

Digital Discovery Across Borders

In his best-selling book *The Post American World* (W.W. Norton 2008), Fareed Zakaria

observes “American business is increasingly aware of the shifts taking place around the world and is responding to them rapidly and un sentimentally. Large U.S.-based multinationals almost uniformly report that their growth now relies upon penetrating new foreign markets. With 2–3 percent a year in the United States and 10–15 percent abroad, they know they have to adapt to a post-American world—or else lose out in it.” (*Id.* at 45–46).

The inverse is also true: non-U.S. corporations have left their footprints in the U.S. and, accordingly, find themselves enmeshed in the intricacies of U.S. litigation and government investigation, with our expansive U.S. pretrial discovery and a concomitant need for guidance in the preservation, collection and production of electronic evidence from off-shore locations.

Over 90 percent of all business documents were digital in 2008. As businesses expand their operations globally, evidence will be found increasingly in countries in the European Union, Asia and South America. Counsel who assume that documents—e-mail, for the most part—and data may be obtained from these countries as easily as from a factory in Indiana, may be in for a very protracted, expensive migraine

E-mail is considered “personal data” in the European Union, and personal data may not be sent outside the European Eco-

nomie Area, which encompasses the EU member states plus Norway, Iceland and Lichtenstein, to a country that provides less personal privacy protection, such as the U.S., unless certain agreements are in place to provide commensurate confidentiality privacy protection. Only Canada and Argentina and the territories of the Isles of Guernsey and Mann meet the EU’s privacy standard. Certain countries, such as France, in its “Blocking Statute,” consider transmitting commercial or technical data for use in a foreign judicial proceeding a criminal offense. Italy affords certain company data the same level of protection as personal data. Bermuda forbids export of financial data, even for compliance with a U.S. subpoena, without explicit court approval. Curiously, Japan, like a number of South American countries, permits employees to demand production of data pertaining to them and, in some cases, to request amendment, correction or even deletion.

If a corporation wants to whistle in the graveyard—unconcerned in difficult circumstances—by deferring attention to cross-border data transmission issues with the attitude, “We never get sued, so why spend money on this?,” they will probably, sooner not later, face a global business reality: transfer of certain *internal data*, such as Human Resources information, can trigger foreign privacy laws because the personal information contained in those files, in most EU countries, is protected under data privacy laws.

So, what is an attorney to do if a Human Resources department in the United States wants to track employee performance in Italy? What if a U.S. court orders produc-

tion of Quality Assurance e-mails created in France, housed on a server in Singapore, and most easily accessed from an employee’s laptop in the U.K? How does one review e-mails for privilege when the laws of 10 countries apply? Or, as in one case in the Southern District of New York (*In Re Rivistagmine Patent Litigation*, 237 F.R.D. 69 (S.D.N.Y. 2006)), how does one proceed if the laws of *nineteen* countries, apply? And how do you respond to the judge who intones, “This is an American court, counselor. We follow U.S. Rules of Civil Procedure. Get the documents here or answer to me,” while you stare down at your shaking hands as your foreign privacy law Protective Order motion vanishes like breath in the winter.

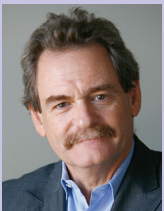
No, the above-mentioned scenarios are not episodes of *The Twilight Zone*, stress-induced nightmares or the final exam essay worth half of the grade in International Commerce 101. The scenarios represent the reality increasingly faced by any business that has, or aspires to have, a multinational footprint.

A management solution is found in the famous Roman proverb, attributed to Julius Caesar, which he employed during the Gallic Wars—*Divide et impera*—divide and conquer. It lies in dividing the digital world challenge into three stages: acquiring knowledge of the issues; establishing practicable and defensible protocols for managing, preserving, accessing and producing evidence from non-U.S. locations; and utilizing consultants and local counsel with expertise in the local privacy and data protection enforcement laws.

Lesson One in Cross-Border Conflicts: Privacy and Discovery Laws Differ

Fundamental to understanding the exquisite complexity of cross-border data transmission for business or litigation is awareness of the significant differences in the concepts of discovery, data privacy and data protection between the U.S. and the rest of the world. Imagine, if you will, the response of a judge in the U.S. faced

■ Kenneth N. Rashbaum is a Director of Consulting at Fios, Inc., working out of New York City and specializing in international data management and discovery. Mr. Rashbaum assists clients with cross-border electronic document management and litigation and investigation readiness. He also consults and advises on offshore outsourcing of data services, readiness for proceedings under the HIPAA Privacy and Security Rules, and protocols for compliance with state identity theft protection laws. He is a member of DRI’s Technology and Electronic Discovery Committees.



with objections by a European Data Protection Authority to a discovery request: “Those Europeans just won’t let us get on with the business of litigation, or even just the conduct of business!” Now envision the response of a German, French or British judge faced with a request from a U.S. court or agency: “Here come the Americans again, trampling on the privacy or our citizens. Will they ever stop?”

Common law and civil law concepts of pre-trial discovery, or “disclosure,” as it is called in Europe, are poles apart. With the exception of the United Kingdom and Canada, the rest of the world follows a civil law as opposed to a common law system. In France, for example, pre-trial discovery disclosure is limited to documents that may be admitted as evidence at trial. Disclosure is supervised by a judge, who decides relevance and admissibility of proposed evidence. In Germany, parties are not required to disclose documents to each other; they must only produce those documents that will support their claims. The timeworn U.S. discovery demand, “Any and all documents related to...” cuts no ice in most civil law jurisdictions, and it will not pass muster even in common law jurisdictions such as the United Kingdom, where documents, for the most part, cannot be described by category.

This discovery/disclosure approach contrasts with that in the United States, where the parties are required, pursuant to FED. R. Civ. P. 26 (recently amended) to provide relevant material, “regarding any matter not privileged.” In the spirit of liberal discovery, a federal court is likely to grant a motion to compel disclosure of documents and data under the standard that it is likely to lead to admissible evidence.

Global businesses must serve both masters; they must navigate a path through the privacy waters between the Scylla of U.S. courts moving cases forward with a minimum of discovery-related delay, and the Charybdis of non-U.S. data protection agencies and like-minded courts charged with enforcing privacy and data protection legislation in the European Union and beyond.

Lesson Two: Differing Notions of Privacy Affect Protection Schemes

The United States’ approach to privacy is a segmented, or industry-specific approach,

as illustrated by HIPAA in the health care industry, and the Gramm-Leach-Bliley Act in personal finance. Additionally, data created and stored on a corporate network is considered the property of the corporation; indeed, most businesses require employees to sign an acknowledgement to that effect and, in the recent case *Scott v. Beth Israel Medical Center* (17 Misc. 3d 934, 847 N.Y.S.2d 436 (Super. Ct. N.Y. Co. 2007)), a New York trial-level court held that, because Dr. Norman Scott had signed such an acknowledgement, Dr. Scott had waived attorney-client privilege in his communications with his counsel, which were transmitted over the hospital’s network. Dr. Scott declined to appeal the decision.

A decision such as *Scott* would cause the rest of the developed world to shudder, or at least shake its collective head. Outside the U.S., privacy is a fundamental right, manifest in the privacy and data protection schemes of the European Union and its member states, Japan, and Venezuela and other Latin American states, as well as common law countries such as Canada and the United Kingdom.

Indeed, France takes the protection of employee privacy to a rarified level. While many U.S. corporations require employees to sign an acknowledgement in which the employee asserts that he or she is aware that e-mails on the company network may be monitored or accessed, French Criminal Law Article 226-15 considers it a “malicious,” and thereby punishable, act for someone other than the recipient of an e-mail to open it. Understanding that privacy is a highly protected right in most of the world will provide a beacon for navigating the myriad of data and privacy protection schemes outside of the United States.

The European Union and Beyond

Within the European Union, data privacy and protection stem from EU Directives 95/46 EC and 97/66 EC. These directives are the end product of a privacy protection initiative that began with the European Convention on Human Rights, a treaty of the Council of Europe. Article 8 of this convention states simply, “Everyone has the right to respect for his private and family life, his home and his correspondence.” Concerned in the 1970s that this provi-

sion would not cover personal information or personal computer data, the Council of Europe took additional steps over the next 20 years, commensurate with advances in technology, culminating in the 1995 European Union Data Protection Directive. Once again, finding eloquence in simplicity, the Directive states, in Article 1, that member states “shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect of the processing of personal data” (emphasis supplied). In pursuit of the goal of this provision, personal data may not be sent outside the European Economic Area to a country that provides less privacy protection. As will be discussed below, exceptions to this provision exist, such as consent of the data subject, and contracts, agreements and conventions that can enable such transmission to countries like the U.S.

The term “shall” indicates that member states must pass legislation enabling the protection provisions of the directives. All member states have implemented such provisions and, in some cases, they are far stricter than those envisioned by the directives. France has implemented a Blocking Statute, French Penal Law No. 80-538, under which it is a criminal offense to “request, seek or communicate, in writing, orally or in any other form, documents or information of an economic, commercial or industrial financial or technical nature leading to the constitution of evidence with a view toward foreign judicial or administrative procedures.”

While the majority of U.S. courts have denied motions for protective orders based upon the Blocking Statutes, *see Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443 (C.D. Cal. 2007), as to the Netherlands’ statute and *United States v. Vetco*, 691 F.2d 1281 (9th Cir. 1981), with regard to Italy’s law, this view may well be changing in light of the first published affirmation of a conviction under this provision. In a case arising out of U.S. litigation in the Southern District of New York, a French attorney ran afoul of the Blocking Statute by speaking to an ex-director with an eye toward obtaining information to be used in the matter of *Strauss v. Credit Lyonnais*, 2000 U.S. Dist. Lexis 38378 (E.D.N.Y. May 25, 2007). The French Supreme Court upheld the conviction and the €10,000 fine.

You may ask how, if faced with a Blocking Statute, can you obtain evidence from a country that has such a provision? Several countries, including France, Germany, Italy, China, Japan, China and the United Kingdom are signatories to the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (The Hague Convention). Under the uniform procedure contained in the Hague Convention, letters of request, also known as letters rogatory, issue from a court in the forum nation to the court in the country where the information is located. Depositions, where permitted by the procedures of the signatory country, are taken before a diplomatic or consular official. It is important to note, however, that each signatory country may carve out exceptions to the Hague Convention through its "Declarations." Thus, the use of local counsel is particularly critical where the Hague Convention is utilized.

Further, despite the holding in *Strauss v. Credit Lyonnais*, it is still only a minority of U.S. courts that will agree that the Hague Convention, rather than the Federal Rules of Civil Procedure, should be used to obtain evidence outside the U.S. Faced with a Blocking Statute, counsel should request that a U.S. court employ the five-factor test articulated by the U.S. Supreme Court in 1987 in the case of *Societe Nationale Industrielle Aerospatiale v. United States District Court* (482 U.S. 522 (1987)). The *Societe Nationale Industrielle Aerospatiale* court, while declining to rule that the Hague Convention is the only means by which parties may obtain evidence abroad, held that factors to be considered included the importance of the documents to the litigation, the availability of alternate means to obtain the information, and the relative interests of the U.S. and the foreign sovereign. The results of this balancing test have not necessarily followed expected logic. While one would think that a statute like France's law, which threatens imprisonment, would indicate rather heightened interest on the part of the foreign sovereign, most courts have held that this factor is outweighed by others, including—although perhaps unspoken—expedient progress of a lawsuit.

Italy treats company data with the same level of protection as personal data, and though it is a signatory to the Hague Con-

vention on Evidence its exception states that it "will not issue letter of request for the purpose of obtaining pre-trial discovery of documents as known in common law countries." Spain recently amended its Organic Law 15.1999, which implements the EU Privacy Directives, with Regulation 1720.2007. This recent provision sets up a mechanism

■

The timeworn U.S.
discovery demand, "Any
and all documents related
to..." cuts no ice in most
civil law jurisdictions.

■

for authorization of international transfers of personal data by Spain's data protection agency, the Agencia Espanola de Proteccion de Datos (AEPD). Unless the parties have agreed to protect the data with an agreement containing Model Contract Clauses approved by the European Commission or the company is registered with the U.S. Safe Harbor Program (as discussed below), all transfers of personal data must be presented to the AEPD for authorization, which is decided by the director of the AEPD, to adopt a resolution approving or rejecting the transfer. However, the regulation gives the director *three months* to decide.

Conditions are not necessarily easier outside the European Union. Japan's Personal Information Protection Act (PIPA) is administered by 11 different ministries. Data may be shared with third parties on a consent basis, although "Notice," may suffice if the purposes of the disclosure are clearly stated, as to an "opt-out," *but*, pursuant to Article 23, paragraph 2, only upon condition that the provision of data will cease upon request of the data subject. Violations of PIPA are punishable by a fine of up to ¥300,000 or imprisonment for up to six months.

Venezuela, interestingly, follows a similar scheme under the auspices of a theory known as *habeus data*. Pursuant to Article 28 of the 1999 Constitution, an individ-

ual may, subject to certain limitations, ask that data on himself or herself be produced, and to "learn its use and purpose." Further, he or she may request "its update, correction or destruction of erroneous or (if it) were to legitimately affect their rights." Like France, Venezuela has sharp-toothed Blocking Statutes. In *Lynondell-Citgo Refining PP v. Petroleos de Venezuela, S.A.*, (2005 WL 102461 (S.D.N.Y. May 2, 2005), the defendant accepted an adverse inference instruction rather than risk violation of Venezuela's Special Law Against Information Systems Crimes.

Similar Blocking Statutes are found in South Africa, Switzerland (for banking information), Canada (for matters that would infringe on sovereign interests) and China (for information deemed a "state secret").

What Is a U.S. Multinational Corporation to Do?

Initially, consider the character of the data. Personal data is protected in most non-U.S. jurisdictions. It is defined very broadly in the EU 1995 directive as "any information relating to an identified or identifiable natural person." E-mail, with the name and identifying information (*i.e.*, e-mail address) of the author is considered "personal data." The U.K., however, may be moving away from such a broad definition. In *Michael John Durant v. Financial Services Authority* ([2003] EWCA Civ. 1746 (8 December 2003), the Supreme Court of Judicature (Civil Division) noted that protections for personal data should be limited to information "that directly names or directly refers to (the data subject)." The U.K. Information Commissioner, though, has declined to follow this case with relaxed standards for e-mail protection.

Next, if the data are not personal, consider whether a Blocking Statute applies. In certain countries such provisions apply for all data sought for use in a foreign judicial proceeding, while in others, these statutes are industry-specific.

The Virtual Aspirin: Privacy Protection Protocols and Approved Agreements

The keys to smoothing the road to transfer of personal data for business purposes and litigation readiness are (1) policies and procedures to protect the privacy of employees'

personal information, (2) early retention of consultants for preparation of those protocols and concomitant training, and (3) local counsel.

Litigation readiness can be simplified, to a degree, if the corporation has utilized one of the four modalities below to bring personal data to the U.S. If the data is already here for business purposes, or can be brought here, without violating a blocking statute, counsel will not have the unenviable task of trying to teach an American judge foreign privacy law to block disclosure that could be illegal in the country of the data's origin.

All four methods below require that the business agree to restrict transfer and disclosure of personal information to certain specified uses, to notify the data subjects—by acknowledgements, web site notice or other means—and protect it to a level commensurate with the European Union. Indeed, a number of non-EU countries, such as Chile, Australia, New Zealand and Russia have adopted data protection and privacy schemes based, to a great extent, on the EU model.

The first method for simplifying litigation readiness is securing the informed, voluntary consent of the data subject. This may be impractical in a business with thousands of employees, and there is a presumption in Germany that consent requested by an employer is not freely given. In certain countries, such as Japan, consent can be obtained through a notice, which sets forth such provisions as (1) the steps taken to safeguard privacy of certain types of “sensitive information” for which the EU provides heightened protection, which include ethnic origin, religion, and trade union membership; (2) how personal information is used by the company, such as employment purposes, the need to establish or defend legal claims, accounts and records, for example; and (3) *importantly*, the fact that the personal data may be transferred outside the European Economic Area, and sometimes to countries that provide less privacy protection.

Some countries provide “opt-outs” for such transfers, while others, like France, require that this notice indicate that such transfers will be subject to existing data protection requirements, or that the trans-

fers will be subject to certain agreements. Accordingly, many multinationals utilize one of the following forms of agreements.

U.S. Safe Harbor Program

Companies that fall within the jurisdiction of the Federal Trade Commission or the U.S. Department of Transportation may register

■

Understanding that
privacy is a highly protected
right in most of the world
will provide a beacon for
navigating the myriad of
data and privacy protection
schemes outside of
the United States.

■

for the U.S. Safe Harbor Program. The company certifies that it has a privacy protocol that adheres to seven principles consistent with EU privacy protection: 1) notice (to data subjects); 2) choice (opt-out and opt-in); 3) onward transfer; 4) access (by data subjects); 5) security; 6) data integrity; and 7) enforcement. Companies must certify such adherence annually, and agree to submit to the jurisdiction of the U.S. Department of Commerce. They also must renew their self-certification annually, agree to cooperate with the Data Protection Agencies of the originator countries and abide by their enforcement orders.

The U.S. Safe Harbor Program is recognized by all European Union member states. Thus, no prior Data Protection Agency approval is required for transfers of personal data. The Safe Harbor Program does not cover transfers from non-EU countries, and it pertains only to transfers to the United States.

Model Contract Clauses

The European Commission has approved

model contract clauses for inclusion in data transfer agreements. These clauses require that the data importer maintain levels of privacy protection commensurate with the EU directives. Agreements incorporating these clauses are acceptable to EU member states, but some members still require prior approval of the agreements, in contrast to U.S. Safe Harbor. Parties to the agreement do not submit to U.S. government jurisdiction, and fault, if any, is apportioned by liability.

Binding Corporate Rules

Binding Corporate Rules (BCRs) are a company's code of conduct with regard to transfer of personal data. The advantage of BCRs is that they constitute one set of rules for transfers around the globe. While an apparently elegant solution to a complex problem, BCRs, until recently, were the distant, third alternative to data transfer agreements because of disagreements within the EU regarding their use and the need to have BCRs approved by Data Protection Agencies in each country of origin. The only countries that have approved BCRs to date are the U.K. (General Electric), Denmark (Phillips) and Germany (Daimler-Chrysler). No company has achieved BCR approval by agencies in all countries in which it transacts business.

This may be about to change. On June 30, 2008, the Article 29 Working Party of the European Commission announced that it plans to issue a BCR “toolbox” that would assist companies and Data Protection Agencies in drafting and approving BCRs by providing a framework for the structure of BCRs, checklists and FAQs. The Article 29 Working Party's statement that BCRs “constitute the best solution for global companies” to cover data transfers around the world, indicates that BCRs may be the solution of choice within the next few years—if Data Protection Agencies outside Europe evince similar enthusiasm.

Virtual Prevention: Planning for Data Transmission Process

Digital maladies, such as improper transfer or disclosure of personal or sensitive information, can strike with unimagined speed. Human reaction time cannot keep pace; there is no way to retrieve an errant

transmission. Once the genie is out of the bottle and the company's reputation is damaged, defense and remediation costs can be considerable. The key to preventing such occurrences is in planning.

As with many medical conditions, the first step for most companies is to acknowledge that they need help and to obtain it. Gap analysis, to determine needs and parameters, is an appropriate first step. Many companies setting out on this journey retain consulting firms with experience in designing cross-border data transmission protocols to perform the gap analysis

and, later, to work with in-house or outside counsel to draft policies and procedures that comport with privacy protection schemes. The procedures, in particular, should be drafted in consultation with interdisciplinary work groups composed of company legal, IT and records management departments, and representatives of the business units most affected by data privacy and protection issues. To be effective, the policies and procedures must be living documents; employees must be trained on their use and implementation, and a structure for compliance monitor-

ing should be created. Courts have stated repeatedly that, while they do not expect perfection, they will require reasonable steps toward compliance.

Courts will expect to see documented evidence of the efforts expended to comply with local privacy and data protection laws. Local counsel, therefore, is a critical ingredient in this virtual formulary, which, if created as outlined above, should go far toward achieving a state of cross-border personal data transmission analgesia. 