Discovery Conflict

Foreign Privacy Laws in U.S. Courts

By Thomas P. Branigan and David J. Gentile

Trend in civil matters is to defer to foreign laws that protect personal information.

During the twentieth century, the world experienced a meteoric rise in technologies related to travel and communication. As a result, countries around the world have become connected in ways never thought possible.

International trade, once a risky and economically questionable endeavor, evolved into a common, necessary occurrence. Now, in the twenty-first century, this transformation into a global economy has given rise to the necessity of resolving conflicts between the laws of sovereign entities and international inconsistencies. One such conflict exists in the area of foreign privacy laws and their effect on discovery in U.S. courts. The European Union and many of its constituent countries, most notably Germany, France and Switzerland, have established and enforce laws that protect personal information owned by each of its citizens. These laws can directly conflict with U.S. policies of relatively broad and open discovery in civil litigation. As a result, our courts are increasingly asked to either require discovery of information located outside of the U.S. or to defer to laws and policies of a foreign country that may preclude such discovery.

This article will explore the privacy laws of various foreign countries, focusing mainly on the German Data Protection Act, and the effect foreign privacy laws may have on discovery in cases filed in the United States. The article will also offer a strategy for using these privacy laws in defense of a lawsuit involving an international client or a client with international operations.

European Privacy Laws

German Federal Data Protection Act

In 1977, the German parliament enacted the Bundesdatenschutzgesetz (BDSG), also known as the "Federal Data Protection Act." The BDSG is intended to protect "personal data" from dissemination. "Personal data" is defined as "information concerning the personal or material circumstances of an identified or identifiable individual." BDSG §3(1). The BDSG was originally intended to regulate the handling of personal data by public administration authorities

■ Thomas P. Branigan is a managing partner at Bowman and Brooke LLP in Detroit. A trial attorney, his practice is primarily focused on the defense of complex product liability matters involving catastrophic exposure and complex commercial cases and business disputes. Mr. Branigan is a member of DRI's Commercial Litigation, Product Liability, and Trial Tactics Committees. David J. Gentile is a trial attorney at Bowman and Brooke LLP in Detroit. He specializes in the defense of complex product liability matters and litigation of commercial disputes.

and by private data processors by enforcing the right of the individual to determine the use of his or her own data. *See* BDSG Preamble.

In 1990, the BDSG was amended to further protect the individual from having his or her personal rights infringed upon. *Id.* at para. 4. The amended act provides that an individual must consent to have his or her personal data being collected or stored, absent a prior statutory arrangement. The BDSG does provide exemptions to the basic rule. These exemptions, however, are found mainly in the fields of police investigations, intelligence services or national defense. *Id.* at para. 4.

Because the BDSG is intended to protect individuals from the dissemination of personal data to outside parties, it often directly conflicts with rules of discovery in U.S. courts. The pertinent provision in the act provides that "[t]he processing and use of personal data shall be admissible only if this Act or any other legal provision permits or prescribes them or if the data subject has consented." BDSG §4(1). This provision bars the disclosure of personal data by a public or private entity to a third party without the express consent of the individual, unless it is otherwise permitted by the BDSG or any other legal provision. Under this provision, a party to a lawsuit in the U.S. responding to discovery may not disclose the personal data of a German citizen, including that person's name, address, and phone number, without first obtaining that person's consent.

Other countries in Europe and the rest of the world have enacted similar laws to protect their citizens from disclosure of their personal data without consent. These countries include, but are not limited to, France, Switzerland, Canada, China, Japan and Great Britain. Moreover, the European Union, following Germany's lead, enacted EU Directive 95/46/EC. As with the German BDSG, Directive 95/46/EC protects "personal data" and bars the disclosure of such information to third parties absent consent of the individual or assurance that the information will have the level of confidentiality protection it is afforded in the European Union.

Comity in the Federal Courts

The Restatement Third of Foreign Relations Law of the U.S.

When faced with a conflict of international law, courts routinely turn to the Restatement of Foreign Relations Law of the U.S., currently in its third generation, for guidance. Specifically, when information subject to production is located in a foreign country, courts have referred to Section 442(1)(a) of the Restatement Third. This section provides that a court may order a person subject to its jurisdiction to produce documents or information relevant to an action or investigation, even if the information is outside the United States. Restatement Third of Foreign Relations Law §442(1)(a) (1987).

The Restatement qualifies §442(1)(a), however, by providing that if the laws of the foreign sovereign protect the requested information, the interests of the domestic court must be balanced with those of the foreign sovereign. Section 442(1)(c) provides that a domestic court should employ a five-part test to determine whether the interests of the domestic court outweigh those of the foreign sovereign. The domestic court should take into account:

- The importance to the investigation or litigation of the documents or other information requested;
- The degree of specificity of the request;
- Whether the information originated in the United States;
- The availability of alternative means of securing the information; and
- 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 country where the information is located.

Restatement Third of Foreign Relations Law §442(1)(c) (1987).

This five-part balancing test was developed, in part, by the U.S. Supreme Court in 1958 in *Societe Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers, Attorney General*, 357 U.S. 197, 78 S. Ct. 1087, 2 L. Ed. 2d 1255 (1958). In *Societe International*, the seminal case regarding the issue of comity, the plaintiff, a foreign national, refused to produce documents evidencing the ownership of certain assets subject to the claim, relying on the Swiss penal laws as his basis. When the foreign national refused to comply with the lower court's order compelling production of the documents, the court dismissed the case. The U.S. Supreme Court reviewed the case and held that the district court did not err in ordering the foreign national to produce documents evidencing ownership of assets and having a vital influence upon litigation, even though Swiss penal laws imposed criminal sanctions for exposing such documents. The Court further ruled, however, that in light of the foreign criminal implications, dismissal of the action for noncompliance was not a just remedy.

Courts have started to defer to foreign privacy laws, except in circumstances of extreme domestic interest.

Specific Venues and Trends

Since *Societe International*, and following a flurry of newly established European privacy laws, courts around the U.S. have analyzed the relationship between domestic rules of discovery and foreign privacy laws. These courts have consistently applied the Restatement Third of Foreign Relations five-part test, at times adapting it to the established law of the venue, and a trend is emerging. As the cases discussed below indicate, courts have started to defer to foreign privacy laws, except in circumstances of extreme domestic interest, such as federal criminal prosecutions.

The Second Circuit has reviewed this issue on two separate occasions, first in 1968 in *U.S. v. First National City Bank*, and again in 1972 in *Trade Development Bank v. Continental Insurance Company.* In *U.S. v. First National City Bank*, 396 F.2d 897 (2d Cir. 1968), the Second Circuit recognized the task before it was not one of defining power but, instead, of developing rules governing the proper exercise of power. Adopting the Restatement of Foreign Relations Law (2d) test, the court held that, in criminal proceedings, the interest of the United States to obtain relevant information outweighed the interest of the foreign sovereign to protect data.

In *Trade Development Bank v. Continen-*

tal Insurance Company, 469 F.2d 35 (2d Cir. 1972), the court was asked to determine whether the lower court abused its discretion when it relied on the Swiss Federal Banking Act to preclude the disclosure of the identities of bank clients whose accounts were misused by the defendant to conceal fraudulent transactions. The Second Circuit held that the trial court properly precluded the information from discovery, because the foreign state's interest in privacy outweighed the appellant's interest in proving he was not liable on a bond. These Second Circuit cases illustrate the emergence of a trend: generally, courts have determined that the interests of a foreign sovereign outweighed those of a private entity but not those of the U.S. government.

Counsel should not assume that an established corporate discovery policy takes foreign privacy law into consideration.

In 1982, the Eleventh Circuit reviewed a matter in which a federal grand jury, conducting a tax and narcotics investigation, was permitted to subpoena records maintained by a foreign chartered bank. *U.S. v. Bank of Nova Scotia*, 691 F.2d 1384 (11th Cir. 1982). Again, following the trend, the appellate court held that, in criminal proceedings, the interest of the U.S. in ensuring effective grand jury investigations and the crucial importance of collection of revenue outweighed another nation's interest in protecting the right of privacy incorporated in its banking confidentiality laws. *Id.* at 1391.

The Ninth Circuit has also applied the Restatement of Foreign Relations Law (3d) balancing test, but it has modified the test to incorporate the conflict of interest laws already established in its venue. *Richmark Corp. v. Timber Falling Consultants*, 959 F. 2d 1468 (9th Cir. 1992). In *Richmark*, the plaintiff, attempting to enforce its judgment against the defendant, sought discovery regarding the defendant's assets. The defendant refused to disclose the requested information on the grounds that disclosure would violate the People's Republic of China's privacy laws. As a result, the trial court held the defendant in contempt of court. The appellate court applied the balancing test suggested by the Restatement of Foreign Relations (3d), but it also included its own established conflict of interest policies. Applying this modified test, the court found that the interests expressed by the People's Republic of China were outweighed by those of the U.S. to allow enforcement of U.S. judgments. *Id.* at 27.

The Supreme Court of Texas approached this issue when it was asked to review a state trial court's order compelling a realtor to produce a corporate phone book, containing the names and addresses of foreign nationals. *Volkswagen, AG, Realtor v. The Honorable Rogelio Valdez*, 909 S.W. 2d 900, 39 Tex. Super. J. 114 (1995). The Texas Supreme Court reversed the trial court's ruling, finding that the trial court did not properly apply the test set forth in the Restatement of Foreign Relations Law (3d). The Texas Supreme Court held that the lower court failed to balance the interests of the foreign sovereign with those of the real parties, and that the trial court abused its discretion in rejecting consideration of German law.

In *Salerno v. Lecia*, 1999 LEXIS 7169 (W.D.N.Y., 1999), the U.S. District Court for the Western District of New York applied a balance test similar to that of the Restatement of Foreign Relations Law (3d) test when it was asked, in an employment discrimination case, to determine whether the defendant should be compelled to disclose the terms of the severance packages it offered to its employees who were European nationals. Denying the plaintiff's motion to compel, the court first ruled that the plaintiff was precluded from requesting the documents based on the doctrine of collateral estoppel. But the court also reviewed the question of whether the documents were protected by European privacy laws. In reaching its decision, the court considered both the German BDSG and the European Directive and concluded that deference to both laws was proper: the severance documents were protected and not subject to discovery.

In *In Re Vitamin Antitrust Litigation*, 2001 LEXIS 11536 (2001), the U.S. District Court for the District of Columbia was asked to rule on this issue pertaining to a motion for a protective order to bar discovery of personal data protected by the German BDSG. The defendants had sought to protect the requested information under the Hague Convention, as well as Swiss and German privacy laws. Applying the Restatement of Foreign Relations Law (3d) balancing test, the court found that the requested discovery was not so intrusive that it affronted the national sovereign interests of Germany and did not warrant Hague intervention. The court also held that the German corporation failed to make a persuasive showing that the requested information was solely in data files so that it fell within Germany's BDSG coverage. The court, therefore, ruled that the defendant must comply with the Federal Rules of Civil Procedure in responding to the request for production of documents.

This last example appears to be an exception to the emerging trend that courts will defer to the protections of the foreign privacy laws in matters involving private entities if the private interests are outweighed by the interests of the foreign country to protect its citizens. On the other hand, courts thus far have drawn the line when a case involves the U.S. government. In these federal criminal cases, courts have found that the interests of the U.S. government outweigh the interests of the foreign entity. This distinction should be carefully considered by counsel defending corporations in civil matters with the potential for international discovery.

Road Map for Use of Foreign Privacy Laws as a Tool in Discovery

When defending a corporation that is exposed to civil discovery of data or information outside of the U.S., counsel should not assume that an established corporate discovery policy takes foreign privacy law into consideration. Counsel should, instead, pay special attention to the discovery requests and communicate closely with the client to develop a response strategy.

Know the Privacy Law of the foreign country that is the situs of information subject to discovery

Upon receiving a discovery request for documents or information in a foreign country,

counsel should first determine whether the foreign country's laws protect the privacy of its citizens. As the cases above illustrate, these laws can be found in a variety of areas of a particular country's statutes. The law may be part of the country's civil procedure law and/or criminal code. Or the law might pertain only to privacy in banking. It is important to know and understand the country's privacy law, even if the law does not apply to the information that is requested in a particular matter. Because of the potential for significant penalties imparted on violators of foreign privacy laws, counsel should ensure that a client is fully informed about applicable law and understands the potential repercussions.

Consider Foreign Privacy Law as a tool to limit discovery

Sophisticated plaintiffs' attorneys too often use civil discovery to gain an advantage over a corporate defendant. Plaintiffs will submit overly broad requests that ask for documents that far exceed the scope of a particular case, that are not relevant and that will impose an enormous burden on a defendant to produce. Upon a defendant's failure or refusal to produce all of the requested documents, plaintiffs often seek discovery sanctions, which, if granted, place the plaintiff in a very powerful negotiating position.

If a plaintiff, as part of this discovery tactic, requests information that is potentially protected by a foreign privacy law, defense counsel should carefully consider whether that law may be used to limit such overly broad discovery. Armed with a sound knowledge of applicable foreign privacy law and the emerging trend of U.S. courts in this area, defense counsel will be better able to take steps to demand that the plaintiff's counsel limit the foreign discovery requests at issue. These steps should include a motion for protective order, citing applicable foreign privacy law that asks the domestic court to preclude plaintiff from discovering the requested information. In some cases, the threat of or entry of such a protective order coupled with plaintiff's counsel's inability to finance a prolonged discovery battle may even lead to a favorable resolution of the case.

Defense counsel should file a timely motion for a protective order under Fed. R. Civ. P. 26(c) or equivalent state law. The motion should focus on the Restatement Third of Foreign Relations Law, as well as the cases described above. Moreover, to show that the foreign state's interest outweighs the plaintiff's interest, defense counsel should consider including an affidavit from a representative of the defendant corporation or the corporation's foreign employees whose privacy will be impacted by the discovery. Defense counsel should also consider consulting with and obtaining an affidavit from a law professor or governmental official from the foreign country that is the situs of the requested information and who can provide the domestic court with additional guidance on the meaning and effect of applicable foreign privacy law.

If the motion is filed in federal court, the moving party must also consider Fed. R. Civ. P. 44.1. That rule provides, "[a] party who intends to raise an issue about a foreign country's law must give notice by a pleading or other writing. In determining foreign law, the court may consider any relevant material or source, including testimony, whether or not submitted by a party or admissible under the Federal Rules of Evidence. The court's determination must be treated as a ruling on a question of law."

Conclusion

Many foreign countries have enacted privacy laws to protect their citizens from improper dissemination of personal data and information, including, but not limited to, name, address, phone number, email address, resume, and income. The potential impact of these laws, which may greatly limit the type and amount of foreign discovery a defendant in a U.S. civil case may be required to disclose, should be carefully considered in cases involving defendant corporations with operations and information beyond the U.S.

Thus far, U.S. courts interpreting these foreign privacy laws have ruled somewhat inconsistently, although a trend appears to be emerging. The rulings in criminal cases seem to favor disclosure of information sought by the U.S. government. However, in civil matters, the trend points to enforcement of foreign privacy laws, because courts have found that the foreign sovereign's interests outweigh the interests of a private entity. This trend should be carefully considered by defendants faced with discovery requests for data and information located outside of the U.S. FD