

U.S. LEGAL HOLDS ACROSS BORDERS: A LEGAL CONUNDRUM?

Kenneth N. Rashbaum, Matthew Knouff** &
Melinda C. Albert****

U.S. legal holds present a conundrum that confronts the bar and bench with increasing frequency. It is the result of a clash between broad U.S. preservation obligations mandated by existing case law and stringent privacy and data protection laws in other jurisdictions, including European Union (“E.U.”) member states. The challenge requires a multinational litigant to decide in which country she would prefer to have sanctions imposed and for what reason: failing to prevent the deletion of data when litigation is “reasonably anticipated,” or illegally preserving it under these same circumstances. Retention of “personal data,” which includes electronic mail, constitutes “processing” in the E.U. and elsewhere, and may only be performed for a purpose permitted by

* Kenneth N. Rashbaum is Principal of Rashbaum Associates, LLC in New York. His practice focuses upon counsel to multinational corporations on privacy, data protection and information governance across borders, litigation, and healthcare compliance. He is a frequent speaker and writer in the area of cross-border discovery and disclosure conflicts, and is an active member of The Sedona Conference, and a Vice-Chair of the International Litigation Committee of the American Bar Association. (www.Rashbaumassociates.com).

** Matthew Knouff is General Counsel of Complete Discovery Source, Inc., a global, full-service provider of electronic discovery and investigation technologies, management, and consulting services headquartered in New York City. Matthew advises global law firms and Fortune 500 companies on e-Discovery best practices and defensible deployment of technology for large-scale managed document reviews. He is an active member of Working Group 1 of The Sedona Conference, on the Board of Directors of the New York County Lawyers’ Association’s Cyberspace Law Committee and has developed numerous e-Discovery programs and CLE courses. (www.cdslegal.com).

*** Melinda C. Albert is Principal of the Law Office of Melinda C. Albert in Media, Pennsylvania. She focuses her practice on complex civil litigation, electronic discovery, and corporate compliance. She is an active member of Working Group 1 (Preservation and Production) of the Sedona Conference and Minority Corporate Counsel Association. (mcalbertesq@aol.com).

regional directives and local laws. However, U.S. litigation may not be a valid reason to preserve personal data under these provisions. In addition, many nations within and beyond the E.U. prohibit the retention of personal data after the reason for its initial collection has been accomplished. A U.S. legal hold may, therefore, violate these laws and expose the multinational litigant to significant civil penalties in jurisdictions where the data may be located.

This article analyzes and discusses these conflicts in the context of the acceleration of global commerce and resulting litigation. It highlights key issues in the dispute between U.S. discovery and non-U.S. legal systems that pose data preservation obstacles for litigants and courts and suggests means to reduce the risks of implementing legal holds beyond the United States.

I. INTRODUCTION

“[T]he courts have a right to expect that litigants and counsel will take the necessary steps to insure that relevant records are preserved when litigation is reasonably anticipated”¹

“There may however be a further difficulty [in the preservation of information] where the information is required for additional pending [U.S.] litigation or where future litigation is reasonably foreseeable [sic]. The mere or unsubstantiated possibility that an action may be brought before the U.S. courts is not sufficient.”²

The General Counsel of a multinational corporation arrives at corporate headquarters in Germany after a much-needed vacation only to be greeted by a subpoena on her desk. So ordered by a United States District Court judge, it demands production of email and other electronic data for a period of five years pursuant to a patent infringement lawsuit. She grimaces as she reads it a second time: the email in question was, she knows, created in Germany, France, Argentina, Japan, and Canada, is stored on servers in

¹ Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC, 685 F. Supp. 2d 456, 461 (S.D.N.Y. 2010).

² Working Document 1/2009 on Pre-Trial Discovery for Cross Border Civil Litigation, at 8 (Feb. 11, 2009) [hereinafter *E.U. Working Document*], available at http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf.

countries she cannot recall, and may also be in Cloud repositories and on portable devices. There may be a procedure for storing and preserving email, she recalls, but probably not for the Cloud, laptops, smartphones or USB drives. She realizes she must move quickly to make sure the data will not be deleted. But how, without violating the laws and regulations of one or more of the countries from which the emails emanated?

Reading the above excerpt from a case articulating the arguably prevailing national standard for preservation in U.S. litigation, the legal hold, and an opinion of a body of the European Commission stating that legal holds may violate law within the European Union, our protagonist may be legitimately confused. In which country, she thinks, would she prefer to have sanctions imposed, and for what reason: (1) failing to prevent the deletion of data when litigation is reasonably anticipated; or (2) preserving it under these same circumstances without legal justification in the host countries?

It is by now a central tenet of litigation in the United States that a party who is on notice that litigation is reasonably foreseeable must issue a “legal hold.”³ A legal hold is a process by which information is identified, preserved, and maintained when it has been determined that a duty to preserve has arisen.⁴ Notice of the

³ See The Sedona Conference, *The Sedona Conference Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 267 (2010), available at <http://www.thosedonaconference.org/> (“The concept of ‘legal holds’ or ‘litigation holds’ has gained momentum in the last 10 years as part of a common process by which organizations can begin to meet their preservation obligations.”). A “legal hold” is also known as a “litigation hold” in the United States, or, in Europe, a “litigation freeze.” *Id.*

⁴ See *id.*; *Pension Comm.*, 685 F. Supp. 2d at 464–65; *cf.* *Steuben Foods, Inc. v. Country Gourmet Foods, LLC*, No. 08-CV-561S(F), 2011 WL 1549450, at *5 (W.D.N.Y. Apr. 21, 2011) (“[T]he requirement of a written litigation hold notice, as stated in the *Pension Committee* case, as a ground to presume or infer loss of relevant documents, has not been adopted in this district.”); *Orbit One Commc’ns v. Numerex Corp.*, 271 F.R.D. 429, 441 (S.D.N.Y. 2010) (“[D]epending upon the circumstances of an individual case, the failure to abide by such standards does not necessarily constitute negligence, and certainly does not warrant sanctions if no relevant information is lost. For instance, in a small enterprise, issuing a written litigation hold may not only be unnecessary, but it could be counterproductive, since such a hold would likely be more general and

hold is issued to those who may have relevant information, in any format, and to personnel in charge of managing an entity's information management and governance systems. The notice clearly instructs "key players" to suspend the automatic or intentional deletion of relevant information.⁵ An effective legal hold process also includes tracking receipt of any notices as well as monitoring compliance with their instructions.⁶ Failing to adequately preserve such information may give rise to court-imposed sanctions, such as cost-shifting to the delinquent party or the issuance of an adverse inference instruction to the jury.⁷ The

less tailored to individual records custodians than oral directives could be." Note that despite case law holding that the absence of a written legal hold should not automatically give rise to sanctions, issuing a written legal hold should be viewed as a best practice in the overwhelming majority of cases, and parties relying on oral holds should proceed with extreme caution and maintain detailed recording of preservation activity.

⁵ See *Zubulake v. UBS Warburg LLC (Zubulake IV)*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

⁶ *Pension Comm.*, 685 F. Supp. 2d at 473.

⁷ See *Quinby v. WestLB AG*, 245 F.R.D. 94 (S.D.N.Y. 2006). After a thorough analysis of the seven-factor test set forth in *Zubulake v. UBS Warburg LLC (Zubulake I)*, 217 F.R.D. 309, 317–18 (S.D.N.Y. 2003), the court shifted a portion of the costs of production to the Plaintiff where the Defendant could not have reasonably anticipated that a particular custodian's emails would have to be produced. *Id.* The *Zubulake I* court noted that:

[C]ost-shifting may effectively end discovery, especially when private parties are engaged in litigation with large corporations. As large companies increasingly move to entirely paper-free environments, the frequent use of cost-shifting will have the effect of crippling discovery in discrimination and retaliation cases. This will both undermine the 'strong public policy favor[ing] resolving disputes on their merits,' and may ultimately deter the filing of potentially meritorious claims.

Thus, cost-shifting should be considered *only* when electronic discovery imposes an 'undue burden or expense' on the responding party. The burden or expense of discovery is, in turn, 'undue' when it 'outweighs its likely benefit, taking into account the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the litigation, and the importance of the proposed discovery in resolving the issues.

Id. However, courts may impose cost-shifting as a sanction for a party's failure to adequately preserve information. *Id.*

adverse inference instruction advises the jury that the producing party had a legal duty to produce the missing items, and that it may presume that the missing information would, if produced, be adverse to the position of the party who should have produced it.⁸ An adverse inference is virtually an insurmountable obstacle for the spoliator. In the trial that originally articulated the legal hold standard, *Zubulake v. UBS Warburg, LLC (Zubulake V)*,⁹ Judge Scheindlin issued an adverse inference sanction against the defendant for discovery violations, which contributed to a jury award of \$29.3 million in damages.¹⁰

The U.S. legal hold requirement is strictly a product of case law; it does not appear in any federal or state statute, nor is it in the Federal Rules of Civil Procedure. There is no national electronic discovery or data retention statute that requires preservation, though industry-specific regulations often require maintenance of certain records for specified periods of time, unrelated to litigation.¹¹ The fact that there is no “discovery” in civil law jurisdictions and no statutory mandate to preserve data for U.S.

⁸ See *Zubulake IV*, 220 F.R.D. at 219–22.

⁹ 229 F.R.D. 422 (S.D.N.Y. 2004).

¹⁰ *Id.* at 422; see also *Zubulake IV*, 220 F.R.D. at 219–20 (“In practice, an adverse inference instruction often ends litigation—it is too difficult a hurdle for the spoliator to overcome. The *in terrorem* effect of an adverse inference is obvious. When a jury is instructed that it may ‘infer that the party who destroyed potentially relevant evidence did so out of a realization that the [evidence was] unfavorable,’ the party suffering this instruction will be hard-pressed to prevail on the merits.”) (quoting *Linnen v. A.H. Robins Co.*, No. 97-2307, 1999 WL 462015, at *11 (Mass. Super. June 16, 1999)).

¹¹ See 29 C.F.R. § 1602.14 (1991) (“Preservation of Records Made or Kept”); see also Sarbanes-Oxley Act § 802, 18 U.S.C. § 1519 (2006) (“Whoever knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of any matter within the jurisdiction of any department or agency of the United States or any case filed under title 11, or in relation to or contemplation of any such matter or case, shall be fined under this title, imprisoned not more than twenty years, or both.”); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936 (1996); 18 C.F.R. § 125.2(l) (2000) (“[I]f a public utility or licensee is involved in pending litigation, complaint procedures, proceedings remanded by the court, or governmental proceedings, it must retain all relevant records.”).

discovery only compounds the often inscrutable nature of the preservation obligations which non-U.S. nationals must confront.¹²

There are five factors which complicate implementing a legal hold outside the United States. The first problem is that the concept of a legal hold itself is somewhat alien to practitioners and judges beyond the U.S.; there is no need to “hold,” or preserve data for discovery in civil law jurisdictions because there is no U.S.-style pretrial discovery in civil law systems.¹³

The second factor is rooted in the concept that privacy within the E.U. and most other countries is a fundamental right, rather than a legislated benefit, and is bolstered through the careful protection of personal data.¹⁴ Electronic mail, the most sought-after form of electronic evidence in the U.S. discovery process, is considered “personal data” within the E.U.¹⁵ “Personal data” may be “processed” only for purposes permitted by the Privacy

¹² See *E.U. Working Document*, *supra* note 2, at 4 (“By way of contrast with the transparency required discovery process in the U.S. and other common law countries, most civil code jurisdictions have a more restrictive approach and often have no formal discovery process. Many such jurisdictions limit disclosure of evidence to what is needed for the scope of the trial and prohibit disclosure beyond this. It is for the party to the litigation to offer evidence in support if its case.”).

¹³ THE SEDONA CONFERENCE WORKING GRP. ON INT’L ELEC. INFO. MGMT., DISCOVERY AND DISCLOSURE, THE SEDONA CONFERENCE FRAMEWORK FOR ANALYSIS OF CROSS-BORDER DISCOVERY CONFLICTS: A PRACTICAL GUIDE TO NAVIGATING THE COMPETING CURRENTS OF INTERNATIONAL DATA PRIVACY AND E-DISCOVERY 14–16 (M. James Daley et al. eds., Public Comment Version 2008) [hereinafter SEDONA FRAMEWORK], available at http://www.thesedonaconference.org/dltForm?did=WG6_Cross_Border.

¹⁴ See generally Directive 95/46, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [hereinafter Directive 95/46], 1995 O.J. (L 281) (EC), available at <http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML>.

¹⁵ See *id.* at art. 2(a) (“‘Personal data’ shall mean 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.”).

Directives and enabling legislation of the Member States.¹⁶ The European Commission Article 29 Data Protection Working Party (“the Working Party”) has opined that, under Directive 95/46 (“the Directive”), even the preservation of data is a form of “processing.”¹⁷ Preservation of data for “purposes of future litigation [i.e. a party issuing a legal hold where litigation is anticipated] may only [be] justified [if it is performed for a purpose specified] under Article 7(c) or 7(f) of Directive 95/46.”¹⁸ The challenge facing multinational counsel is that U.S. litigation may not be considered a purpose for which processing of personal data is permitted.¹⁹

To make matters even more puzzling, a third complicating factor is that many countries proscribe the retention of personal data past the period necessary to accomplish the function for which it was originally collected. Thus, a legal hold that requires information to be retained for an amorphous amount of time may be inconsistent with these laws.²⁰

The fourth problem in implementing a legal hold is that corporate culture in many jurisdictions places the onus on employees to decide what to preserve without any input from senior management or corporate counsel. This cultural/legal conflict enhances the risk of sanctions in the U.S. for loss of relevant information.²¹ The employees may not have sufficient

¹⁶ *Id.* at art. 7(a), 7(c), 7(f).

¹⁷ See *E.U. Working Document*, *supra* note 2, at 8; see also Directive 95/46, *supra* note 14, at art. 2(b) (“‘Processing’ shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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.”).

¹⁸ *E.U. Working Document*, *supra* note 2, at 8.

¹⁹ *Id.* at 9.

²⁰ *Id.*

²¹ See *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 685 F. Supp. 2d 456, 473 (S.D.N.Y. 2010) (holding that Counsel did not meet the standard for a litigation hold, in part, by instructing plaintiffs to be over, rather than under, inclusive in collecting and preserving documents since that directive placed “total reliance on the employee to search and select what

knowledge to predict what information may be “relevant” to future litigation.

The fifth and final problem is that U.S. discovery demands, which can spawn holds that require the preservation of “any and all” data within certain time periods, may run afoul of civil law frameworks. In the civil law setting, where the court decides specifically what documents and potentially relevant data will be exchanged, the documents and data must be delineated with great specificity, narrowly tailored to the issues in the case.²²

The goal of this article is to highlight the uncertainty that exists for litigants subject to suit in a foreign jurisdiction, and U.S. litigants whose evidence comprises foreign electronic evidence, with regard to the preservation of electronic data, and to contribute to a dialogue that will ultimately generate solutions that respect the litigation processes of both civil and common law jurisdictions. In the preceding Part we have defined the challenges presented by the differing international legal frameworks. Part II will describe the underpinnings of the preservation obligation in U.S. litigation. We will also illustrate both the broad parameters of the duty as well as how it is commonly fulfilled. In Part III we present the civil law framework and how the focus on data protection and individual privacy outside of the U.S. serves to prevent the seamless transfer of data into the U.S. for litigation. We will conclude with a discussion of key issues that will help practitioners both in and outside the U.S. make better informed decisions as to how to comply with the laws of each jurisdiction where their clients do business, as well as posit some potential means to reconcile data preservation in the U.S. with data protection and privacy in the E.U. and other nations.

that employee believed to be responsive records without any supervision from Counsel”); *see also* Phillip M. Adams & Ass’n v. Dell, Inc., 621 F. Supp. 2d 1173, 1194 (D. Utah 2009) (holding that defendant had violated its duty to preserve information, in part because the defendant’s preservation practices “place operations-level employees in the position of deciding what information is relevant”).

²² SEDONA FRAMEWORK, *supra* note 13, at 16.

II. THE OBLIGATION TO PRESERVE IN THE U.S. AND THE LEGAL HOLD

A. *The Broad Scope of U.S. Discovery*

The U.S. Federal Rules of Civil Procedure (“FRCP”) are based on the notion that broad access to potentially relevant material is the most effective way to resolve disputes on their merits.²³ To this end, the scope of pre-trial civil discovery in the United States extends far beyond relevance to include anything that “appears reasonably calculated to lead to the discovery of admissible evidence.”²⁴ In order to effectuate such a broad mandate, the parties are left to make their own determinations about what information must be produced in order to satisfy their discovery obligations. While this party-driven process is subject to protracted disputes among counsel, the potential for abuse is evident, and, therefore, standards are necessary to ensure compliance with the basic tenets of discovery.

B. *The Many Challenges Posed by Electronic Information*

The transient nature of email and other electronic information further compounds counsels’ burden of ensuring proper identification, preservation, and collection of everything they are obliged to produce. Courts, therefore, must ensure the availability and reliability of potentially relevant information for the discovery process to have its intended effect. Accountability in discovery hinges on sufficient preservation efforts. Electronically Stored Information (“ESI”) must be properly preserved lest it become lost, corrupt, altered, or rendered useless causing spoliation.²⁵ When

²³ The Sedona Conference, *The Case for Cooperation*, 10 SEDONA CONF. J. 339, 356 (2009), available at <http://www.thosedonaconference.org/> (noting that the Federal Rules of Civil Procedure, adopted in 1938, were designed to broaden pre-trial discovery to “promote the resolution of disputes . . . based on facts underlying the claims and defenses with a minimum of court intervention.”).

²⁴ FED. R. CIV. P. 26(b).

²⁵ THE SEDONA CONFERENCE WORKING GRP. ON ELEC. DOCUMENT RETENTION & PRODUCTION, THE SEDONA CONFERENCE GLOSSARY: E-DISCOVERY & DIGITAL INFORMATION MANAGEMENT 20 (Sherry B. Harris et al. eds., 3d ed. 2010), available at <http://www.thosedonaconference.org/dltForm?did=glossary2010.pdf> (“ESI, as referenced in the United States Federal

spoliation occurs, “the integrity of the judicial process is harmed.”²⁶

C. *A Lack of Uniformity Regarding How to Satisfy the Duty to Preserve*

A litigant’s duty to preserve potentially relevant information, and the appropriate sanctions applicable when that duty is not met, are sources of jurisprudential controversy in the U.S.²⁷ The duty to preserve requires a party to identify, locate, and maintain information and tangible evidence that is relevant to a specific and identifiable litigation.²⁸ This duty arises not only during litigation, but also extends to that period before the litigation “when a party reasonably should have known that the evidence may be relevant to future litigation.”²⁹ The triggering event could “arise from statutes, regulations, ethical rules, court orders, or the common law . . . a contract, or another special circumstance.”³⁰ The lack of any bright-line rules regarding triggering events creates the first layer of uncertainty for parties facing a discovery obligation in the U.S. Severe spoliation sanctions can arise not only from the destruction or material alteration of evidence, but also from “the failure to

Rules of Civil Procedure, is information that is stored electronically, regardless of the media or whether it is in the original format in which it was created, as opposed to stored in hard copy (i.e., on paper).”).

²⁶ *Pension Comm.*, 685 F. Supp. 2d at 462.

²⁷ See discussion *infra* pp. 11–15.

²⁸ The Sedona Conference, *supra* note 3, at 267.

²⁹ *Kronisch v. United States*, 150 F.3d 112, 126 (2d Cir. 1998); see also The Sedona Conference, *supra* note 3, at 269–87 (setting forth a series of factors for determining when a duty to preserve may arise and providing examples of triggering events).

³⁰ *Victor Stanley, Inc. v. Creative Pipe (Victor Stanley II)*, 269 F.R.D. 497, 521 (D. Md. 2010) (quoting The Honorable Paul W. Grimm et al., *Proportionality in the Post Hoc Analysis of Pre-Litigation Preservation Decisions*, 37 U. BALT. L. REV. 381, 390 (2008)); see also FED. R. CIV. P. 37(f) (stating in the Advisory Committee Note that “a preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case”).

preserve property for another's use as evidence in pending or reasonably foreseeable litigation."³¹

Our General Counsel may be able to clearly identify that a duty to preserve has been triggered, but she then faces two additional challenges: (1) identifying those whose data and documents must be preserved; and (2) determining how that information will be retained. A landmark set of opinions handed down in 2003–2004 by U.S. District Judge Shira Scheindlin, collectively referred to as “*Zubulake*,” served as the initial beacon of light for practitioners adrift in the uncertain waters of preservation.³² In *Zubulake IV*, Judge Scheindlin stated that “[t]he broad contours of the duty to preserve are relatively clear.”³³ The general scope of disclosure under FRCP 26(b)(1) is that “[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party’s claim or defense.”³⁴ In an effort to describe the broad scope of FRCP 26 as it relates to the preservation obligation, the court explained that a “party or anticipated party must retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches, and any relevant documents

³¹ *Silvestri v. Gen. Motors Corp.*, 271 F.3d 583, 590 (4th Cir. 2001) (citing *West v. Goodyear Tire & Rubber Co.*, 167 F.3d 776, 779 (2d Cir. 1999)).

³² The five opinions are *Zubulake I*, 217 F.R.D. 309 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC (Zubulake II)*, 230 F.R.D. 290 (S.D.N.Y. 2003); *Zubulake v. UBS Warburg LLC (Zubulake III)*, 216 F.R.D. 280 (S.D.N.Y. 2003); *Zubulake IV*, 220 F.R.D. 212 (S.D.N.Y. 2003); and *Zubulake V*, 229 F.R.D. 422 (S.D.N.Y. 2004).

³³ *Zubulake IV*, 220 F.R.D. at 217–18 (“That duty should certainly extend to any documents or tangible things made by individuals likely to have discoverable information that the disclosing party may use to support its claims or defenses.”). Judge Scheindlin went on to state that the duty also includes documents prepared for those individuals, to the extent those documents can be readily identified and to information that is relevant to the claims or defenses of any party, or which is “relevant to the subject matter involved in the action.” *Id.* (quoting FED. R. CIV. P. 34(a), 26(a)(1)(A)).

³⁴ FED. R. CIV. P. 26(b)(1) (stating, under the Rules as amended in 2006, FRCP 26(b)(1) is subject to the limitation under FRCP 26(b)(2)(B) that “[a] party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost.”).

created thereafter.”³⁵ At first glance, Judge Scheindlin’s comment that a party retains “*all relevant documents*”³⁶ seems to create an overwhelming burden for all parties to litigation in the U.S., especially in light of the wide net cast by FRCP 26. However, it has been widely noted that a standard of perfection is simply unattainable,³⁷ and that it would be unreasonable for a company to try and “preserve every shred of paper, every e-mail or electronic document, and every backup tape.”³⁸ Instead, the more prevalent opinion is that the scope of a party’s preservation efforts is narrowed by the concepts of reasonableness and proportionality.³⁹

³⁵ *Zubulake IV*, 220 F.R.D. at 218.

³⁶ *Id.*

³⁷ *Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of Am. Sec., LLC*, 685 F. Supp. 2d 456, 462 (S.D.N.Y. 2010).

³⁸ *Zubulake IV*, 220 F.R.D. at 217.

³⁹ *Victor Stanley II*, 269 F.R.D. 497, 523 (D. Md. 2010); *see also Pension Comm.*, 685 F. Supp. 2d at 463–64; THE SEDONA CONFERENCE WORKING GRP. ON ELEC. DOCUMENT RETENTION & PROD., THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION (Jonathan M. Redgrave et al. eds., 2d ed. 2007), available at http://www.thosedonaconference.org/dltForm?did=TSC_PRINCP_2nd_ed_607.pdf (“The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information.”); The Sedona Conference, *supra* note 3, at 269 (setting eleven Guidelines, which are “intended to facilitate compliance by providing a framework an organization can use to create its own preservation procedures”); *cf. Steuben Foods, Inc. v. Country Gourmet Foods, LLC*, No. 08-CV-561S(F), 2011 WL 1549450, at *4 (W.D.N.Y. Apr. 21, 2011) (“[T]he requirement of a written litigation hold notice, as stated in the Pension Committee case, as a ground to presume or infer loss of relevant documents, has not been adopted in this district.”); *Orbit One Communs. v. Numerex Corp.*, 271 F.R.D. 429, 441 (S.D.N.Y. 2010) (“[D]epending upon the circumstances of an individual case, the failure to abide by such standards does not necessarily constitute negligence, and certainly does not warrant sanctions if no relevant information is lost. For instance, in a small enterprise, issuing a written litigation hold may not only be unnecessary, but it could be counterproductive, since such a hold would likely be more general and less tailored to individual records custodians than oral directives could be.”). Note that despite case law holding that the absence of a written legal hold should not automatically give rise to sanctions, issuing a written legal hold should be viewed as a best practice in the overwhelming majority of cases, and parties relying on oral holds should

However, as discussed *infra*, these two concepts are key areas of consternation for the non-U.S. litigant walking the tight rope between broad preservation and personal privacy.

Even after a duty has been triggered, and the key custodians and their documents have been identified, a question still looms: how do you actually preserve? While all circuit courts in the U.S. recognize the “duty to preserve information relevant to anticipated or existing litigation,”⁴⁰ the means of defensibly satisfying that duty remains a subject of fierce debate. Many jurists have provided insight into the practical mechanics of complying with the U.S. duty to preserve, but there are no clearly defined national standards. Despite this lack of guidance, the most widely endorsed mechanism for satisfying the duty to preserve is the legal hold.

A legal hold is the formalized suspension of a party’s retention and destruction policies pertaining to documents that are potentially relevant to a lawsuit that has either been filed or is reasonably anticipated.⁴¹ It is designed to ensure that key parties are notified of document preservation requirements while preventing spoliation of relevant data. However, as often happens in cross-border information disclosure law, answers in one jurisdiction simply create more questions in another.

Six years after *Zubulake IV*, Judge Scheindlin brought preservation issues to the forefront of U.S. jurisprudence yet again with her decision in *Pension Committee*.⁴² In this controversial opinion, Judge Scheindlin identified several specific preservation omissions that support a per se finding of gross negligence, including: (i) failure to issue a written legal-hold; (ii) failure to identify all key players; (iii) failure to preserve a prior employee’s

proceed with extreme caution and maintain detailed recording of preservation activity.

⁴⁰ The Honorable Paul W. Grimm et al., *Proportionality in the Post Hoc Analysis of Pre-Litigation Preservation Decisions*, 37 U. BALT. L. REV. 381, 412 n.38 (2008); see also *Pension Comm.*, 685 F. Supp. 2d at 462 (“By now it should be abundantly clear that the duty to preserve means what it says and that a failure to preserve records—paper or electronic—and to search in the right places for those records, will inevitably result in the spoliation of evidence.”).

⁴¹ See *Victor Stanley II*, 269 F.R.D. at 521–22.

⁴² *Pension Comm.*, 685 F. Supp. 2d at 462.

documents in the party's possession, custody, or control; and (iv) failure to preserve backup tapes when they are the sole source of relevant information.⁴³ A court strictly applying the holding set forth in *Pension Committee* would find sanctions due to specific conduct or omissions absent any additional inquiry, such as relevance of the information, or prejudice to the requesting party by loss of the data.⁴⁴

The reaction to *Pension Committee* from various jurisdictions in the U.S., including Judge Scheindlin's own district (e.g. *Orbit One* discussed below), underscores the difficulties associated with issuing any bright-line preservation rules. One such opinion from the Southern District of Texas is *Rimkus Consulting Group Inc. v. Nickie G. Cammarata*.⁴⁵ In *Rimkus*, Judge Rosenthal⁴⁶ held that "it can be difficult to draw bright-line distinctions between acceptable and unacceptable conduct in preserving information and in conducting discovery, either prospectively or with the benefit (and distortion) of hindsight."⁴⁷ Judge Rosenthal noted that judging conduct turns on what is reasonable under the circumstances and must be weighed in proportion to the case at hand.⁴⁸ She rejected Judge Scheindlin's categorical approach to sanctions, opting for a

⁴³ *Id.* at 465.

⁴⁴ See *Victor Stanley II*, 269 F.R.D. at 536 n.37 (stating that with regards to ruling that failure to issue a written legal hold is per se gross negligence, a "[court] is inexorably poised to give an adverse jury instruction without further analysis.").

⁴⁵ 688 F. Supp. 2d. 598 (S.D. Tex. 2010).

⁴⁶ *Judge Rosenthal Issues Sanctions for Failure to Preserve E-Mail*, LEGAL HOLDS AND TRIGGER EVENTS (Feb. 24, 2010), <http://legalholds.typepad.com/legalholds/2010/02/judge-rosenthal-issues-sanctions-for-failure-to-preserve-email-in-rimkus.html> ("Judge Rosenthal was at the helm of the Federal Rules Advisory Committee when the e-discovery amendments were developed and enacted in 2006."). The article proceeds to explain that in the Advisory Committee Notes it was expressly stated that bright line rules on preservation were avoided. *Id.*

⁴⁷ *Rimkus*, 688 F. Supp. 2d at 613. Judge Rosenthal rejected the notion that the absence of defined factors, such as a written hold, constituted a breach of the preservation obligation, instead holding that the concepts of "reasonableness" and "proportionality" should guide preservation efforts. *Id.*

⁴⁸ *Id.*

more ad hoc assessment.⁴⁹ The severity of sanctions applied must be based on an evaluation of the level of culpability as well as an assessment of the prejudice to the affected party, which includes a determination of relevance.⁵⁰

The importance of relevance in determining whether to impose sanctions was echoed by Magistrate Judge James Francis in *Orbit One Communications, Inc. v. Numerex Corp.*⁵¹ In *Orbit One*, Magistrate Judge Francis, sitting in the Southern District of New York with chambers a short distance from those of Judge Scheindlin, expressly rejected both bright-line standards set forth in *Pension Committee* as well as the less rigorous *Rimkus* test.⁵²

Despite the divergent opinions amongst various U.S. jurisdictions regarding the levels of culpability and relevance with regards to the imposition of sanctions, one point is quite clear: a failure to preserve potentially relevant information risks the

⁴⁹ *Id.* Judge Rosenthal “rejected a categorical approach to sanctions,” but it is not clear that that “categorical approach” is attributable to Judge Scheindlin; rather, the cited text only indicates that Judge Scheindlin contends that the proportionality/reasonableness analysis “depends heavily on the facts.” *Id.*

⁵⁰ *Id.*

⁵¹ 271 F.R.D. 429 (S.D.N.Y. 2010).

⁵² *Id.* at 436–41. The Court, in discussing sanctions for failing to preserve evidence, stated:

The implication of *Pension Committee*, then, appears to be that at least some sanctions are warranted as long as any information was lost through the failure to follow proper preservation practices, even if there have been no showing that the information had discovery relevance, let alone that it was likely to have been helpful to the innocent party. If this is a fair reading of *Pension Committee*, then I respectfully disagree.

Id. at 440. The Court went on to reference *Victor Stanley II* and *Rimkus* stating:

Although some cases have suggested that the definition of what must be preserved should be guided by principles of ‘reasonableness and proportionality,’ this standard may prove too amorphous to provide much comfort to a party deciding what files it may delete or backup tapes it may recycle. Until a more precise definition is created by rule, a party is well-advised to ‘retain all relevant documents (but not multiple identical copies) in existence at the time the duty to preserve attaches.’

Id. at 436 (quoting *Victor Stanley II*, 269 F.R.D. 497, 523 (D. Md. 2010); *Zubulake IV*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003)).

imposition of sanctions so severe that they can imperil the outcome of a case.⁵³ Before a multinational litigant faces the task of crafting a process for preserving data that may be relevant to U.S. litigation, a more general question presents itself: does the attempt to satisfy the U.S. common law duty to preserve by implementing a legal hold *itself* cause a violation of privacy laws outside the U.S. to which compliance is equally expected?

III. GEOGRAPHY AND CULTURE BREED DIFFERENCES IN PERSPECTIVE: THE VIEW OF PRESERVATION OUTSIDE THE U.S.

The international practitioners' dilemma is exacerbated in civil law countries by the lack of experience with "discovery." The analysis, and the potential pathway out of this conundrum, should therefore begin with an appreciation of some fundamental differences between the U.S. and the rest of the world when it comes to the concept of "discovery." Also to be noted are the key distinctions between the discovery process of common-law systems⁵⁴ versus civil law systems.⁵⁵

The scope of pre-trial discovery in the U.S. is as wide as it is deep, even permitting discovery of evidence that is not necessarily admissible and may never see the light of a courtroom.⁵⁶ No other country permits such expansive pre-trial demands for the production of information. Apart from the U.S., the common-law jurisdictions do permit some form of discovery, but it is quite circumscribed.⁵⁷

⁵³ See, e.g., *Zubulake V*, 229 F.R.D. 422 (S.D.N.Y. 2004).

⁵⁴ Countries with common-law systems include the U.S., U.K., Canada except Quebec, New Zealand, Australia and, as historical vestiges, Hong Kong and Singapore.

⁵⁵ See SEDONA FRAMEWORK, *supra* note 13, at 14–16.

⁵⁶ FED. R. CIV. P. 26(b)(1).

⁵⁷ Ontario, Canada: R.R.O. 1990, REGULATION 194, RULES OF CIVIL PROCEDURE, Rule 29.1; see also THE SEDONA CONFERENCE WORKING GRP. 7, THE SEDONA CANADA PRINCIPLES: ADDRESSING ELECTRONIC DISCOVERY 14–15 (Colin Campbell et al. eds., 2008), available at http://www.thesedonaconference.org/dltForm?did=canada_pincpls_FINAL_108.pdf; *Hong King Practice Direction 5.2*, http://legalref.judiciary.gov.hk/doc/whats_new/prac_dir/html/PD5.2.pdf (last visited Oct. 15, 2011); *CM 6—Electronic Technology in Litigation*, FEDERAL COURT OF AUSTRALIA, <http://www.fedcourt.gov.au/how/>

Civil law countries permit no discovery as that concept is known in the United States.⁵⁸ In civil law jurisdictions, parties exchange electronic data and paper documents in a process known as “disclosure.” The court directs each party to disclose materials that support its case or, in some instances, the adversary’s case. This information is often stated with specificity.⁵⁹ Almost all of the data and documents disclosed are admitted into evidence at trial, in stark contrast to the U.S., where the rules of evidence restrict admissibility to a very small percentage of the often millions of pages produced during the discovery phase.⁶⁰ This distinction perhaps creates an aversion on the part of civil law jurisdictions to processing data for purposes of U.S. litigation. This reluctance may well extend to the preservation of ESI by means of a legal hold. The variations between civil and common law systems inform the analysis of whether a U.S. legal hold may violate data protection and privacy laws in the E.U. and elsewhere.⁶¹

The next level of inquiry concerns the character of the data sought to be preserved: is it personal data or is it data that is otherwise protected by statute or other provision? If so, does preservation pursuant to a U.S. legal hold constitute “processing” of that data? If data retention as a result of a legal hold is

practice_notes_cm6.html (last visited Oct. 15 2011); *Practice Direction 31A—Disclosure and Inspection*, UK MINISTRY OF JUSTICE, http://www.justice.gov.uk/guidance/courts-and-tribunals/courts/procedure-rules/civil/contents/practice_directions/pd_part31a.htm (last visited Oct. 15, 2011) (noting that these provisions do provide for preservation of information, though the U.K. is a member of the E.U. and is subject to its laws passed to enable the Directives).

⁵⁸ See *E.U. Working Document*, *supra* note 2, at 3–5.

⁵⁹ *Id.* at 4.

⁶⁰ SEDONA FRAMEWORK, *supra* note 13, at 16.

⁶¹ Privacy and data protection laws in many parts of the world are, to greater or lesser degrees, modeled on the European Union Privacy Directives. See, e.g., *Chile and Argentina adopt data protection laws*, PRIVACY LAW AND BUSINESS INTERNATIONAL NEWSLETTER, <http://www.worldlii.org/int/journals/PLBIN/2000/48.html> (last visited Oct. 15, 2011) (explaining that Argentina adopted similar privacy laws to Chile, both of which were modeled after EU Privacy Directives); [Act on the Protection of Personal Information], Law No. 57 of 2003 (Japan), *translated at* <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>; *Personal Information Protection and Electronic Documents Act*, S.C. 2000, c.4 (Can.).

considered “processing,” is the requirement to preserve the data a legitimate legal obligation for which processing can occur? If not, are there any other exceptions or derogations that would allow the issuance of a hold? Alternatively, can a hold be tailored and implemented in a way that comports with regional and local law?⁶² These concerns can be addressed, as will be discussed in Part IV, by drafting a legal hold notice tailored to the facts and issues of the litigation at hand, and implementing the hold in a way that minimizes the potential intrusion upon the concept of privacy of the individual.

Within the European Union, the discussion should begin with Directive 95/46/EC on the processing of personal data and the free movement of such data.⁶³ “Personal Data” is defined as that which can be traced to an identifiable person and includes email.⁶⁴ Email, which readily identifies the author and/or the recipient associated with its content, is the category of information most demanded in U.S. discovery and is often the main subject of legal holds.⁶⁵

The act of processing personal data is subject to the provisions of the Directive, and member states’ enabling legislation. “Processing” is a term of art, and outside the U.S. it comprises a far broader swath of activities than those to which American lawyers and judges are accustomed, including, according to the European Commission Article 29 Working Party on data protection, preservation of the sort conducted during the implementation of a U.S. legal hold.⁶⁶

Within the E.U., personal data may only be processed in pursuit of a purpose allowed by the Directive. The Directive is, in effect, a regulation of exclusion (i.e., the activity is prohibited, except where it is expressly permitted).⁶⁷ Litigation in the U.S. is not necessarily considered a legitimate purpose for processing

⁶² SEDONA FRAMEWORK, *supra* note 13, at 3–4.

⁶³ Directive 95/46, *supra* note 14.

⁶⁴ *See id.* at art. 2(a).

⁶⁵ *See* European Commission, *Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data* (June 20, 2007), <http://europa.eu.int>.

⁶⁶ *E.U. Working Document*, *supra* note 2, at 8–10.

⁶⁷ Directive 95/46, *supra* note 14, at art. 7(c).

pursuant to the Directive.⁶⁸ “Processing” is defined broadly, as “any set of operations . . . (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.”⁶⁹ The Working Party does not distinguish between preserving-in-place, which may require no affirmative steps other than a “Do Not Delete” notification sent to those covered by the hold, and more affirmative steps such as imaging the hard drive and sending a copy to a server, or actually segregating potentially relevant data and removing it to a secure location. The Working Party went on to pose a potential complication for U.S. entities and counsel by stating, “there may be a further difficulty where the data is retained for additional pending litigation or where future litigation is reasonably foreseeable.”⁷⁰ Notwithstanding the fine semantic distinctions of the phrases “reasonably anticipated” and “reasonably foreseeable,” the Working Party statement provides some support for the notion that following the dictates of *Zubulake* and *Pension Committee* may place a U.S. corporation with a subsidiary abroad, or a non-U.S. entity facing U.S. litigation with data in an E.U. member state, on the wrong side of the Directives and the member states’ enabling legislation.⁷¹ Other laws of E.U. and non-E.U. states require that personal data be deleted after the purpose for its collection has been accomplished.⁷²

⁶⁸ *E.U. Working Document*, *supra* note 2, at 9.

⁶⁹ Directive 95/46, *supra* note 14, at art. 2(a) (emphasis added).

⁷⁰ *Id.* at 8.

⁷¹ *Id.* at art. 7(c), 7(f). To make sure that no one were to miss the point, the Working Party also noted that “any retention, preservation or archiving of data for such purpose would amount to processing,” and, as such, may only be justified under Articles 7(c) or 7(f) of the Directive. *Id.*

⁷² [Personal Data Protection Code], Decreto Legge 30 giugno 2003, n. 196 (It.), *translated at* <http://www.garanteprivacy.it/garante/document?ID=1219452>; Bundesdatenschutzgesetz [BDSG] [Federal Data Protection Act], Jan. 14, 2003, Bundesgesetzblatt, Teil I [BGBl. I] [Federal Law Gazette I] at 66, § 20, as amended Aug. 14, 2009, BGBl. I at 2814 (Ger.), *translated at* http://www.bfdi.bund.de/cae/servlet/contentblob/1086936/publicationFile/87545/BDSG_idFv01092009.pdf; Loi 78-17 du 6 janvier 1978 de informatique et

Putting data controllers on notice of the issues surrounding preservation of data for litigation purposes, the Working Party stated that “[c]ontrollers in the European Union *have no legal ground to store personal data at random for an unlimited period of time because of the possibility of litigation in the United States however remote this may be.*”⁷³

Justification for retention on the basis of an existing legal obligation in U.S. litigation or the *reasonable anticipation of such litigation* may prove elusive. While the Directive states that the processing of personal data may be undertaken where necessary to fulfill a legal obligation,⁷⁴ it is not definitive whether an obligation arising out of U.S. jurisdictions may qualify for this derogation under the prevailing case law.⁷⁵ Nonetheless, the Directive contains the basis for crafting a legal hold that may meet the dictates of privacy and data protection provisions within and beyond the E.U.

IV. DAWN FOLLOWING DARKNESS: A POTENTIAL WAY FORWARD?

By now, our harried and sleepless General Counsel may be rubbing her eyes in earnest, but she should take heart. The legal risk surrounding the implementation of a legal hold outside the U.S. can be reduced by tailoring the hold to be consistent with

libertes [Law 78-17 of Jan. 6, 1978 on Information Technology, Data Files, and Civil Liberties], Journal Officiel de la République Française [J.O.] [Official Gazette of France], 7 janvier 1978, p. 227–31 as amended by Loi 2004-801 du 6 août 2004, Loi 2009-526 du 12 mai 2009, Loi organique 2010-704 du 28 juin 2010, and Ordonnance 2011-1012 du 24 août 2011, *translated at* <http://www.cnil.fr/fileadmin/documents/en/Act78-17VA.pdf>; [Act on the Protection of Personal Information], Law No. 57 of 2003, art. 27 (Japan), *translated at* <http://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf>; Chan-Mo Chung, *Korea's Recent Legislation on Online Data Protection*, 6 Privacy L. & Pol’y Rep. 38 (1999), *available at* <http://www.austlii.edu.au/au/journals/PLPR/1999/46.html>; *see also* European Data Retention Directive, Council Directive 2006/24/EC, 2006 O.J. (L 105) 54 OR Directive 2006/24/EC, 2006 O.J. (L 105) 54.

⁷³ *E.U. Working Document*, *supra* note 2, at 7 (emphasis added).

⁷⁴ Directive 95/46, *supra* note 14, at art. 7(c), 7(f).

⁷⁵ *E.U. Working Document*, *supra* note 2, at 9.

regional and local rules. It is important to note that the Working Party stated, at the outset of WP 158, that the Directive does not expressly prohibit compliance with U.S. discovery provisions.⁷⁶ The Working Party also acknowledged the bind in which U.S. companies and companies with facilities within the E.U. falling under U.S. jurisdiction may find themselves.⁷⁷ The WP 158 document attempts to reconcile these conflicts through suggestions for a balanced approach to e-discovery, and data retention in particular.⁷⁸ This may bespeak a trend. WP 158 was followed within a short time by a similar set of opinions and guidelines by the data protection authority in France, the Commission Nationale de L'Informatique et des Libertes (CNIL). Both documents were authored by the same individual, Alexander Turk, and demonstrate clear efforts to account for the need to harmonize the demands of the civil and common law systems with regard to disclosures of protected data.⁷⁹

The Directive, like the privacy and data protection laws in most countries, requires notice to the data subject of the uses and disclosures of his or her personal data.⁸⁰ A corporation can meet this requirement by issuing the legal hold notice only to those individuals whose data would be sent to the U.S., as opposed to subjecting the entire company to a broad legal hold, as is customarily done in the U.S. In addition, the typical legal hold notice sets forth the reason for the issuance of the hold (i.e., the litigation caption and venue, as well as a few words about the claims), the categories and formats of information subject to preservation (e.g., email, texts, etc.), the method by which the information should be safeguarded, and the contact information for

⁷⁶ *Id.* at 2.

⁷⁷ *Id.* at 2, 7.

⁷⁸ Alan C. Raul, et al., BNA Privacy and Security Law Report: Assessing the E.U. Working Party's Guidance On Harmonizing U.S. Discovery and E.U. Data Protection Requirements, 8 Privacy & Security L. Rep. (BNA) 409 (Mar. 9, 2009).

⁷⁹ CNIL, *Deliberation No. 2009-474 of 23 July 2009 concerning recommendations for the transfer of personal data in the context of American court proceedings known as "Discovery"* (July 23, 2009), http://www.cnil.fr/fileadmin/documents/enDDDiscovery_EN.pdf.

⁸⁰ *E.U. Working Document, supra* note 2, at 8–10.

any questions.⁸¹ It is arguable that by acknowledging receipt of a notice, the recipient has consented to the use of his or her personal data in U.S. litigation. However, the Working Party's statement casts doubt on whether this constructive acknowledgment would suffice to make the hold fully consistent with the Directive and member state requirements for consent.⁸² Especially in cases where consent is requested by an employer, it may be deemed to have been obtained by coercion inherent in that relationship and consequently, insufficient.⁸³

The concept of proportionality in e-discovery, which has received a great deal of attention in the U.S. in recent years,⁸⁴ may come into play with international legal holds. This notion may make a hold more palatable to data protection authorities outside the U.S. WP 158 notes that the Directive requires that personal data collected must be limited to that which is relevant and not excessive to a particular investigation.⁸⁵ Accordingly, counsel may undertake to craft the legal hold notice so that it is limited to specific issues relevant to the case, rather than merely a date range (e.g. "preserve all email with John Smith from January 1, 2000–January 1, 2005,") or to a broad category of activity (e.g. "preserve all communication relevant to hiring procedures"), as is frequently done in the U.S. Similarly, counsel may instruct data controllers in non-U.S. facilities to limit retention of the subject data to a more focused subset. Such a regimen would require a protocol for defensibly drafting the instructions in the legal hold notice such that any data preserved and retained is only that which is relevant to the issues in the case.

In this regard, it is often helpful to assemble an e-Discovery/Legal Hold Response Team, comprised of local counsel, U.S. counsel experienced in cross-border disclosure

⁸¹ The Sedona Conference, *supra* note 3.

⁸² *E.U. Working Document*, *supra* note 2, at 8. Consent between employer and employee may be deemed per se involuntary by certain jurisdictions. *Id.*

⁸³ *Id.*

⁸⁴ The Sedona Conference, *The Sedona Conference Commentary on Proportionality in Electronic Discovery*, 11 SEDONA CON. J. 289, 294 (2010).

⁸⁵ Directive 95/46, *supra* note 14, at art. 6; *E.U. Working Document*, *supra* note 2, at 10.

issues, IT personnel, a compliance officer or in-house counsel, and a technical consultant. Among other things, the Team will assess the issues involved in the subject litigation and identify the various repositories, devices, and other locations where potentially relevant data subject to a preservation duty may reside. They will then craft the hold notice accordingly and communicate the hold to the target data custodians. This Team could also craft a targeted hold notice and process to focus on information specifically relevant to the subject litigation (i.e., excluding facially irrelevant data and sensitive personal data such as union affiliation, political affiliation, health information, etc).⁸⁶

One could also envision an international agreement on a safe harbor, similar to that of FRCP 37(e), whereby a U.S. court would not impose sanctions for failing to provide data that was not produced due to it falling outside the scope of a reasonably tailored legal hold that was implemented in good faith.⁸⁷ In addition, practitioners should also consider abiding by the current U.S. trends toward more cooperation among adversaries to international legal holds, and open the channels of communication as early as possible to discuss preservation challenges and parameters applicable to the countries at issue.⁸⁸

International comity may also provide an approach for recognition of and respect for the U.S. obligation of preservation. In this regard, counsel may, where appropriate and practicable, seek the advice of local counsel in the jurisdiction where the data was created, for the possible purpose of notifying the local data protection authority or judicial authorities before a legal hold is

⁸⁶ However, it is important to consider situations in which sensitive information may be highly relevant, such as employment matters and cases involving trade secret theft.

⁸⁷ FED. R. CIV. P. 37(e) (“Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system.”).

⁸⁸ It should be noted that the possibility of cooperation with regards to a legal hold may be viable when the preservation duty is triggered at the time a complaint is filed, or when a party is on similar notice, as opposed to cases where the reasonable anticipation of litigation occurs well before parties are in a position to communicate directly.

implemented. This would, at a minimum, show respect for the laws of the non-U.S. sovereign and might aid in the mutual understanding of the exigencies of the differing legal systems. U.S. courts, for example, must follow a five-factor balancing test, first enunciated by the U.S. Supreme Court in *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*,⁸⁹ when considering the application of non-U.S. law.⁹⁰ Furthermore, the WP 158 and the 2009 CNIL opinion speak to the need for flexibility in an era of accelerating global commerce and communications.⁹¹ A standardized set of “legal process protocols” could provide a cost-effective, consistent solution that respects important data protection values of legitimacy, proportionality, and notice in the EU, while accommodating the truth-seeking and dispute resolution functions of the U.S. litigation system.⁹²

⁸⁹ 482 U.S. 522, 545 (1987). The five-factor *Aérospatiale* test, codified in the Restatement (Third) of Foreign Relations Law § 442 (1987), directs courts to consider the importance of the documents to the litigation, the specificity of the request, the origin of the documents, the availability of other means to obtain the documents, and the balance between the interests of the U.S. and that of the situs of the documents. *Id.* Following an analysis of these factors, § 442(1)(c) gives U.S. courts the power to order production of information previously shielded by foreign law. Other factors that a U.S. court may look to include the hardship a party faces in complying with a discovery request, the good faith efforts of the party refusing production, as well as whether the entity is a party or a non-party to the litigation. *Aérospatiale*, 482 U.S. at 545.

⁹⁰ *Id.* at 545 n.28 (“While we recognize that § 437 of the Restatement may not represent a consensus of international views on the scope of the district court’s power to order foreign discovery in the face of objections by foreign states, these factors are relevant to any comity analysis: (1) the importance to the . . . litigation of the documents or other information requested; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; and (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.”).

⁹¹ CNIL, *Deliberation No. 2009-474 of 23 July 2009 concerning recommendations for the transfer of personal data in the context of American court proceedings known as “Discovery”* (July 23, 2009), http://www.cnil.fr/fileadmin/documents/enDDiscovery_EN.pdf.

⁹² Alan C. Raul, et. al., *supra* note 78, at *4.

V. CONCLUSION

In addition to tailoring the legal hold to comport with non-U.S. law, it behooves foreign corporations that do business in the U.S. to also consider implementing records retention protocols that include U.S. litigation hold procedures, to the extent possible under local law, lest they face sanctions if preservation efforts are deemed to fall short of U.S. standards. With mutual understanding of how U.S. judges may rule on a particular choice of law matter and how non-U.S. data protection and judicial authorities may view retention of protected data, foreign litigants and U.S. parties with facilities outside the U.S. can better construct their efforts to assure needed information is there when its production is required.
