules and practices applied at a corporate-wide level. Due to this limitation, BCRs would not allow transfers to litigators or U.S. courts.

The Directive also provides for several derogations, or exceptions, from these three mechanisms. These occur, in relevant part, when the individual unambiguously consents to the transfer, or when the transfer is necessary for the exercise or defense of a legal claim:

- *Consent*: Here, consent follows the same standard as consent as a basis for processing personal data. Because of its limitations, consent remains an unreliable basis for cross-border data transfers.
- *Necessity for Legal Claim*: Article 26(1) (d) of the Directive creates an exception for international transfers that are ''necessary or legally required on important public interest grounds, or for the establishment, exercise, or defense of legal claims.'' Derogating from earlier Member State interpretation, the Working Party's Paper appears to apply the legal claims exception to ''single'' international transfers of data in compliance with foreign discovery obligations unless a ''significant'' amount of data are involved. There is no further guidance on what a ''single'' transfer or a ''significant'' amount of data would mean. However, according to the Working Party, the exception is subject to ''strict interpretation.''[24] In addition, the Working Party has opined that the exception would not apply to a data transfer undertaken ''on the grounds of the possibility that such legal proceedings might one day be brought.''[25] The Working Party's examples may further imply that the exception is only relevant where the individual is a party to the litigation. This would severely limit the practical application of this concept. Moreover, Working Party's Papers and Opinions are nonbinding and each Member State can vary its interpretation (which has happened in several other areas, such as whistleblowing).

With the appropriate mechanisms in place, the Working Party's Paper seems to permit international transfers of data in compliance with foreign discovery obligations under the balance of interest test and the legal claims derogation. However, these exceptions are narrowly cast, and the examples cited in the Paper may imply that they are only relevant where the litigation has already commenced, and may not support anticipatory or ''preventive'' discovery or document hold requests. Here, further guidance from the Working Party on what is meant by *''the mere or unsubstantiated possibility that an action may be brought before U.S. courts,''* would be very helpful. In particular, the Working Party should clarify that while a remote possibility for litigation may not suffice, disclosure should be permitted when necessary for prospective proceeding.

Importantly, where data *are* legitimately transferred, the Paper affirms that there is no waiver of data protection rights. Individuals may exercise their access and correction rights during the proceedings, as afforded to individuals under the Directive. Advance general notice of the possibility of data transfer should be provided to all individuals, *e.g.*, through a detailed technology use policy or data protection notice to all employees. When the data are actually collected and transferred, additional, more concrete notices should be given *''as soon as reasonably practicable,''* and should include information on the identity of any recipients, the purposes of the processing, and the categories of data concerned, as well as details on individuals' rights. All data must be protected through appropriate security standards and policies in order to keep the data confidential and secure. Where service providers are used, they should be bound by contract to ascertain compliance with purpose limitation obligations, retention policies, and security standards. To many litigators in the United States, where court records are public, these concepts often appear foreign and counterintuitive.

IV. THE BALANCING TEST AND DATA PROTECTION

Litigants or other recipients of a subpoena must be aware that U.S. courts may ''overrule'' or disregard data protection laws or other mechanisms designed to limit cross-border discovery. Indeed, the weight of the case law suggests that a party seeking to resist U.S. discovery obligations on this basis face an uphill battle. But the results of these cases are driven largely by the nature of the foreign laws that were before the court—blocking statutes designed to thwart U.S. policy objectives. EU data protection laws are different from these protective blocking statutes. They are motivated not by some generalized antipathy to U.S. discovery approaches or to substantive U.S. law (like antitrust, or the pursuit of financial crimes that requires interfering with bank secrecy), but rather by an affirmative view of the substantive privacy rights of EU citizens. In other words, they are good faith attempts to forward affirmative EU policy goals, not merely schemes to block U.S. policy goals.

In light of this background, parties facing conflicting legal obligations in the United States and the European Union need to advocate for application of a balancing test that recognizes both: (i) their own good faith in seeking to balance the conflicting legal obligations and (ii) the good faith of the EU regulatory regimes in seeking to advance the public policy interests reflected in data protection laws that have equal application to both. Existing balancing tests can work, but only so long as the U.S. courts can be persuaded to look closely at the EU data protection laws rather than simply equating them with traditional blocking statutes.

A recent report suggests that at least some U.S. courts may engage in the sort of balancing and compromise approach that would give due weight to both U.S. discovery demands and EU data protection laws. In a recently published report, the Bavarian data protection authority (''DPA'') referred to a U.S. court decision from early 2011 that restricted a document production request to reconcile the competing demands of U.S. discovery and EU data protection.[26] In the case, the U.S.

[24] Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 adopted on 25 November 2005, page 13.

[25] Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October 1995 adopted on 25 November 2005, page 15.

[26] The Bavarian data protection authority's 102-page 2009-2010 Activity Report is available, in German, at http://www.regierung.mittelfranken.bayern.de/aufg_abt/abt1/

plaintiff issued a broad document production request to the Bavaria-based German defendant. The defendant asked the DPA for guidance on the production of such data.

In its response, the DPA held that the plaintiff had a legitimate interest and need to defend the claim: the production of certain documents was permitted. However, the DPA opposed the production of other documents that were not directly related to the disclosure request or did not clarify the claim. Further, the DPA specified that any additional data must be filtered out, and any personal data irrelevant for the case had to be redacted.

The German defendant thus responded to the discovery request by providing only the documents the DPA permitted it to provide, and challenged the overall scope of the discovery request. In early 2011, the United States ruled in favor of the German defendant, stating that the denial of access to the requested documents would not damage the plaintiff's claim, where consistent with the Bavarian DPA's response.

This case may be helpful in guiding organizations in resolving conflicting obligations. Although the outcome may be due to the specifics of the case (the defendant was a German company and not, as is often the case, a U.S. company with offices in Europe), by raising data protection concerns and cooperating with both EU authorities and U.S. courts, parties can come to an agreeable and compliant solution. Whether the case demonstrates the beginnings of a change in U.S. courts' approach—and a real willingness to account for EU data protection laws—remains to be seen.

V. RECOMMENDATIONS

We recognize that the above analysis is not going to completely reassure an entity facing conflicting discovery obligations and EU data protection obligations. What is perhaps even more troubling than the substance of the conflicting obligations is the dizzying array of often differing and uncertain legal standards that U.S. courts will use to judge a party's compliance with relevant law. These standards often seem to be applied to justify a particular result (and that result is usually to require disclosure), rather than to weigh the parties' conflicting legal obligations.

Organizations faced with potentially conflicting mandates from a U.S. court and from EU data protection laws should consider the following measures in order to navigate the risks:

- **Plan Ahead to Avoid Issues in the First Place.** A U.S. court is going to be far more persuaded by an entity's inability to produce discovery without violating foreign law if it can be persuaded that the entity did everything it could beforehand to mitigate its exposure. This might include the following:
  - ***Clear policies on record management:*** Data should only be retained if relevant and if there is a legal or business need to retain the information.
  - ***Technology use policy:*** All employees should be clearly informed about the possibility that data located on the organization's infrastructure may need to be retained and shared for discovery purposes.
  - ***Notice:*** Where appropriate, employees should be informed about the details of discovery requests, including possible recipients, third party service providers and the right to access and modify information. In some countries, works council or similar employee representatives or public authorities would also need to be informed. Data protection officers should be consulted on a regular basis, and have their views taken into consideration.
- **Raise Potential Data Protection Law Restrictions Early in the Discovery Process.** If you wait until the document production date to raise potential data protection law issues, you are likely to face a very hostile audience when you go to court to seek protection.
  - ***As soon as practicable, raise potential issues with your adversary:*** Alert the other side to the potential issues, and to the extent possible get them to take partial ownership of the issue. Express your willingness to cooperate with them to get the discovery, or to work around the discovery issue with them. Eventually, the judge is going to ask if you are acting in good faith, so act in good faith early and often. You want the court to conclude that you and your client have done your collective best to satisfy the discovery obligations.
  - ***Context is important:*** If you are a third party witness subpoenaed in U.S. litigation, you will have more scope to prioritize your EU discovery obligations. On the other hand, if you are a party to the litigation—and especially if you are a plaintiff—be prepared to find a way to respond to your adversary's discovery requests notwithstanding apparently conflicting EU data protection requirements.
  - ***Use Existing Balancing Tests, But Adapt Their Application to EU Data Protection Laws.*** Notwithstanding what appears to be a one-sided slate of results, there is nothing inherently wrong with the five- or seven-factor balancing tests currently being applied by U.S. courts. When applying those tests in this context, however, it is vital to emphasize to the court that the EU data protection laws in question protect ''important interests of the state where the information is located,'' and are nothing like the historical blocking statutes viewed with such suspicion by the U.S. courts.
- **Remember Your Data Protection Obligations During the Discovery Process.** If you do produce documents that are potentially subject to EU data privacy laws, protect the data.
  - ***Use protective orders carefully:*** Protective orders should be used to restrict information on a case-by-case basis for relevant data, rather than all data. Terms can be negotiated to restrict who may access the information sought and for what purposes. These terms could also impose sanctions for U.S. parties' non-compliance with the terms of the order as an additional safeguard against breach of EU data protection requirements. The parties can agree that sensitive data should be withheld where appropriate, ''anonymized,'' or redacted to preserve data protection interests. Personal data should be redacted if not directly related to the discovery request, or if irrelevant to the case.
  - ***Cooperate with EU data protection authorities:*** Official guidance from EU data protection authorities

baylda_daten/dsa_Taetigkeitsbericht_2010.pdf. The U.S. court and the parties were not identified due to a confidentiality agreement between the data protection authority and the defendant.

  PVLR ISSN 1538-3423

may have greater weight and may help convincing U.S. courts of the need to account for EU data protection obligations. Be careful—you do not want the U.S. court to conclude that you are ''conspiring'' with the EU data protection authority to defeat the discovery. Instead, you want all authorities and courts to conclude that you are looking to comply with all of your legal obligations in good faith, and that so long as you can do so you are essentially neutral on whether the discovery proceeds. In other words, you do not want anyone to conclude that you are (i) actively seeking to resist discovery, or (ii) actively seeking to violate your data protection obligations.

- o ***Apply appropriate security standards:*** Security standards should be applied to all relevant data, including contractual arrangements with service providers, to ensure uniform standards.

- **Try to work through issues creatively.** Try to determine if a mutually agreeable solution can be reached that complies with your obligations under both the U.S. discovery rules and the EU data protection regulations. Even if a complete solution cannot be reached, your willingness to work toward one will likely be viewed favorably by both the U.S. court and the relevant EU authorities.
  - o For example, as was discussed above, prior to disclosing any documents or information, it may be possible for the parties to negotiate terms that restrict who may access the data sought, as well as the purposes for which it may be used, in accordance with the security, transparency, and finality principles of the Directive.
  - o Also, upon review, any particularly sensitive aspect of the disclosure could be withheld, ''anonymized,'' or redacted to preserve the European party's privacy interest, but not with substantial prejudice to the U.S. party. A protective order could also provide for the redaction of information within a requested record that is not relevant or that is obtainable through other sources, in keeping with the Directive's objective of proportionality.
  - o Finally, a protective order could impose sanctions for the U.S. party's non-compliance with the terms of the order as an additional safeguard against abuse of the European party's disclosures, as well as a further display of cooperation.
- **Seek to educate U.S. judges on the importance of EU Data Protection Regimes.** Judges in the United States are unlikely to be familiar with EU data protection regimes and blocking statutes, and are likely to view them with some suspicion. From the U.S. perspective, this suspicion is somewhat natural given the historic lack of enforcement. As the entity at the sharp end of the stick when it comes to the need to strike the right balance here, it is up to the target of the conflicting legal obligations to make sure the U.S. judge becomes familiar with these rules, and how they can be balanced with U.S. litigation needs.

There is one additional consideration each for the U.S. lawyer and the EU lawyer to keep mind in each and every case:

- **For the U.S. lawyer:** Do not underestimate the importance of complying with EU data protection laws and blocking statutes, or the seriousness with which EU regulators and EU courts view these laws even in the face of what appears to be a contradictory mandate from across the ocean. Failure to comply with EU laws can do significant damage.

- **For the EU lawyer:** Do not underestimate the importance of complying with U.S. discovery obligations, or the seriousness with which U.S. courts view these obligations even in the face of what appears to be a contradictory mandate from across the ocean. Failure to comply with these laws can do significant damage.

In the long term, both the U.S. and EU's legislative frameworks on international data transfers must adapt to accommodate each other's legal needs. Without a stronger, clearer, and streamlined compliance mechanism, the issue of whether to compel international document production will continue to occupy U.S. courts.[27] Amendments to both the U.S. and EU legislative frameworks will be a vital part of future efforts toward the harmonization of international discovery policies, and U.S. district courts will need to bring their hardship analysis in line with current attitudes towards enforcement. Judges and regulators on both sides of the ocean need to give more deference to the laws of the other jurisdiction.

Karin Retzer is of counsel to Morrison & Foerster LLP, Brussels, where her practice focuses on electronic commerce and data protection, technology licensing, and intellectual property law. Michael Miller is a partner with Morrison & Foerster's New York City office. His practice includes all aspects of complex antitrust and commercial litigation in federal and state courts. Miller also frequently counsels clients on antitrust and privacy-related issues.

[27] The issue of document production in cross-border discovery is not the only instance in which EU data protection laws have come into conflict with U.S. laws. The U.S. Sarbanes-Oxley Act requires U.S. public companies to establish codes of conduct for employee behaviors with respect to finance, accounting, and corporate governance. These codes should be enforced through compliance hotlines (''whistle blowing'' hotlines) that allow employees to report violations anonymously. When the Act came into force and multinational companies established hotlines for foreign branch offices or subsidiaries, EU authorities held that the hotlines ran afoul of EU privacy laws. Through direct negotiations, the United States, European Union, and various individual Member States issued guidelines for the operation of these hotlines that successfully reconciled the conflicting legal requirements.