



DIGITAL DISCOVERY & E-EVIDENCE



VOL. 8, NO. 9

REPORT

SEPTEMBER 1, 2008

Reproduced with permission from Digital Discovery & e-Evidence, Vol. 08, No. 09, 09/01/2008. Copyright © 2008 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

PRODUCTION OF DATA PROTECTED BY FOREIGN STATUTES

More and more litigators are representing companies with interests and employees both in the United States and abroad. Whether as defendant or plaintiff, these multinational corporations face the very real prospect that to litigate their case in the United States they may be required to obtain and produce information and data from around the world. This article suggests an approach for resolving a demand for the production of data that is protected from disclosure by a foreign nation’s laws.

Is Personal Data Located Outside the United States ‘Not Reasonably Discoverable?’

BY DAVID J. KESSLER, CHRISTOPHER P. COVAL AND PETER BLENKINSOP

There has always been a degree of tension between U.S. discovery and certain foreign laws. While selected countries have enacted “blocking statutes” declaring various categories of data (such as banking information) to be secret or non-transferable, U.S. courts have found such documents to be discoverable, and parties can be sanctioned for not producing them.

The ensuing conflicts have historically been relatively minor because the blocking statutes either have covered only a specific set of data from a specific industry (i.e., Swiss banking laws) or were from a jurisdiction that involved little U.S. litigation (i.e., Panamanian criminal codes regarding confidential corporate information). However, their incidents are now mounting due to the convergence of two forces: globalization and the protection of personally identifiable information around the world, particularly in the European Union.

As more and more countries conduct business in the United States and abroad they increase the probability that they will sue or will be sued in the United States and be in possession of potentially relevant data abroad. Simultaneously, personally-identifiable information, protected by foreign statutes, is often commingled with other data, which increases the probability that the protected data could be called for in a U.S. litigation. Thus, the potential for conflict is rising on both sides and companies and counsel unprepared to navigate these waters risk violating court orders at home or data protection laws abroad.

A New Defense Against Foreign Production. However, the recent Amendments to the Federal Rules of Civil Procedure may have strengthened a company’s defense against having to produce protected data from overseas, particularly new Rule 26(b)(2)(B). In a nutshell, this new rule allows parties to argue that they should not be required to search, collect, and produce data

from “not reasonably accessible sources due to *undue burden and cost*” (emphasis supplied).

This article looks at how Rule 26(b)(2)(B) can be used in conjunction with the historical comity analysis undertaken by federal courts when a foreign statute purports to block U.S. discovery. First, it discusses foreign blocking statutes and, in particular, the EU Data Protection Directive. Second, it reviews the traditional analysis of such statutes by federal courts. Third, this article analyzes Rule 26(b)(2)(B) and its possible application to international discovery. Fourth, and finally, it examines some of the potential advantages of using Rule 26(b)(2)(B) in conjunction with the standard comity analysis.

Foreign ‘Blocking Statutes’ and the EU Data Protection Directive

The broad civil discovery permitted by federal courts can conflict with a wide range of foreign regulations that seek to protect the confidentiality of information. See, e.g., *In re Westinghouse Electric Corp. Uranium Contracts Litigation*, 563 F.2d 992, 994-995 (10th Cir. 1977) (involving discovery orders that conflicted with the Canadian Uranium Information Security Regulations, promulgated under the Canada’s Atomic Energy Control Act).

Article 273 of the Swiss Penal Code, for example, prohibits, with the threat of fines or imprisonment, the disclosure of “a manufacturing or business secret” to a “foreign official agency, a foreign organization, a private enterprise, or their agents.” The definition of a “business secret” under Swiss law is apparently much broader than a “trade secret” in an American jurisdiction.¹

In France, French Penal Code Law No. 80-538 is intended to protect French businesses from excessive discovery in foreign litigation by requiring that discovery of documents located in France must be conducted under the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, T.I.A.S. No. 7444, codified at 28 U.S.C. § 1781; see, e.g., *Madden v. Wyeth*, 3-03-CV-0167, 2006 U.S. Dist. LEXIS 880 (N.D. Tex. Jan. 12, 2006).

Even more problematic examples are Articles 89 and 93 of the Panamanian Commercial Code, which prohibit the disclosure of copies of corporate records or even the removal of such records outside of Panama. Articles 168 and 170 of the Panamanian Criminal Code make it punishable by fines and imprisonment to disclose confidential information without proper authorization by Panamanian authorities.

In the Cayman Islands, similar laws protect the confidentiality of banking and financial documents. See *In re Grand Jury Proceedings*, 532 F.2d 404, 406 (5th Cir. 1976).

EU Directive 95/46. One looming source of potential conflict with the American tradition of broad civil discovery is the European Union’s Data Protection Direc-

tive (Directive 95/46), which affirms the individual’s right to determine the use of her or his personal data.² Personal data, which is defined very broadly as “any information relating to an identified or identifiable natural person,” may only be “processed” (i.e., collected, used or disclosed) for one of several legitimate grounds for processing specified in Article 7 of the Directive.

On their face, these grounds would appear broad enough to permit processing activities undertaken to meet foreign civil discovery requirements. They include, for example, processing that is necessary to comply with a legal obligation, processing that is necessary for the purposes of one’s “legitimate interests,” and processing pursuant to the data subject’s consent.

However, in practice, EU Member State data protection authorities interpret and apply these requirements narrowly.

EU regulators have previously expressed the position that foreign legal requirements may not automatically qualify as “legal obligations” for purposes of Article 7 because such an interpretation would make it easy for foreign rules to circumvent the objectives of the Directive.

Similarly, under Article 7(f), processing may be found necessary for purposes of a “legitimate interest” only if such an interest is not “overridden by the interests for fundamental rights and freedoms of the data subject.” Even consent can be a problematic basis for processing because EU authorities will examine whether the consent could be withheld or withdrawn by the data subject without adverse consequences, a prerequisite for freely-given, valid consent.

In addition to requiring an adequate justification for the processing of personal data, Article 25(1) of the Directive places restrictions on the transfer of data to a party in a non-member state that does not ensure “an adequate level of protection.” To date, only a handful of countries have been found to offer an adequate level of protection, and the U.S. is not among them.

Moreover, Article 8 of the Directive invokes even stronger protections for sensitive personal data. This applies to data “revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, and trade-union membership,” and data concerning “health or sex life.”

In light of these international protections, how should an American court resolve a demand for the production of data that is protected from disclosure by an EU member nation’s laws?

Compelling the Production of Foreign Data: The Comity Analysis

It is well settled law that the mere fact that data or records are located outside the United States does not mean that they are not discoverable in Federal Court so long as the party has “possession, custody or control.”

Further, it is also well settled that just because the data or records may be governed by foreign laws that

¹ “The term ‘business secret’ has been defined to include ‘all facts of business life to the extent that there are interests worthy of protection in keeping them confidential.’ ” *United States v. Vetco, Inc.*, 691 F.2d 1281, 1287 (9th Cir. 1981) (quoting *Swiss Federal Attorney v. A.*, 98 BGE IV 209 (September 7, 1972)).

² European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *Official Journal of the European Communities of 23 November 1995 No L. 281 p. 31* (available at http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part1_en.pdf).

“block” their discoverability or transfer to the United States, does not deprive U.S. courts from ordering their production. See *Societe Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers*, 357 U.S. 197, 204-206 (1958).

Thus, a multinational company in the midst of litigation might be ordered to produce data from outside the United States which could violate civil or criminal codes from the resident jurisdiction. See, e.g., *Madden v. Wyeth*, 3-03-CV-0167, 2006 U.S. Dist. LEXIS 880 (N.D. Tex. Jan. 12, 2006) (ordering the production of documents from Wyeth’s French affiliates despite the French blocking statute).

However, a multinational party can bring this problem to the attention of the court and seek protection from the request and need to produce. *Societe Nationale Industrielle Aerospatiale et al. v. United States District Court for the Southern District of Iowa*, 482 U.S. 522, 544 n. 28 (1987).

First, the company has the burden to establish that the foreign law bars the discovery at issue, i.e., that there is a foreign “blocking statute.” See *United States v. Vecto*, 691 F.2d 1281, 1289 (9th Cir. 1981); *Columbia Pictures, Inc., et al. v. Bunnell*, 245 F.R.D. 443, 453-454 (C.D. Cal. 2007). Assuming that a party can meet that burden, then the party must persuade the court that the “blocking statute” should excuse the party from producing the pertinent data from abroad.

Comity Factors. When examining these questions, courts conduct a “comity” analysis that balances several factors including, but not limited to:

- (1) the importance of the information requested in the litigation;
- (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;
- (5) the extent to which compliance would undermine important interests of the United States or compliance would undermine important interests of the state where the information is located; and

(6) the degree of hardship on the producing party and whether should hardship is self-imposed. *Columbia Pictures, Inc., v. Bunnell*, Case No. CV 06-1093 FMC (JCx), Order (1) Granting in Part and Denying in Part Motion to Require Defendants to Preserve and Produce Server Log Data and for Evidentiary Sanctions and (2) Denying Defendants’ Request for Attorneys’ Fees and Costs (May 29, 2007); see also, *Societe Nationale*, 544 n. 28.

Courts in the Second Circuit, however, tend to characterize two factors in this comity analysis—the competing interests of the countries involved and the hardship imposed by compliance—as “far more important in the balancing test” than other factors. *Minpeco, S.A. v. ContiCommodity Services, Inc.*, 116 F.R.D. 517, 522 (S.D.N.Y. 1987); see also *Reino de Espana v. Am. Bureau of Shipping*, 03 Civ. 3573, 2005 U.S. Dist. LEXIS 15685, at *9-10 (S.D.N.Y. Aug. 1, 2005).

Given the factually sensitive nature of the various multi-factor comity analyses, it is hardly surprising that court opinions reach different results.

Not Reasonably Accessible Data Sources

One of the biggest changes to the Federal Rules of Civil Procedure that occurred on December 1, 2006 was the introduction of “not reasonably accessible sources” of information in Rule 26(b)(2)(B). The new rule states:

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. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

Id.

Two Tiers. The new rule sets up a “two-tier” system for handling potentially relevant information in not reasonably accessible sources. First, a responding party must identify sources of information that it is not going to provide in discovery because of “undue burden or cost.” See 2006 Advisory Notes (“The responding party must also identify, by category or type, the sources containing potentially responsive information that it is neither searching nor producing.”)

If the opposing parties cannot reach an agreement and the discovery issue spills into motion practice, then the responding party has the obligation to establish that the source is not reasonably accessible. See *id.* (“The parties must confer before bringing either motion.”) and (“The responding party has the burden as to one aspect of the inquiry—whether the identified sources are not reasonably accessible in light of the burdens and costs required to search for, retrieve, and produce whatever responsive information may be found.”).

Second, if the responding party does establish that the source is not reasonably accessible, the requesting party has the opportunity to show “good cause” that discovery should still be allowed from the data source. *Id.* (“The requesting party has the burden of showing that its need for the discovery outweighs the burdens and costs of locating, retrieving, and producing the information.”).

Even if discovery is allowed into the not reasonably accessible data source, the court can limit the scope of such discovery including, but not limited to, shifting the costs of the discovery, including the cost of the review. *Id.*

Identifying Data Sources. The identification of data sources “should, to the extent possible, provide enough detail to enable the requesting party to evaluate the burdens and costs of providing the discovery and the likelihood of finding responsive information on the identified sources.” *Id.*

Unfortunately, the Advisory Notes do not provide much guidance as to what constitutes sufficient “undue burden and cost” to establish that a source of information is “not reasonably accessible.” The case law on this issue has only just begun developing. What is “undue” burden, however, is determined by the context of the case including the parameters set out in Rule 26(b)(2)(C).

Also, the requesting party may obtain limited discovery to test the responding party’s assertions of burden

and cost. *Id.* (“Such discovery might take the form of requiring the responding party to conduct a sampling of information contained on the sources identified as not reasonably accessible; allowing some form of inspection of such sources; or taking depositions of witnesses knowledgeable about the responding party’s information systems.”)

‘Good Cause’ Factors. Where a responding party has established that a source of information is not reasonably accessible, the requesting party can still establish good cause for the discovery. The Advisory Notes provide a non-exhaustive list of factors that courts should consider in its “good cause” analysis:

- (1) the specificity of the discovery request;
 - (2) the quantity of information available from other and more easily accessed sources;
 - (3) the failure to produce relevant information that seems likely to have existed but is no longer available on more easily accessed sources;
 - (4) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources;
 - (5) predictions as to the importance and usefulness of further information;
 - (6) the importance of the issues at stake in the litigation; and
 - (7) the parties’ resources.
- Id.*

Although Rule 26(b)(2)(B) expressly applies to “electronically stored information,” the “two-tier” analysis and “good cause” factors may also apply to paper documents and tangible things under the Rule 26(b)(2)(C) proportionality test. Indeed, Judge Scheindlin first identified the seven-factor “good cause” test before the Federal Rules were amended to address electronically stored information. *Zubulake v. UBS Warburg LLC (Zubulake III)*, 216 F.R.D. 280, 283 (S.D.N.Y. 2003) (creating a two-tier analysis and good cause factors before Rule 26(b)(2)(C) was promulgated, which applies to both electronic and paper documents).

Thus, the principles of the Rule 26(b)(2)(B) analysis should apply to all unduly burdensome forms of discovery, not simply those involving electronic data.

Comity Analysis and the ‘Good Cause’ Factors Under Rule 26(b)(2)(B)

The question of whether a discovery will involve “undue burden or cost” under Rule 26(b)(2)(B) tends to focus on the financial costs associated with retrieving or restoring deleted or downgraded electronic information. See, e.g., *Best Buy Stores, L.P. v. Developers Diversified Realty Corp.*, Civil No. 05-2310, 2007 U.S. Dist. LEXIS 88771, at *9 (D. Minn. Nov. 29, 2007) (finding that a downgraded database was not reasonably accessible because of the high cost to restore and maintain the database).

But the rule has two parts: undue (1) burden, or (2) cost.

If the rule were limited to “cost” alone, then the undue “burden” language would be superfluous. A serious argument can be made, therefore, that a realistic potential for civil or criminal liability under a foreign jurisdiction’s “blocking” law constitutes “undue burden” that should relieve the responding party of the obliga-

tion to provide discovery of electronically-stored information absent a showing of “good cause.”

Assuming that such foreign liability can be considered an undue burden, then the factors used to establish “good cause” under Rule 26(b)(2) are quite similar to the factors balanced by courts under the various comity analyses. Both analyses consider (1) the degree of specificity of the request, (2) the availability of alternative means of securing the information, and (3) the importance and usefulness of the information.

Other Similarities. Other factors also are very similar. For example, under the comity analysis, courts in the Second Circuit consider whether the hardship is self-imposed or could have been avoided by the party resisting the foreign discovery. See, e.g., *Minpeco, S.A.*, 116 F.R.D. at 526.

Similarly, courts will not “permit a party who has failed to preserve accessible information without cause to then complain about the inaccessibility of the only electronically stored information that remains.” *Disability Rights Council of Greater Wash. v. Wash. Metro. Transit Auth.*, 242 F.R.D. 139, 147 (D.D.C. 2007). Furthermore, the question of “hardship,” an important factor in the comity analysis, is comparable to the threshold question of “undue burden” under Rule 26(b)(2)(B).

Advisory Notes’ ‘Good Cause Factors’ Not Exclusive. Indeed, the only comity factor with no comparable “good cause” factor under Rule 26(b)(2)(B) is “the extent to which compliance would undermine important interests of the United States or compliance would undermine important interests of the state where the information is located.” But the list of “good cause” factors under the Advisory Committee Notes to Rule 26(b)(2)(B) is not exclusive; rather, good cause must be evaluated in light of the “circumstances of the case.”

The “good cause” analysis, therefore, could be tailored to include such international comity considerations where the “undue burden” at issue is a foreign blocking statute. In sum, the entire comity analysis could be replaced by Rule 26(b)(2)(B) in the context of electronically-stored information.

Advantages of Asserting Rule 26(b)(2)(B) Before or With Comity

Despite the similarities between the comity analysis and the “good cause” factors under Rule 26(b)(2)(B), arguing that documents protected by foreign statutes are not “reasonably accessible” has several advantages over the traditional comity analysis for a party seeking to resist or focus discovery.

Under the comity analysis, the burden of proof always rests with the party resisting discovery. *United States v. Vetco, Inc.*, 691 F.2d 1281, 1289 (9th Cir. 1981) (“The party relying on foreign law has the burden of showing that such law bars production.”) (collecting cases).

Rule 26(b)(2)(B), however, involves a burden shifting analysis. The responding party has the initial burden to show that the discovery is inaccessible due to undue burden or cost. See 2006 Advisory Notes (“The responding party has the burden as to one aspect of the inquiry—whether the identified sources are not reasonably accessible in light of the burdens and costs required to search for, retrieve, and produce whatever responsive information may be found.”)

Once that undue burden is shown, however, the requesting party has the burden of proving that “good cause” exists. See 2006 Advisory Notes (“The requesting party has the burden of showing that its need for the discovery outweighs the burdens and costs of locating, retrieving, and producing the information.”)

Thus, if a party can establish that documents are not reasonably accessible because of foreign blocking statutes—something it would need to undertake under the comity analysis—the party seeking discovery would need to establish the good cause factors, which traditionally would have been the responding party’s burden.

Given the fact-dependent nature of this inquiry, one can see where this burden-shifting could be the difference between international data not being discoverable and a party being sanctioned for failing to produce it.

Is Comity Applicable Only to Sanctions? This leads directly to the second advantage to arguing Rule 26(b)(2)(B): some courts have held that the comity analysis goes to the question of sanctions only, and has no bearing on the question of whether the data is discoverable in the first instance. See, e.g., *Arthur Andersen & Co. v. Finesilver*, 546 F.2d 338, 341 (10th Cir. 1976) (“Societe implies that consideration of foreign law problems in a discovery context is required in dealing with sanctions to be imposed for disobedience and not in deciding whether the discovery order should issue.”)

In these jurisdictions, the responding party must initially decide whether to comply with discovery, risking sanctions if its predictions regarding the court’s comity analysis turn out to be incorrect. Rule 26(b)(2)(B), however, clearly addresses the issue of whether data is discoverable in the first instance. Thus, asserting that protected ESI or other documents are not reasonably accessible eliminates the predicament confronting responding parties in jurisdictions where the comity analysis is a question of sanctions.

A party who fails to persuade the court that the protected data is not reasonably accessible still has the op-

portunity to choose between bearing the burden and cost of producing the information in the United States, or facing sanctions.³

Necessary Showing. The recent Amendments to the Federal Rules of Civil Procedure may have made it easier for companies to avoid producing protected data from overseas. However, regardless of whether a responding party relies on Rule 26(b)(2)(B) or the traditional comity analysis, or both, the party must be prepared to present evidence, perhaps expert evidence, that the foreign blocking statute actually applies and that it has been and likely will be enforced. It must be remembered that, under any of these analyses, the responding party will have to establish undue burden or hardship, and the mere existence of a foreign law that purports to block discovery is unlikely to impress an American court.

David J. Kessler is a partner at Drinker Biddle & Reath LLP in the firm’s Intellectual Property group. In addition to his litigation practice, David is the founder of the firm’s Electronic Discovery and Data Management Task Force.

Christopher P. Coval is an associate at the law firm of Conrad O’Brien Gellman & Rohn, PC, 1515 Market Street, 16th Floor, Philadelphia, PA 19102, T: 215-864-9600, F: 215-523-9620, ccoval@cogr.com.

Peter Blenkinsop is an associate in the Washington, D.C. office of Drinker Biddle & Reath LLP., where he focuses on privacy and data security law.

³ In theory, a party could argue the comity analysis after losing its argument under 26(b)(2)(B), but for all the reasons outlined here this is not likely to be successful. The analysis is very similar and Rule 26(b)(2)(B) is more respondent-friendly.