PAPER:

THE EU DATA PROTECTION DIRECTIVE AND MAJOR FACTORS RELIED UPON BY U. S. COURTS IN TRANSBORDER DISCOVERY REQUESTS

By **Daniel W. Perry,** Esq.

Some lawyers mistakenly conclude that the European Union Data Protection Directive[1] is a burden on the transborder discovery of electronically stored information (ESI). The Data Protection Directive does not, in fact, place a burden on the discovery of ESI. It simply mandates that EU member states enact legislation in harmony with the Directive. Lawyers must, instead, focus upon the individual legislation, policies, and procedures of the EU member states. Finally, lawyers need to understand the factors relied upon by United States courts in applying the United States Federal Rules of Civil Procedure and The Hague Convention Rules in transborder discovery requests.[2]

This short paper has a very narrow focus, and does not cover the ground in great detail, but aims to provide a short, high-level introduction to the factors that US courts will consider when assessing transborder discovery requests.

An outline of the EU Directive and UK law

The Data Protection Directive requires that EU member state legislation exempt transborder data transfers from data protection laws, as provided in Article 26(1)(d):

> (d) the transfer is necessary or legally required on important public interest grounds, or for the establishment, exercise or defence of legal claims

In the United Kingdom, Article 26(1)(d) of the Data Protection Directive is implemented by paragraph 5 of Schedule 4 of the Data Protection Act 1998:

> The transfer—
> (a) is necessary for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),
> (b) is necessary for the purpose of obtaining legal advice, or
> (c) is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

In addition, the Data Protection Act of 1998 exempts

[1] *Directive 95/46/EC 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, OJ L281, 23.11.95, p. 31.*

[2] *Two relatively up-to-date sources that will lead the reader to further relevant discussions include Erica M. Davilla, 'International E-Discovery: Navigating the Maze', 8 PGH. J. Tech. L. & Pol' y. 5 (There is one concern with respect to this article: paragraph 19 suggests that, using a double negative: 'These holdings, combined with the Data Protection Directive's finding that personal data includes e-mail, [see footnote] raise some serious concerns about whether international law will prohibit discovery of foreign e-mail in United States litigation in the future.' (footnote) n23 Article 29 Data Protection Working Party, Opinion 8/2001 on the Processing of Personal Data in the Employment Context, at 24, 5062/01/EN/Final WP 48 (Sept. 13, 2001) (concluding that '[t]here should no longer be any doubt that data protection requirements apply to the monitoring and surveillance of workers whether in terms of email use, internet access, video cameras or location data'). It seems that Ms. Davilla is confusing the issues. The issue of whether data protection prohibits e-mail surveillance is a different issue from whether those e-mails should be disclosed as ESI.), and David W. Ogden and Sarah Rapaway, 'General Commentary, Discovery in Transnational Litigation' in John Fellas, general editor, Transnational Litigation: A Practitioner's Guide (Oxford University Press, New York, 2008).*

transborder data transfers, as set out in section 35:

> Disclosures required by law or made in connection with legal proceedings etc
> (1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.
> (2) Personal data are exempt from the non-disclosure provisions where the disclosure is necessary—
> (a) for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings), or
> (b) for the purpose of obtaining legal advice, or is otherwise necessary for the purposes of establishing, exercising or defending legal rights.

Personal data is also exempt in the case of legal professional privilege, as provided for in Schedule 7, paragraph 10:

> Personal data are exempt from the subject information provisions if the data consist of information in respect of which a claim to legal professional privilege or, in Scotland, to confidentiality as between client and professional legal adviser, could be maintained in legal proceedings.

How U.S. courts apply U.S. Federal Rules of Procedure

United States courts will apply the Federal Rules of Procedure rather than Hague Convention Rules where the court has analyzed the importance of the discovery requests; weighed the United States' interest in enforcement of its own laws; analyzed the effectiveness of Hague Convention Rules and Procedures, and weighed these interests against the burden and intrusiveness of the discovery requests on foreign defendants.

In the case of *In re Vitamins Antitrust Litigation*,[3] the United States Federal District Court upheld a Special Master's rejection of a claim by German and Swiss defendants that discovery would violate German and Swiss privacy laws. The court found disclosure was warranted, because of a compelling United States interest in the enforcement of its antitrust statutes. The court agreed that disclosure of information protected by the German Federal Data Protection Act would be warranted if the information is necessary to protect public interests or the interests of the plaintiffs, or both, and the data subjects have no legitimate interest in preventing disclosure. The court acknowledged that by compelling disclosure, it may implicate 'legitimate privacy law concerns' and possible criminal liability in Germany. Since the discovery was a small subset of a larger discovery request, the court allowed the defendants to file a preliminary privacy log detailing which information that would be covered by the German and Swiss privacy laws. The court directed the plaintiffs to determine whether such information was essential and whether to amend a protective order to safeguard the defendants from liability.

Summary of factors relied upon by United States courts in compelling disclosure

In the 2008 United States case of *Strauss v. Credit Lyonnais, S.A.*,[4] the Federal Eastern District Court of New York considered transnational discovery sought by the heirs of victims of terrorist attacks from the defendant French bank Credit Lyonnais, alleging that the bank provided material support to the terrorists. The defendants filed a motion for protective orders, requesting that the court: compel plaintiffs to seek discovery through the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters; and excuse Credit Lyonnais from providing discovery protected under French bank secrecy laws, a violation of which would be a criminal offense. The court denied the motion for protective orders.

Citing *Societe Nationale Industrielle Aerospatiale v. United States District Court for the Southern District of Iowa*,[5] and Restatement (Third) of Foreign Relations Law of the United States § 442(1)(c), the court in *Strauss* considered five primary factors:

1. the importance to the investigation or litigation of the documents or other information requests;
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
6. the extent to which compliance with the request would undermine the important interests of the state where the information is located.

[3] *2001 U.S. Dist. LEXIS 8904, 2001-2 Trade Cas. (CCH) P73338 (D.D.C. June 20, 2001).*

[4] *242 F.R.D. 199, 68 Fed.R.Serv.3d 72, 2008 U.S. Dist. LEXIS 39428 (E.D.N.Y. Mar. 10, 2008).*

[5] *482 U.S. 522 (1987), 107 S.Ct. 2542, 96 L.Ed.2d 461 (1987).*

The *Strauss* court also considered 'the hardship of compliance on the party or witness from whom discovery is sought and the good faith of the party resisting discovery.'[6]

In the 1987 United States Federal Rules Decision case of *Minpeco, S.A. v. Conticommodity Services, Inc.*,[7] the court identified seven factors relevant to a foreign discovery, and then highlighted four of those as the principal factors:

1. the competing interests of the nations whose laws are in conflict,
2. the hardship of compliance on the party or witness from whom discovery is sought,
3. the importance to the litigation of the information and documents requested, and
4. the good faith of the party resisting discovery.

Two of those factors - the competing national interests of each nation, and the importance to the litigation of the requested discovery - are also identified in the Restatement.

In addition to the four 'principal' factors, the *Minpeco* court also identified three additional factors:

1. the extent to which the required conduct is to take place outside of the United States,
2. the nationality of the entity, and
3. the extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by that state.

A closer look at the factors as applied by the court in *Strauss v. Credit Lyonnais*, S.A.

First, the information requested was crucial to the plaintiffs' claims that Credit Lyonnais provided financial services to terrorist organization for more than thirteen years. Second, the discovery requests were narrowly tailored – the plaintiffs' sought documentation and testimony regarding the relationship between the defendant and terrorist organization, the nature and extent of the services that defendant provided, the collection or distribution of funds by Credit Lyonnais that may have been used by the terrorist organization or its associates or both to support terrorism, and any knowledge that Credit Lyonnais had of their alleged terrorist connections. Third, the majority of the requested discovery originated outside the United States, but Credit Lyonnais could have designated a witness who resided outside France and who could have testified after a review of the relevant records. Fourth, the availability of alternative methods – the plaintiffs did not have direct or ready access to the records of Credit Lyonnais through means other than discovery demands. Credit Lyonnais acknowledged that certain discovery would not be granted under the Hague Convention. Fifth, the mutual interests of the United States and France in combating terrorism favour disclosure and outweighed the French interest, if any, in protecting the disputed discovery. The interests of the United States and France in combating terrorist financing, as evidenced by the legislative history of the US Antiterrorism Act, Presidential Executive Orders, and both countries' participation in international treaties and task forces aimed at disrupting terrorist financing, outweighed the French interest in bank secrecy laws and its generally-asserted interest in sovereignty. Despite numerous and ample opportunities to do so, the French Ministry of Justice never specifically objected to the plaintiffs' discovery demands. The United States also has a substantial interest in fully and fairly adjudicating matters before its courts. In addition, Credit Lyonnais was not likely to face substantial hardship by complying with the plaintiffs' requests. If the objecting litigant is a party to the action, as was Credit Lyonnais, courts accord that party's hardship less weight. Credit Lyonnais' potential hardship was reduced further, since the parties were bound by previously issued protective orders that forbade them from publicly disclosing any sensitive information produced to them. Finally, Credit Lyonnais only made 'good faith and diligent efforts' to secure discovery after court orders were issued.

The lessons of *Strauss v. Credit Lyonnais*, S.A.

First, that US courts will broadly support transborder discovery in terrorism, taxation, and securities or financial fraud cases, and will broadly construe the relevance of the requested discovery, rewarding efforts to tailor clear and not too onerous discovery requests. In addition, US judges will expect some reasonable and early efforts at document preservation, review, and production by foreign discovery custodians. In contrast, a court will minimize most claims of hardship, particularly when a requested discovery is digital in format or physical copies exist in various jurisdictions.

US courts will apply US Federal Rules of Procedure in

[6] *Reino De Espana v. American Bureau of Shipping, No. 03 Civ. 3573, 2005 U.S. Dist. LEXIS 15685, 2005 WL 1813017 (S.D.N.Y. Aug. 1, 2005), 2005 A.M.C. 2257.*

[7] *116 F.R.D. 517, 523 (S.D.N.Y. 1987), 8 Fed.R.Serv.3d 1121.*

the absence of a clearly superior or expedient alternative under the Hague Convention. Great weight will be given to US interests, and judges will strive to find similar or arguably equivalent foreign interests, minimizing a generalized invocation of a foreign country's sovereignty or data protection laws, although rewarding specific objections by the foreign country's data protection authorities that are directed to specific items of requested discovery. In addition, US courts will readily fashion confidentiality orders to minimize claims that disclosure will violate a foreign county's privacy or secrecy laws.

Finally, it is interesting to note that US courts are starting to invoke a broad and substantial interest in fully and fairly adjudicating matters before its courts.

Daniel W. Perry, Attorney, former judge, is a U.S. Civil-Law Notary dealing with digital evidence and discovery, international computer contracts and technology agreements and General Counsel to Identity Commons, Inc., an organization for collaborating in digital identity metasystems. He frequently speaks and writes on computer law, data protection and privacy issues.

dan@danielperry.com.

