2009

The U.S. Discovery-EU Privacy Directive Conflict: Constructing a Three-Tiered Compliance Strategy

Carla L. Reyes
Southern Methodist University, Dedman School of Law

Author ORCID Identifier:

https://orcid.org/0000-0002-2448-8309

THE U.S. DISCOVERY-EU PRIVACY DIRECTIVE CONFLICT: CONSTRUCTING A THREE-TIERED COMPLIANCE STRATEGY

CARLA L. REYES*

INTRODUCTION

Because of the different regulatory approaches of the United States and the European Union, litigants involved in U.S.-EU trans-border litigation face a difficult situation regarding discovery. U.S. discovery procedures require litigants to produce any requested information under their control without regard to whether the information originated within U.S. borders.[1] Meanwhile, the European Union prohibits the transfer of data originating within its borders to the United States because it has determined that the United States lacks adequate data protection standards.[2] The steady increase of trans-border litigation has brought the conflict between U.S. discovery rules and EU data protection laws into sharp focus and spurred intense debate.

Despite calls from EU member states' data protection authorities for the Article 29 Working Party ("Working Party") to comment on the issue,[3] the lead EU administrative data protection body has remained silent. In the absence of such guidance from the Working Party, litigants in U.S.-EU trans-border disputes are left floundering in their attempts to comply with U.S. discovery rules without violating EU data protection law. This note sifts through the quagmire of regulations to help trans-border litigants view the U.S. discovery-EU

---

* Candidate for the degrees of J.D. and LL.M in International and Comparative Law, Duke University School of Law, and MPP, Duke University Terry Sanford Institute of Public Policy. I would like to thank Joseph Cutler of Perkins Coie, LLP, for his insight and guidance during the drafting of this piece.

1. *See* FED. R. CIV. P. 26.

2. *See infra* notes 11-12 and accompanying text.

3. Alan Charles Raul & Edward McNicholas, *French CNIL Examines Data Protection Issues Linked to U.S. Litigation Disclosures*, 3 PRIV. & DATA SEC. L.J. 358, 358, 361 *2008) (describing the French Data Protection Authority ("CNIL") analysis of the problem and the French push to put the issue on the Working Party's agenda).

data protection conflict through a transnational legal lens, and thereby, construct a strategy for compliance that respects U.S., EU and international law.

This note proceeds in three parts. Part I describes the nature and scope of the U.S. discovery-EU Privacy Directive conflict and investigates its roots in the larger differences between civil and common legal systems' approach to evidence gathering. Part II examines possible solutions to the legal quandary posed by the conflicting requirements, and Part III constructs the best possible compliance strategy for real world litigants.

I. UNDERSTANDING THE CURRENT CONFLICT AND ITS HISTORICAL ROOTS

Litigants in U.S. courts face strict penalties for failure to comply with the discovery process.[4] When data involved in the discovery process is located or originated in the European Union, these same litigants face strict penalties under EU data protection law for transferring the data to the United States.[5] This places litigants in U.S.-EU trans-border disputes in a difficult position. The conflict between the two sets of requirements has been a recent source of heated debate,[6] fueled, in part, by the long-standing disagreement between civil and common legal systems over the appropriate nature of evidence-gathering procedures.

A. The Conflict: EU data protection law confronts U.S. discovery rules.

The European Union began harmonizing the data protection laws of its member states with the adoption of Directive 95/46/EC ("Privacy Directive").[7] The Privacy Directive restricts the transfer

4. *See* Fed. R. Civ. P. 37.

5. For example, the French Data Protection Authority (CNIL) fined Tyco Healthcare € 30,000 (approximately $40,350) for violations of its data protection law. CNIL, La CNIL condamne la société Tyco Healthcare France à 30,000 euros d'amende pour manque de coopération et de transparence (May 31, 2007), http://www.cnil.fr/index.php?id=2206&news[cur]=6&news[uid]=440&cHash=20af941343 [hereinafter CNIL, Tyco].

6. *See* CNIL, Discovery Case: Another Sensitive Issue, www.cnil.fr/index.php?2464 (describing France's concern over the growing conflict between U.S. discovery rules and the privacy of personal data); Michael B. de Leeuw & Phillip A. Wellner, *What to do About Data in the EU?*, N.Y. L.J., May 23, 2008 (detailing the difficulties for EU-U.S. trans-border litigants).

7. Council Directive 95/46, on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, 1995 O.J. (L 281) 31 [hereinafter Privacy Directive]. The Privacy Directive creates an administrative data protection authority for

and processing of "personal data," which is broadly defined as "any information relating to an identified or identifiable natural person."[8] Privacy Directive Article 25 forbids the transfer of personal data to a third country unless the third country provides an adequate level of data protection.[9] Furthermore, if a specific third country is found to lack adequate data protection, EU member states are required to take affirmative steps to prevent the transfer of personal data to that country.[10] The EU position is that the United States lacks adequate data protection standards.[11] As a result, the United States and the European Union negotiated a safe harbor mechanism by which companies may voluntarily increase their level of data protection and become eligible for data transfers from the European Union.[12] The safe harbor, however, does not cover all sectors of data,[13] and, while specifically designed to govern data transfers, it also imposes

---

the entire European Union, the Article 29 Data Protection Working Party ("Working Party"). *See id.* art. 29 (creating the Working Party). *See also id.* arts. 30-31 (detailing the Working Party's responsibilities). As part of its mandate, the Working Party issues opinions and interpretations of the Privacy Directive and its application. The opinions and recommendations of the Working Party are not binding on EU member states. Joseph Cutler & Carla L. Reyes, *Was That Your Computer Talking to Me? The EU and IP Addresses as "Personal Data"*, CYBERSPACE Law., Aug. 2008, at 1, 5 (correction printed in Note from the Editor, CYBERSPACE LAW., Nov. 2008, at 2, 3). Nonetheless, "the Working Party opinions are often adopted by Members States and influence EU policy making in the privacy field." *Id.*

8. Privacy Directive, *supra* note 7, art. 2(a). Furthermore, "an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identification number or . . . one or more factors specific to his physical, physiological, mental, economic, cultural or social identity." *Id.* Thus, to qualify as personal data, the Working Party requires that the data fit within each of the following criteria: (1) any information, (2) relating to, (3) an identified or identifiable, (4) natural person. Article 29 Data Protection Working Party [hereinafter Working Party], *Opinion 4/2007 on the Concept of Personal Data*, at 6, 01248/07/EN, WP 136 (June 20, 2007) [hereinafter WP 136] (detailing the specific requirements for meeting each of the four criteria).

9. Privacy Directive, *supra* note 7, art. 25(1).

10. *Id.* art. 25(4).

11. Working Party, *Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT)*, at 21, 01935/06/EN, WP 128 (Nov. 22, 2006) [hereinafter WP 128].

12. U.S. Dep't of Commerce, Safe Harbor Privacy Principles (July 21, 2000), www.export.gov/safeharbor/SH_Privacy.asp [hereinafter Safe Harbor Principles].

13. *Id.* at pmbl. (defining "personal data" as "data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form").

restrictions on data processing which render the use of the Safe Harbor framework problematic in the U.S. discovery context.[14]

The Privacy Directive also places a variety of restrictions on the processing of personal data. For example, Privacy Directive Article 6 requires personal data to "be processed fairly and lawfully[,]. . .be collected for specified, explicit and legitimate purposes, and not be used for incompatible purposes."[15] Furthermore, "the processed data must be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed."[16] Additionally, data subjects must have the opportunity to correct erroneous data,[17] and personal data may not be retained longer than necessary.[18]

The Privacy Directive restrictions on transfers and processing of personal data pose a problem for litigants involved in U.S.-EU trans-border litigation. First, the Privacy Directive transfer provisions restrict the scope of discoverable data. Second, because "processing" is defined as the "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" of personal data,[19] the processing requirements apply to "virtually any action that a U.S. litigator would take" in preparation for trial.[20]

Thus, parties to U.S.-EU trans-border litigation may not be able to comply with U.S. discovery requirements without violating EU data protection law. However, full compliance with the Privacy Directive may require refusal to comply with a U.S. discovery request. Notably, entities subject to the Privacy Directive face strict monetary penalties for any violation,[21] and failure to comply with U.S.

---

14. *See generally* Safe Harbor Principles, *supra* note 12 (detailing requirements for onward transfers to be lawfully made and imposing restrictions on how that data can be further processed).

15. Working Party, *Opinion 1/2006 on the Application of EU Data Protection rules to Internal Whistleblowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking and Financial Crime*, at 9, 00195/06/EN, WP 117 (Feb. 1, 2006) [hereinafter WP 117] (citing Privacy Directive, *supra* note 7, art. 6).

16. *Id.*

17. *Id.* at 14.

18. *Id.* at 12.

19. Privacy Directive, *supra* note 7, art. 2(b).

20. Leeuw & Wellner, *supra* note 6.

21. For example, the Italian data protection authority fined GS, a supermarket chain, 54,000 euros for violations of the Italian legislation implementing the Privacy Directive.

discovery requests can result in "severe sanctions, including contempt proceedings, monetary fines, prosecution for obstruction of justice, prejudicial jury instructions, and dismissal of claims."[22] Litigants are therefore left to decide which set of laws to violate – EU data protection or U.S. discovery.

B. The U.S. discovery-EU Privacy Directive conflict is part of a larger disjunction between common and civil legal approaches to evidence gathering.

The tension between EU data protection law and U.S. discovery rules presents a new manifestation of an enduring conflict between civil and common law evidence-gathering procedures. The differences in common and civil legal systems with regard to evidence gathering have been the source of tension for decades. At its core, the disagreement centers not on the goals of evidence gathering, but on the mechanism for achieving those goals.

The United States, a common law jurisdiction, employs an evidence-gathering procedure referred to as pre-trial discovery.[23] Pre-trial discovery is the gathering of evidence after a lawsuit is filed but prior to trial.[24] The United States adopted pre-trial discovery procedures to encourage the free flow of information, truth-finding, and informational equity between parties.[25] Specifically, the pre-trial discovery rules embodied in the Federal Rules of Civil Procedure[26] allow litigants to obtain any information relevant to the claim or defense of a party.[27] To be discoverable, information need not be admissible at trial; it must only be relevant and reasonably calculated to lead to the discovery of admissible evidence.[28] Notably, the scope

---

ADDLESHAW GODDARD, DATA AND INFORMATION UPDATE 14 (2008), http://www.addleshawgoddard.com/asset_store/document/data_information_update_summer_08_101528.pdf. In France, CNIL has also fined companies. *See* CNIL, Tyco, *supra* note 5.

22. Stanley W. Crosley, Alan Charles Raul, Edward R. McNicholas & Julie M. Dwyer, *A Path to Resolving European Data Protection Concerns with U.S. Discovery*, 6 BNA PRIVACY & SEC. L. REP. 1, 2 (2007), *available at* http://www.sidley.com/files/Publication/7ed26a68-1ec7-44eb-9db6-3660d938f575/Presentation/PublicationAttachment/166eaabb-2a74-43fe-8a963d78194ec198/EuroDataProtection.pdf.

23. Stephen F. Black, *United States Transnational Discovery: The Rise and Fall of the Hague Evidence Convention*, 40 INT'L & COMP. L. Q. 901, 902 (1991).

24. *See, e.g., id.* at 902-03.

25. *Id.*

26. *See* FED. R. CIV. P. 26-37.

27. *Id.* R. 26(b)(1).

28. *Id.*

of information potentially covered by the discovery rules is extremely broad, and it is the parties themselves that gather the evidence.[29] These two aspects of the discovery process give rise to most of the objections raised by civil law countries, which view the scope of U.S. discovery as intrusive and the identity of the fact-finder inappropriate.[30]

Civil law countries also seek to promote justice through rules of civil procedure, but they do so in an entirely different fashion. First, most civil law countries view evidence gathering as a sovereign function best carried out by an active judge.[31] Typically, in civil systems "the judge questions the witnesses and decides which documents to request."[32] Because of this active role, the scope of discovery is naturally limited in civil law systems by the discretion of the judge, and foreign litigators often view the U.S. discovery process, placed in the hands of the parties, "as fostering 'fishing expeditions' by U.S. lawyers eager to build a case and perhaps impose costs on their adversaries."[33] Some countries, such as France, so vehemently oppose the U.S. discovery model that they enacted statutes specifically designed to block the application of U.S. discovery rules to their citizens.[34]

Given the historical tension between U.S. discovery rules and European approaches to evidence gathering, it is unsurprising that U.S. discovery rules conflict with EU data protection law, since it is another area where the European Union views U.S. regulation as inadequate. After all, given the general distaste in civil legal systems for U.S. discovery procedures, it is only natural that in an area viewed as a fundamental human right, such as data privacy, the conflict would increasingly grow. The question then becomes not how to

---

29. *See id.* R. 26(a) (describing duty of one party to disclose to the others); *id.* R. 26(b)(1) (detailing the scope of discoverable information).

30. ANTITRUST LAW SECTION OF THE AM. BAR ASS'N, OBTAINING DISCOVERY ABROAD 1-2 (2d ed. 2005).

31. *Id.* at 1. *See also* Harold G. Maier, *Extraterritorial Discovery: Cooperation, Coercion and the Hague Evidence Convention*, 19 VAND. J. TRANSNT'L L. 239, 242-43 (1986).

32. ANTITRUST LAW SECTION OF THE AM. BAR ASS'N, *supra* note 30, at 1.

33. *Id.* at 3.

34. For France's blocking statute, see Law No. 80-538 of July 16, 1980, Journal Officiel de la République Française [J.O.] [Official Gazette of France], July 17, 1980, p. 1799. Switzerland and the United Kingdom also have blocking statutes. For Switzerland's blocking statute, see Strafgesetzbuch [StGB] [Criminal Code] Nov. 8, 1934, art. 271. For the blocking statute of the United Kingdom, see British Protection of Trading Secrets Act, 1980, c. 11. For further discussion of blocking statutes, see generally ANTITRUST LAW SECTION OF THE AM. BAR ASS'N, *supra* note 30.

eliminate the tension, but whether litigants can navigate both sets of laws without incurring penalties.

II. POSSIBLE SOLUTIONS TO THE U.S.-EU TRANS-BORDER LITIGANT'S LEGAL QUANDARY

A litigant involved in a U.S.-EU trans-border dispute may generally seek to comply with both U.S. discovery rules and the Privacy Directive by either persuading U.S. courts to accept restricted discovery production or using exceptions to the Privacy Directive to fully comply with U.S. discovery rules. A litigant seeking to persuade U.S. courts to accept restricted production may seek to either substitute the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters ("Hague Evidence Convention") procedures for the Federal Rules of Civil Procedure, or obtain a protective order on the basis of EU data protection laws. On the other hand, a litigant using Privacy Directive exceptions to fully comply with U.S. discovery requirements must both use exceptions to the Privacy Directive's transfer provisions to remove restrictions on the scope of discovery and justify processing of lawfully transferred data under Privacy Directive Article 7.

Solution A: Persuade U.S. courts to accept restricted discovery production.

A litigant in a U.S.-EU trans-border dispute generally has two options for persuading U.S. courts to accept restricted discovery production. First, the litigant may argue that the Hague Evidence Convention governs the dispute rather than the Federal Rules of Civil Procedure.[35] Alternatively, the litigant may seek a protective order on the basis that full discovery will expose the litigant to sanctions in the European Union.[36] Notably, the first strategy has not yet been used by a litigant in the specific context of the U.S. discovery-EU Privacy Directive conflict. The second strategy of seeking a protective order, however, has been successfully employed by litigants in this context.[37]

35. *See infra* notes 54-60 and accompanying text.
36. *See infra* notes 70-78 and accompanying text.
37. *See infra* notes 90-98 and accompanying text.

Option 1: Persuade the court to use the Hague Evidence Convention instead of the Federal Rules of Civil Procedure.

Although this option has not yet been pursued by litigants in this context, a litigant could overcome the U.S. discovery-EU Privacy Directive conflict by persuading the court to use the Hauge Evidence Convention instead of the Federal Rules of Civil Procedure. The Hague Evidence Convention, concluded on March 18, 1970,[38] sought to bridge the gap between evidence gathering procedures in civil and common law countries by providing three mechanisms to be used in either system: letters of request, diplomatic or consular officers, and appointed commissioners.[39]

The most helpful of these procedures for dealing with a conflict between the Privacy Directive and U.S. discovery rules is the letter of request. A letter of request is a formal procedure whereby the court presiding over a civil or commercial judicial proceeding in one country can ask the judicial authority of another country to gather evidence for use in the judicial proceeding in the requesting state.[40] Each country that ratified the Hague Evidence Convention designated a central authority to which all letters of request are sent for execution.[41] A letter of request must be executed expeditiously[42] and may only be refused in specific cases.[43] However, the person or persons from whom the executing country must gather the evidence

38. Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, 847 U.N.T.S. 231 [hereinafter Hague Evidence Convention].

39. *Id.* chs. I, II.

40. Hague Conference on Private International Law, *Outline of the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in civil or Commercial Matters* (2008), http://hcch.e-vision.nl/upload/outline20e.pdf [hereinafter HCCH, *Outline of the Hague Evidence Convention*].

41. *See* Hague Evidence Convention, *supra* note 38, art. 2.

42. In order to cut down on the time required to execute a letter of request, the European Union issued Council Regulation 1206/2001, Cooperation Between the Courts of the Member States in Taking of Evidence in Civil or Commercial Matters, 2001 O.J. (L174) 1, 2 [hereinafter Evidence Regulation]. The Evidence Regulation replaces the Hague Evidence Convention as between EU member states and streamlines the process in order to reduce the time necessary for gathering evidence when litigation involves parties in multiple EU member states. *Id.*

43. HCCH, *Outline of the Hague Evidence Convention*, *supra* note 40, at 1. A letter of request can only be refused in its entirety if execution is not within the function of the judiciary or execution would threaten the country's sovereignty or security. *See* Hague Evidence Convention, *supra* note 38, art. 12. A letter of request cannot be refused in its entirety solely because the requested country would not recognize the underlying legal claim or because the country asserts it has exclusive jurisdiction over the subject matter. *Id.*

"may refuse to give evidence in so far as he has a privilege or duty to refuse to give the evidence... under the law of the State of execution."[44]

Hague Evidence Convention letters of request can allow litigants to fulfill U.S. discovery requirements while simultaneously complying with the Privacy Directive in one of two ways: lawfully producing only non-personal data, or fully producing all relevant information, including personal data, pursuant to an order of an EU Member State judicial authority.

First, if the litigant facing an evidence request from an EU Hague Evidence Convention executing authority successfully shows that compliance would require the production of personal data in violation of the Privacy Directive, the EU executing authority may rely on Article 11 of the Hague Evidence Convention and excuse production.[45] It appears that as long as the letter of request is executed to the fullest extent under the executing country's domestic law, U.S. discovery requirements implemented via the Hague Evidence Convention are fulfilled without violating the Privacy Directive.

Alternatively, if the EU executing country could be persuaded that the personal data sought is vital to establishing a legal claim or defense, the executing judicial authority could lawfully order full compliance with the letter of request despite the Privacy Directive's transfer and processing restrictions. The Privacy Directive allows transfer of personal data to an entity in a third country lacking adequate data protection standards if "the transfer is necessary... for the establishment, exercise or defense of legal claims."[46] Additionally, processing of personal data is legitimate if it "is necessary for a legal obligation to which a data controller is subject."[47] Notably, the legal obligation must be one imposed by an EU member state.[48] If a

---

44. Hague Evidence Convention, *supra* note 38, art. 11.

45. Article 11 of the Hague Evidence Convention states that "[i]n the execution of a Letter of Request the person concerned may refuse to give evidence in so far as he has a privilege or duty to refuse to give the evidence under the law of the State of execution." *Id.*

46. Privacy Directive, *supra* note 7, art. 26(1)(d).

47. *Id.* art. 7(c).

48. *See* WP 117, *supra* note 15, at 8 ("[A]n obligation imposed by a foreign legal statute or regulation... may not qualify as a legal obligation by virtue of which data processing in the EU would be made legitimate."). *See also* WP 128, *supra* note 11, at 18 (confirming that foreign legal obligations do not satisfy Article 7(c) because "[a]ny other interpretation would make it easy for foreign rules to circumvent the EU rules laid down in the Directive").

European judicial authority required production of personal data pursuant to a letter of request, the resulting transfer would be for the establishment or defense of legal claims and any processing would therefore be for compliance with a legal obligation imposed on the data controller. Under such circumstances, any processing must also comply with Privacy Directive requirements that personal data be processed fairly and lawfully,[49] that it be used only for the purposes for which it was received,[50] and that no data regarding a person's racial or ethnic origins, political opinions, religious beliefs, trade-union membership, health, or sex life be processed.[51]

Each of these alternatives requires persuading a U.S. court to use the Hague Evidence Convention procedures rather than the Federal Rules of Civil Procedure. Because the United States ratified the Hague Evidence Convention, the Supreme Court has long held that "both the discovery rules set forth in the Federal Rules of Civil Procedure and the Hague [Evidence] Convention are the law of the United States."[52] However, the Hague Evidence Convention was meant as "a supplement, not a pre-emptive replacement, for other means of obtaining evidence located abroad."[53] As such, the Hague Evidence Convention will not automatically apply in trans-border litigation, and a party must persuade the court to use letters of request instead of the Federal Rules of Civil Procedure.[54] In analyzing a party's motion to use the Hague Evidence Convention in a trans-border dispute, courts use a three-part test to examine: first, "the particular facts of the case, particularly with regard to the nature of the discovery requested,"[55] second, "the sovereign interests in issue, and,"[56] third, "the likelihood that the Convention procedures will

49. Privacy Directive, *supra* note 7, art. 6(a).

50. *Id.* art. 6(b).

51. *Id.* art. 8. At this juncture, it is important to note that Privacy Directive Article 8 provides three exceptions to its prohibition of processing sensitive data that would allow such processing during a lawsuit: (1) the data subject has given his specific consent, (2) "processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law insofar as it is authorized by national law providing for adequate safeguards," and (3) "the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims." *Id.* art. 8(2)(a), 8(2)(b), 8(2)(e).

52. Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for the S. Dist. of Iowa, 482 U.S. 522, 533 (1987).

53. *Id.* at 536.

54. *See id.* at 533-40.

55. *In re* Perrier Bottled Water Litig., 138 F.R.D. 348, 354 (D. Conn. 1991).

56. *Id.*

prove effective."[57] The party moving to substitute the Hague Evidence Convention for the Federal Rules of Civil Procedure bears the burden of persuasion.[58]

Under the first prong, which requires an examination of the nature of the discovery requested, courts will favor the Hague Evidence Convention procedures when the discovery calls for broad responses rather than being narrowly tailored.[59] This result stems from the Supreme Court's requirement that, because of foreign litigants' unfamiliarity with U.S. discovery procedures, "American courts, in supervising pretrial proceedings, [must] exercise special viligance [sic] to protect foreign litigants from the danger that unnecessary, or unduly burdensome, discovery may place them in a disadvantageous position."[60]

Under the second prong, "the appropriate inquiry . . . is the 'host' country's amenability to the manner of discovery sought to be utilized by the plaintiffs."[61] To that end, courts consider the domestic law of the host country regarding civil procedure.[62] The second prong will especially favor the Hague Evidence Convention if the host country has directly stated its opposition to U.S. discovery procedures or ratified the Hague Evidence Convention with a strong Article 23 reservation.[63]

---

57. *Id.*

58. *Id.*

59. *Id.* at 354-55.

60. Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Court for the S. Dist. of Iowa, 482 U.S. 522, 546 (1987).

61. *Perrier Bottled Water*, 138 F.R.D. at 355.

62. *See id.*

63. *See id.* (noting that France was the most emphatic critic of U.S. discovery procedure, adopted a blocking statute, ratified the Hague Evidence Convention, and even adopted laws preventing the unauthorized use of procedures other than the Hague Evidence Convention in trans-border disputes).

Article 23 reservations allow state-parties to the Hague Evidence Convention to declare that they will not enforce any pre-trial discovery order. Some countries have stronger Article 23 reservations than others, especially since the Hague Conference on Private International Law cleared up the misunderstanding shared by many countries that "pre-trial" discovery meant discovery prior to the filing of a legal claim. For an example of a strong Article 23 reservation, see that of France, which states:

> In accordance with the provisions of Article 33, the French Government declares: that in pursuance of Article 4, para. 2, it will execute Letters of Request only if they are in French or if they are accompanied by a translation into French; that, in pursuance of Article 23, Letters of Request issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries will not be executed;
>
> ....

Lastly, the third prong will favor the Hague Evidence Convention unless there is a fact specific reason the procedures will be ineffective.[64] An allegation that the Hague Evidence Convention procedures will cause time delays is insufficient to cause the third prong to favor the Federal Rules of Civil Procedure.[65]

Importantly, if the Hague Evidence Convention is used and the U.S. court is not satisfied with the scope of evidence obtained, the court retains the power to order production under the Federal Rules of Civil Procedure.[66] If production is ordered, especially after a European court relied on the Privacy Directive in refusing to fulfill the production requests, compliance would require violating data protection laws of the European Union.

Option 2: Obtain a protective order on the basis of EU data protection law.

When U.S. discovery requests conflict with the law of a foreign nation, U.S. courts sometimes grant a protective order releasing the party from its obligation to produce evidence. The party relying on foreign law bears the burden of showing that foreign law actually bars

---

> The declaration made by the French Republic in accordance with Article 23 relating to Letters of Request issued for the purpose of obtaining pre-trial discovery of documents does not apply when the requested documents are enumerated limitatively in the Letter of Request and have a direct and precise link with the object of the procedure.

Hague Conference on Private International Law, *France's Reservations and Declarations to the Hague Evidence Convention*, http://www.hcch.net/index_en.php?act=status.comment&csid=501&disp=resdn.

For an example of a moderate, and more common, Article 23 reservation, see that of the United Kingdom, which states:

> In accordance with Article 23 Her Majesty's Government declare that the United Kingdom will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents. Her Majesty's Government further declare that Her Majesty's Government understand "Letters of Request issued for the purpose of obtaining pre-trial discovery of documents" for the purposes of the foregoing Declaration as including any Letter of Request which requires a person: (a.) to state what documents relevant to the proceedings to which the Letter of Request relates are, or have been, in his possession, custody or power; or (b.) to produce any documents other than particular documents specified in the Letter of Request as being documents appearing to the requested court to be, or to be likely to be, in his possession, custody or power.

Hague Conference on Private International Law, *United Kingdom's Reservations and Declarations to the Hague Evidence Convention*, http://www.hcch.net/index_en.php?act=status.comment&csid=564&disp=resdn.

64. *Perrier Bottled Water*, 138 F.R.D. at 355-56.

65. *Id.*

66. *Id.* at 356.

production of evidence.[67] That burden is met by "providing the [c]ourt with information of sufficient particularity and specificity to allow the [c]ourt to determine whether the discovery sought is indeed prohibited by foreign law."[68] In meeting this burden, it is helpful to obtain a statement from the foreign country that its law actually bars disclosure of the information.[69]

Even if the party resisting discovery proves a conflict between U.S. and foreign law, the court retains the power to deny the protective order. In deciding how to rule, the court engages in a case-specific analysis of five factors:[70] first, "the importance to the investigation or litigation of the documents or other information requested,"[71] second, "the degree of specificity of the request,"[72] third, whether the information originated in the United States,[73] fourth, the availability of alternative means of securing the information,"[74] and fifth, "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."[75]

The first factor regarding the importance of discovery usually weighs in favor of parties resisting the production of documents that

---

67. Alfadda v. Fenn, 149 F.R.D. 28, 34 (S.D.N.Y. 1993) (citing United States v. Vetco, 691 F.2d 1281, 1289 (9th Cir. 1981)).

68. *Id.*

69. *See* Volkswagen, A.G. v. Valdez, 909 S.W.2d 900, 902 (Tex. 1995) (noting that Germany's amicus brief declaring disclosure would violate the German Data Protection Act made the conflict between the U.S. discovery order and foreign law obvious); *Alfadda*, 149 F.R.D. at 34-35 (finding that the failure of the Swiss government to submit a statement that disclosure of the information at issue threatened their national interests evidenced that no threat existed).

70. Courts have adopted these factors from the *Restatement (Third) of Foreign Relations*. *See Volkswagen*, 909 S.W.2d at 902; Richmark Corp. v. Timber Falling Consultants, 959 F.2d 2468, 1474-75 (1992) (citing Societe Nationale Industrielle Aeropostale v. U.S. Dist. of Iowa, 482 U.S. 522, 544 n.28 (1987) as the key case anticipating the adoption of the *Restatement (Third)* factors by U.S. Courts). *See also Alfadda*, 149 F.R.D. at 34 (relying on a modified version of the *Restatement* factors). The adoption of the *Restatement (Third)* factors is a natural progression from the earlier use of the *Restatement (Second) of Foreign Relations*, upon which the *Restatement (Third)* was built. *See, e.g.*, Laker Airways v. Pan Am. World Airways, 103 F.R.D. 42, 45 (1984); *Vetco*, 691 F.2d at 1288.

71. RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 442(1)(c) (1987).

72. *Id.*

73. *Id.*

74. *Id.*

75. *Id.*

may aid in proving their own claim or defense.[76] When parties resist the production of documents that will hurt their case, this first factor weighs in favor of denying the protective order.[77] Furthermore, "[c]ourts have refused to require production where the documents sought are largely cumulative of records already produced."[78] Under the second factor, the key inquiry is "how burdensome it will be to respond to [the] request."[79] In particular,"[g]eneralized searches for information are discouraged,"[80] and overbroad requests will be disfavored as abusive and overly intrusive.[81] The third factor will usually weigh in favor of granting the protective order when the discoverable material originated in the foreign nation and remains there, beyond the scope of U.S. jurisdiction.[82]

The fourth factor requires courts to "consider whether substantially equivalent alternate means for obtaining the requested information are available."[83] It often causes courts "considerable discomfort to think that a court of law should order a violation of law, particularly on the territory of the sovereign whose law is in question," and courts seek to avoid such orders whenever possible.[84] If a court feels that an alternative means of producing the information

---

76. *See generally* Societe Internationale v. Rogers, 357 U.S. 197, 212-13 (1958) (citing an example where unproduced information may have been helpful to the resisting party's own cause).

77. *See* United States v. Vetco, Inc., 691 F.2d 1281, 1288 (9th Cir. 1981) (relying on the fact that the documents Vetco sought not to produce were relevant to proving their tax liability in determining that the importance of the documents weighed in favor of denying the protective order).

78. Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (1992); *Vetco*, 691 F.2d. at 1290 (using the *Restatement (Second)* factor, "importance of documents," which eventually became the first factor in the *Restatement (Third)* test).

79. *Richmark*, 959 F.2d at 1475.

80. *Id.*

81. *In re* Perrier Bottled Water Litig., 138 F.R.D. 348, 354-55 (D. Conn. 1991).

82. Volkswagen, A.G. v. Valdez, 909 S.W.2d 900, 902-03 (Tex. 1995) (using the fact that the eleven materials sought were in Germany to support a decision that the trial court abused its discretion in issuing the production order). *See also Richmark*, 959 F.2d at 1475 ("The fact that all the information to be disclosed (and the people who will be deposed or who will produce the documents) are located in a foreign country weighs against the disclosure . . . .").

83. *Vetco*, 691 F.2d at 1290 (relying on the *Restatment (Second)* version of this factor). *Vetco*'s formulation of this test was retained after the move from the *Restatement (Second)* to the *Restatement (Third)* and thus continues to be the test under the *Restatement (Third)*'s fourth factor. *Richmark*, 959 F.2d at 1475 (citing *Vetco*, 691 F.2d at 1290) ("[T]he alternative means must be "substantially equivalent" to the requested discovery.").

84. *In re* Sealed Case, 825 F.2d 494, 498 (D.C. 1987).

is equivalent to the one requested and will not violate foreign law, this fourth factor will weigh in favor of granting the protective order.[85]

When evaluating the fifth factor, the effect of the court's action on U.S. and foreign interests, U.S. interests are weighed against the interests of the foreign sovereign. The U.S. interest is generally articulated as "ensuring parties a full and fair adjudication of their case."[86] In assessing the interests of the foreign sovereign, U.S. courts value input from the foreign government. In fact, the party seeking the protective order is more likely to prevail if the foreign sovereign submits a statement or otherwise expresses that violating the foreign law, even to comply with a U.S. discovery order, severely undermines sovereign interests.[87] The party seeking the protective order is also more likely to prevail if the very act of producing documents will violate foreign law, rather than when foreign law requires an event to trigger a violation, such as a report or return to the home country.[88]

Lastly, apart from any formal factors, courts are more likely to grant a protective order to a party which, although resisting discovery, notably made good faith efforts to comply with the discovery process to the greatest possible extent.[89]

Two courts have granted protective orders specifically on the basis of EU data protection laws. In *Volkswagen v. Valdez*, Volkswagen objected to a discovery request for its current corporate telephone book containing the names, work telephone numbers, and home telephone numbers of over 20,000 employees.[90] Using the five-

85. *See generally Volkswagen*, 909 S.W.2d at 903 (holding that the company was not required to produce a German copy of a document when its American equivalent was available).

86. ANTIRUST LAW SECTION OF THE AM. BAR ASS'N, *supra* note 30, at 58 (citing Minpecov. Conticommodity Servs., Inc., 667 F. Supp 151 (S.D.N.Y. 1988)).

87. *See Volkswagen*, 909 S.W.2d at 902-03. *See also* Alfadda v. Fenn, 149 F.R.D. 28, 34-35 (S.D.N.Y. 1993) (counting the fifth factor against the party resisting discovery because, in part, Switzerland did not submit a statement that violation of the secrecy laws would seriously undermine Swiss interests). In many instances, U.S. courts view these statements from the foreign soverign as confirmation that an important foreign national interest exists apart from a general dislike of U.S. pre-trial discovery. ANTITRUST LAW SECTION OF THE AM. BAR ASS'N., *supra* note 30, at 57. When the foreign law at issue is a blocking statute, U.S. courts will generally give the foreign interest less weight. *Id.* at 53. Genuine concern for data privacy, on the other hand, will generally be respected; however, U.S. courts appreciate confirmation that the law at issue represents the latter rather than the former. *Id.*

88. *See Vetco*, 691 F.2d at 1290; *Alfadda*, 149 F.R.D. at 35.

89. *In re Sealed Case*, 825 F.2dat 498. *See Volkswagen*, 909 S.W.2d at 903; *Alfadda*, 149 F.R.D. at 40.

90. *Volkswagen*, 909 S.W.2d at 901.

factor test, the court ruled in favor of Volkswagen. Agreeing with a brief submitted by Germany, the court found that: production of the book would violate German data protection law,[91] sufficiently equivalent alternative production methods had already been used by Volkswagen,[92] and production of the current corporate book was requested solely to enable the plaintiffs to re-check the information already discovered through other sources.[93]

Similarly, in *Salerno v. Lecia*, the court denied a motion to compel discovery because production of the documents requested would violate both the Privacy Directive and the German Data Protection Act.[94] Although the court did not specifically rely on the five-factor test when conducting its analysis, it did find that the European Union had overtly expressed its interests in upholding the Privacy Directive, alternative methods of production were not sufficiently equivalent, and serious ramifications exist for violating the Privacy Directive and its implementing legislation such as the German Data Protection Act.[95]

As the above discussion reveals, U.S. courts can be persuaded to accept restricted production, whether by protective order or substitution of the Hague Evidence Convention Procedures for the Federal Rules of Civil Procedure. Such decisions to restrict production, however, are within the discretion of the court, leaving litigants vulnerable to violations of EU data protection law in the absence of a favorable ruling. As a result, it is important to also examine the possible solutions to the U.S.-EU trans-border litigants' legal quandary provided by the EU Privacy Directive.

Solution B: Use exceptions to the Privacy Directive to fully comply with the U.S. discovery requirements.

If the U.S. court requires the Federal Rules of Civil Procedure be used instead of the Hague Evidence Convention and denies the protective order, a litigant may nevertheless attempt to fully comply with U.S. discovery requirements by relying on exceptions to the Privacy Directive. In order to fully comply with the Privacy Directive, however, the litigant must both establish that an exception to the

91. *Id.* at 902-03.
92. *Id.* at 903.
93. *Id.*
94. Salerno v. Lecia, Inc., No. 97-CV-973S(H) 1999 WL 299306, *3 (W.D.N.Y. Mar. 1999).
95. *Id.*

transfer restrictions in Article 25 applies and justify processing under Article 7.[96]

Part 1: Use exceptions to the Privacy Directive transfer provisions to remove the restrictions on the scope of personal data available for discovery.

The Privacy Directive prohibits the onward transfer of personal data originating in the European Union to third countries lacking adequate data protection.[97] Nevertheless, such transfers can lawfully occur under the Privacy Directive framework. There are three alternatives for lawfully transferring personal data to third countries lacking adequate data protection; however, the Working Party has created an order of preference for these alternatives.[98] The most favored method for onward transfers to the United States, a country lacking adequate data protection, is transferring data to an entity participating in the safe harbor program.[99] If use of the safe harbor is not available, the Working Party recommends using the derogations listed in Privacy Directive Article 26(2).[100] According to the Working Party, the third method, the exceptions in Privacy Directive Article 26(1), should only be used as a last resort.[101]

Option A: Safe Harbor.

Although the Working Party prefers that transfers to U.S. entities take place through the safe harbor mechanism, the safe harbor was not designed to encompass transfers for compliance with U.S. discovery requirements.[102] The safe harbor mechanism creates a presumption of adequate data protection standards in any U.S. entity that adopts the required processing principles and allows EU entities to transfer personal data to qualified U.S. entities without violating the Privacy Directive.[103] Thus, conceivably, if the United States party to a U.S.-EU trans-border dispute qualified under the safe harbor

96. Privacy Directive, *supra* note 7, arts. 7, 25.

97. *Id.* art. 25.

98. Working Party, *Working Document on a Common Interpretation of Article 26(1) of Directive 95/46/EC of 24 October* 1995, at 9, 2093/05/EN, WP 114 (Nov. 25, 2005) [hereinafter WP 114].

99. *Id.*

100. *Id.*

101. *Id.*

102. Safe Harbor Principles, *supra* note 12.

103. *Id.*

mechanism, direct transfers between the parties would be covered. However, transfers to opposing counsel or a U.S. court would be considered additional onward transfers and be specifically prohibited under the terms of the safe harbor principles.[104] As a result, the safe harbor mechanism is of little utility in the U.S. discovery context.[105]

Option B: Rely on Privacy Directive Article 26(2) derogations to create an alternative structure for the transfer of personal data to litigants in the United States.

Article 26(2) allows "transfers to a 'non-adequate' third country 'where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights.'"[106] The Working Party has identified two types of adequate safeguards a controller may adopt in order to satisfy the Article 26(2) derogation from Article 25: contractual clauses and binding corporate rules.[107]

Contractual clauses. In order to constitute an "adequate safeguard" under Article 26(2), a contractual clause must "determin[e] how the responsibility for data protection compliance is split between the two parties [and] provide additional safeguards for

---

104. *Id.* The Safe Harbor Onward Transfer Principle allows, under certain conditions, a safe-harbor participating organization to transfer data to third parties not participating in the Safe Harbor for processing. If the non-safe-harbor participating third party is acting as the organization's agent, data may be transferred to it for processing if the participating organization first ascertains that the non-safe-harbor third party is obligated to uphold the principles of the Privacy Directive, either by application of another law or by contractual obligations between the parties. *Id.* If, however "the [participating] organization knew or should have known the third party would process it in" a way contrary to the Privacy Directive, the participating organization will be held responsible for the third party's violations. *Id.* This is helpful in the U.S. discovery-Privacy Directive context because it allows transfers of data from the participating organization to their U.S. legal counsel under the Safe Harbor provisions when the U.S. legal counsel is being retained as an agent of the participating organization and contractually agrees to provide the same level of protection as the Safe Harbor Principles. Transfers to non-participating third parties that are not acting as the participating organization's agent may also occur as long as the participating organization complies with the Notice and Choice principles of the Safe Harbor. *Id.* This exception, however, has little application in the U.S. discovery-EU Privacy Directive context, as U.S. courts disfavor subjecting the discovery process to the consent of the data subject.

105. *See* Leeuw & Wellner, *supra* note 6 (arguing briefly that the safe harbor mechanism does not control the discovery process and "is, in fact, incompatible with, typical discovery in the U.S.").

106. Working Party, *Working Document on Transfers of Personal Data to Third Countries: Applying Articles 25 & 26 of the EU Data Protection* Directive, at 15, DG XV D/5025/98, WP 12 (July 24, 1998) [hereinafter WP 12].

107. WP 114, *supra* note 98, at 5. *See also* Privacy Directive, *supra* note 7, art. 26(2).

the data subject made necessary by the fact that the recipient in the third country is not subject to an enforceable set of data protection rules providing an adequate level of protection."[108] Specifically, the contract must provide substantive data protection,[109] provide redress to the data subject,[110] and provide support to the affected data subjects.[111] While contractual clauses are generally favored by the Working Party[112] and standard contractual clauses have been formulated to encourage their standardized use,[113] there are two situations in which the Working Party finds them unworkable: first, when no supervisory body exists in the third country in which the data recipient is located[114] and second, where the third country authorities possess the power to access information which "go[es] beyond those permitted by internationally accepted standards of human rights protection."[115]

Given the long-standing disagreement between civil and common legal systems' approach to evidence gathering[116] and the Working Party's specific disapproval of data protection standards in the context of U.S. legal investigations,[117] it is likely that the United

---

108. WP 12, *supra* note 106, at 16.

109. *Id.* at 17-20. The contract must provide for the following substantive data protection principles: the purpose limitation principle, the data quality and proportionality principle, the transparency principle, the security principle, the rights of access, rectification and opposition, and restrictions on onward transfers, with possible additional principles needed for sensitive data, direct marketing, and automated individual decisions. *Id.* at 6-7.

110. *Id.* at 18-20. This refers to enforcement mechanisms so that data subjects whose rights have been violated can seek redress. *Id.*

111. *Id.* at 20. This refers to an institutional mechanism providing for complaint investigation and a mechanism for compensating data subjects whose rights have been violated. *Id.*

112. Working Party, *Working Document: Transfers of Personal Data to Third Countries: Applying Article 26(2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers*, at 6, 11639/02/EN, WP 74 (June 3, 2003) [hereinafter WP 74] (stating that Safe Harbor and contracts are both adequate safeguards which are preferred over binding corporate rules).

113. Commission Decision 2001/497, On Standard Contractual Clauses for the Transfer of Personal Data to Third Countries Under Directive 95/46/EC, 2001 O.J. (L 181) 19 (creating a set of standard contractual clauses); Commission Decision 2004/915, Amending Decision 2001/497/ED as Regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385) 74.

114. WP 12, *supra* note 106, at 22.

115. *Id.* at 23.

116. *See supra* notes 22-34 and accompanying text.

117. *See* WP 117, *supra* note 15, at 5, 8, 11 (describing the conflict between U.S. whistleblowing schemes and the Privacy Directive and pointing out specific problems with

States would be considered a third country that falls within both of the unworkable situations for standard contractual clauses. As a result, the standard contractual clauses will provide little relief for litigants facing the U.S. discovery-Privacy Directive conflict.

Binding corporate rules.[118] Intended as a tool only to be used when the safe harbor and contractual clauses are particularly problematic,[119] binding corporate rules are best suited to deal with "the international transfer of personal data within the same corporate group at a multinational level."[120] In order to create an "adequate safeguard" under Article 26(2), the binding corporate rules must be approved by the relevant national data protection authority.[121] The national data protection authority will only approve such schemes if they are binding both internally within the group and externally in a court of law.[122] Additionally, the binding corporate rules must provide for: audits,[123] cooperation with data protection authorities,[124] a clearly delineated complaint handling department,[125] and mechanisms providing redress and appropriate compensation to data subjects when necessary.[126]

Importantly for the U.S. discovery context, binding corporate rules only make transfers *within* the corporate group lawful under

---

anonymous reports). *See also* WP 128, *supra* note 11, at 8-9, 18-22 (describing how the Society for Worldwide Interbank Financial Telecommunication's ("SWIFT") compliance with subpoenas from the U.S. Treasury violated the Privacy Directive because SWIFT did not use an adequate safeguard when transferring the data to the U.S. government).

118. Note that the term "binding corporate rules" is meant to encompass policies akin to codes of conduct, but the Working Party did not want to confuse their discussion with Article 27, so it used the term "binding corporate rules." WP 74, *supra* note 112, at 8.

119. *Id.* at 6.

120. *Id.* at 5.

121. Privacy Directive, *supra* note 7, art. 26(1). *See also* WP 114, *supra* note 98, at 5; WP 74, *supra* note 112, at 5 ("Data protection authorities receive requests for authorization for the transfer of personal data to third countries within the meaning of Article 26(2) of the directive.").

122. WP 74, *supra* note 112, at 10-11. As regards the externally binding aspect of the binding corporate rules, data subjects must be regarded in law as third party beneficiaries of the rules with certain rights. *Id.* at 12. *See also id.* at 12 n.12.

123. *Id.* at 16.

124. *Id.* at 17.

125. *Id.*

126. *Id.* at 18. Data subjects must also be entitled to take action against the controller. *See id.* at 19. Furthermore, data subjects must be told of the transfers and the controller needs proof that data subjects were so informed. *Id.*

Article 26(2), not all transfers.[127] Thus, while a party to U.S. litigation might be able to gather discoverable materials through the use of binding corporate rules, it could not transfer the discoverable materials to the parties in the litigation not bound by the rules, or their counsel. Thus, although binding corporate rules are encouraged by the Working Party over the exceptions found in Article 26(1),[128] they have limited utility in the U.S. discovery context.

Option C: Rely on Privacy Directive Article 26(1) exceptions to fully excuse the transfer of personal data to litigants in the United States.

Article 26(1) of the Privacy Directive provides exceptions to the requirement in Article 25 that onward transfers of personal data originating in the European Union only be to countries providing an adequate level of data protection.[129] However, as a matter of general EU legal interpretation, exceptions from a general rule "must be interpreted restrictively."[130] As such, the Working Party insists that

---

127. *Id.* at 9 ("Transfers of personal data to companies outside the corporate groups would remain possible but not on the basis of the arrangements put in place by legally enforceable corporate rules but on the basis of any other legitimate grounds under Article 26 of the Directive . . . .").

128. The Working Party has issued several documents instructing how to comply with the requirements for binding corporate rules in hopes of encouraging corporate groups to adopt them when applicable. *See* Working Party, *Working Document on Frequently Asked Questions (FAQs) Related to Binding Corporate Rules*, 1271-00-02/08/EN, WP 155 (June 24, 2008) (clarifying "particular requirements for applicants in order to assist them in gaining approval for their BCRs"); Working Party, *Working Document Setting Up a Framework for the Structure of Binding Corporate Rules*, 1271-00-01/08/EN, WP 154 (June 24, 2008) (suggesting "what the BCRs might look like when incorporating all of the necessary elements identified in documents WP 74 and WP 108"); Working Party, *Working Document Setting Up a Table with the Elements and Principles to be Found in Binding Corporate Rules*, 1271-00-00/08/EN, WP 153 (June 24, 2008) (clarifying and synthesizing Working Party statements on the necessary content of binding corporate rules); Working Party, *Recommendation 1/2007 on the Standard Application for Approval of Binding Corporate Rules for the Transfer of Personal Data*, WP 133 (Jan. 10, 2007) (creating a standard document for applying to Data Protection Authorities for the approval of binding corporate rules); Working Party, *Working Document Setting Forth a Co-Operation Procedure for Issuing Common Opinions on Adequate Safeguards Resulting From "Binding Corporate Rules,"* 05/EN, WP 107 (Apr. 14, 2005) (creating a procedure for synthesizing the data protection authority approval process in multiple E.U. countries); Working Party, *Working Document Establishing a Model Checklist Application for Approval of Binding Corporate Rules*, 05/EN, WP 108 (Apr. 14, 2005) [hereinafter WP 108] (creating a checklist for compliance with the requirements for binding corporate rules); WP 74, *supra* note 112 (describing briefly the content necessary for Binding Corporate Rules).

129. WP 114, *supra* note 98, at 6.

130. *Id.* at 7.

Article 26(1) can only be applied appropriately when recourse to the Article 26(2) "framework is impossible in practice, where the risks to the data subject are small and Articles 6, 7, and 8 applied appropriately."[131] Additionally, EU member states can provide, via domestic law, for the exceptions not to apply in certain cases.[132] Furthermore, when an entity relies on Article 26(1), the authorities can, with sufficient reason, "intervene at any time and recommend that an international transfer of data should be carried out on the basis of adequate safeguards in the meaning of Article 26(2) rather than by applying the exceptions listed in Article 26(1)."[133]

Despite the many restrictions accompanying the Article 26(1) exceptions, it appears that two exemptions may apply to onward transfers of personal data originating in the European Union to U.S. entities for discovery purposes: consent under Article 26(1)(a), and establishing a legal claim or defense under Article 26(1)(d).

Article 26(1)(a) – Consent. To rely on this exception, consent must be obtained from each data subject affected by the transfer.[134] Consent usually cannot be implied,[135] but instead must be freely given, specific, and informed.[136] Consent is only considered freely given if it was given prior to the transfer, the data subject truly had the ability to withhold consent without suffering harm, and the data subject retains the right to withdraw consent at any point.[137] The consent must be specific in the sense that the data subject authorizes a particular transfer or a category of transfers.[138] Lastly, the data subject must have given consent after receiving information regarding the transfer recipient's purpose and identity, and the specific risk resulting from the fact that the data is being transferred to a country providing inadequate data protection.[139]

The Privacy Directive exception for consent is unreliable in the U.S. discovery context for two reasons. First, in conformance with the

131. *Id.* at 9.

132. *Id.* at 7.

133. *Id.* at 10.

134. Privacy Directive, *supra* note 7, art. 26(1)(a) (allowing transfers to inadequate third countries if "the data subject has given his consent") (emphasis added). *See also* WP 114, *supra* note 98, at 10-12 (describing the content to be obtained from each data subject).

135. WP 12, *supra* note 106, at 24.

136. WP 114, *supra* note 98, at 11-12.

137. *See id.* at 10-11.

138. *Id.* at 12.

139. *Id.*

Privacy Directive, the data subject retains the right to withdraw consent at any time. A withdrawal of consent would mean that the party that received the data must delete it, rendering it useless in a litigation context. Second, U.S. courts generally disfavor allowing the discovery process to be dictated by the will of third parties. In fact, one court went so far as to say that "attempting to obtain consents from affected third parties is not an alternate means of production" because "[i]t may limit the information obtainable."[140] As such, the consent exception of Article 26(1)(a) has limited utility in the context of the U.S. discovery-EU Privacy Directive conflict.

Article 26(1)(d) – Establishing a Legal Claim or Defense. Article 26(1)(d) allows transfers to a third country lacking adequate standards of data protection when "the transfer is necessary . . . for the establishment, exercise or defense of legal claims."[141] To rely on this exception, the receiving entity must be party to a present legal proceeding, not an anticipated proceeding.[142] Furthermore, this exception can only be invoked if the parties have complied with the Hague Evidence Convention.[143] To explain the reach of this exception, the Working Party used the following hypothetical: where "the parent company of a multinational group established in a third country [is] sued by an employee of the group currently posted to one of its European subsidiaries. The exception in Article 26(1)(d) appears to allow the company to legally request the European subsidiary to transfer certain data relating to the employee if these data are necessary for its defense."[144] In this hypothetical, once the data is lawfully transferred to the parent company headquartered in the United States, the data would then be subject to the U.S. discovery process.

The Privacy Directive exception for the establishment of a legal claim or defense is the most reliable exception to the Article 25 prohibition on transfers to third parties in countries with inadequate data protection in the U.S. discovery-Privacy Directive context. The Working Party specifically indicated that Article 26(1)(d)

140. United States v. Vetco Inc., 691 F.2d 1281, 1290 (9th Cir. 1981).

141. Privacy Directive, *supra* note 7, art. 26(1)(d). *See also* WP 12, *supra* note 106, at 25.

142. WP 114, *supra* note 98, at 15 (stating that the exception cannot be used to justify transfers of data "on the grounds of the possibility that such legal proceedings might be brought some day").

143. *Id.*

144. *Id.*

encompasses cross-border litigation through the use of the above hypothetical. The key to successfully relying on this exception is overcoming a common misunderstanding as to the meaning of the term "pre-trial discovery" in the U.S. legal system.[145] Many countries with civil legal systems understand this term to mean document recovery before a suit is filed, which the Working Party has specifically stated is not encompassed by the Article 26(1)(d) exception.[146] It behooves litigants relying on this exception, therefore, to demonstrate through detailed documentation and provision of the court record to the relevant data protection authority that the data sought is part of an ongoing legal proceeding.

Part 2: Use Privacy Directive Article (7) to justify processing of lawfully transferred data by litigants in preparation for trial.

Even when personal data is lawfully transferred to a non-adequate third country pursuant to one of the three Privacy Directive alternatives, any processing conducted by the receiving entity must also be lawful. When data is transferred pursuant to the safe harbor, the processing principles set forth in that mechanism apply and would only permit processing that is consistent with the specific purposes for which the data was collected.[147] When data is transferred pursuant to an Article 26(2) "adequate safeguard," the Privacy Directive processing principles apply in full.[148] When data is transferred pursuant to an Article 26(1) exception, however, only Articles 6, 7, and 8 apply to the processing of the transferred data.[149] Notably, for data to be lawfully processed under any of these three transfer schemes, processing must satisfy the Article 7 test of legitimate

145. Hague Conference on Private International Law, *Conclusions and Recommendations Adopted by the Special Commission on the Practical Operation of the Hague Apostille, Evidence and Service Conventions*, ¶ 31 (Oct. 28-Nov. 30, 2003), http://www.hcch.net/upload/wop/lse_concl_e.pdf.

146. WP 114, *supra* note 98, at 15.

147. Safe Harbor Principles, *supra* note 12.

148. *See* WP 114, *supra* note 98, at 5 (noting that Article 26(2) adequate safeguards "ensure that the indifiduals in question continue to be protected as regards processing of their data, once the data has have been transferred").

149. *Id.* at 8 (noting compliance with Articles 6 and 8 is required); Working Party, *Opinion 8/2001 on the processing of personal data in the employment context*, at 26, 5062/01/EN/Final, WP 48 (Sept. 13, 2001) [hereinafter WP 48] (noting that Article 7 must also be complied with).

purposes.[150] In the U.S. discovery context, there are three possible justifications for processing discoverable personal data under Privacy Directive Article 7: first, "necessary for compliance with a legal obligation to which the controller is subject,"[151] second, unambiguous consent of the data subject,[152] and third, "necessary for the legitimate interests pursued by the controller."[153]

Option A: Legal obligations under Privacy Directive Article 7(c).

Article 7(c) authorizes a data controller to process personal data if it is "necessary for compliance with a legal obligation to which the controller is subject."[154] The Working Party has twice stated that "an obligation imposed by a foreign legal statute or regulation . . . may not qualify as a legal obligation by virtue of which data processing in the European Union would be made legitimate."[155] Privacy Directive Article 7(c) can only provide an avenue of relief for litigants facing the U.S. discovery-Privacy Directive conflict if the U.S. discovery request is enforced against the data controller by an EU judicial authority pursuant to a letter of request under the Hague Convention.[156]

Option B: Unambiguous consent - Privacy Directive Article 7(a).

Article 7(a) of the Privacy Directive provides that processing of personal data is lawful if the data subject gives unambiguous consent to the processing.[157] Like the Article 26(1)(a) consent exception to the

---

150. WP 48, *supra* note 149, at 26 ("It must be remembered that whatever the basis of the transfer under Articles 25 and 26, processing involved in the transfer must still satisfy Article 6 to 8.").

151. Privacy Directive, *supra* note 7, art. 7(c).

152. *Id.* art. 7(a).

153. *Id.* art. 7(f).

154. *Id.* art. 7(c).

155. WP 117, *supra* note 15, at 8. *See also* WP 128, *supra* note 11, at 18 (confirming that a U.S. subpoena will not trigger the Article 7(c) exception because it is a foreign legal obligation rather than a legal obligation arising within the European Union).

156. *See supra* text accompanying notes 134-37. Notably, Article 7(c) could also be used where an EU member state imposes national legal obligations that are the same as U.S. legal obligations. *See* WP 117, *supra* note 15, at 8 (noting that although U.S. Sarbanes Oxley whistleblowing schemes do not satisfy Article 7(c), EU whistleblowing schemes in the form of national law in the same fields as Sarbanes Oxley would). However, the nature of the conflict between U.S. discovery mechanisms and those employed in civil legal systems and the conflict between U.S. and EU regulatory approaches to data protection law makes it unlikely that Article 7(c) can be relied upon in that context.

157. Privacy Directive, *supra* note 7, art. 7(a).

transfer of personal data, Article 7(a) requires that the consent be freely given, specific, and informed.[158] Depending on the nature of the data involved in the discovery requests, litigants can seek consent from the data subjects themselves. In fact, litigants in several cases employed this technique. While some U.S. courts consider such efforts evidence of a good-faith attempt to comply with U.S. discovery procedures,[159] other courts have ruled that "attempting to obtain consents from affected third parties is not an alternate means of production" because "[i]t may limit the information obtainable."[160] In this way, reliance on Article 7(a) may be appropriate in some cases, but not in others.

Option C: Preparation of a legal claim or defense under Privacy Directive Article 7(f).

Article 7(f) provides that processing of personal data is lawful if "necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."[161] The Working Party has recognized that an entity subject to both U.S. and EU jurisdictions has "a legitimate interest in complying with subpoenas under U.S. law."[162] In making this determination, the Working Party found it particularly important that failure to comply with U.S. subpoenas could lead to strict U.S. legal sanctions.[163] Similarly, litigants in a civil or commercial dispute have a legitimate interest in complying with U.S. discovery rules, as they will otherwise face serious sanctions under the Federal Rules of Civil Procedure.[164]

Nevertheless, before processing is lawful under Article 7(f), the legitimate interest of the data controller must be balanced against "the fundamental rights of data subjects."[165] According to the

158. *See supra* text accompanying notes 134-37.

159. Societe Internationale v. Rogers, 357 U.S. 197, 202-03, 211 (1958); Alfadda v. Fenn, 149 F.R.D. 28, 40 (S.D.N.Y. 1993) ("Mr. Radwan's attempt to secure secrecy waivers, if genuine, is indeed evidence of good faith.").

160. United States v. Vetco Inc., 691 F.2d 1281, 1290 (9th Cir. 1981).

161. Privacy Directive, *supra* note 7, art. 7(f).

162. WP 128, *supra* note 11, at 18.

163. *Id.*

164. *See* FED. R. CIV. P. 37 (listing possible sanctions as finding disputed factual issues in favor of the other party, limiting claims, dismissing the action, rendering a default judgment, and contempt of court).

165. WP 128, *supra* note 11, at 18.

Working Party, any determination of lawfulness under Article 7(f) must "take into account issues of proportionality, subsidiarity, the seriousness of the alleged offences that can be notified and the consequences for the data subjects."[166] If the balancing test weighs in favor of the controller and makes processing lawful under Article 7(f), the controller must also: give data subjects "the right to object at any time on compelling legitimate grounds to the processing of the data relating to them,"[167] "inform data subjects about the existence, purpose and functioning of its data processing, the recipients of the personal data and the right of access, rectification and erasure by the data subject,"[168] and notify the appropriate national data protection authorities of their processing activities.[169] Despite these substantial processing requirements, Article 7(f) seems to be the most reliable processing justification in the U.S. discovery context because the Working Party has already determined that compliance with U.S. court orders can constitute a legitimate interest for the purposes of Article 7(f).[170]

As the foregoing analysis demonstrates, it may be possible to use specific provisions of the EU Privacy Directive to fully comply with EU data protection law while simultaneously complying with a U.S. discovery request. To do so, however, a litigant must first justify transfer under Article 26(1)(d) and processing under Article 7(f). As with the options for persuading U.S. courts to accept restricted discovery, this strategy is unpredictable, necessitating a detailed, comprehensive strategy for full compliance with both EU and U.S. laws.

III. CONSTRUCTING A STRATEGY FOR FULL COMPLIANCE

Although the conflict between U.S. discovery rules and the Privacy Directive initially appears irreconcilable, deeper analysis

166. *Id.*

167. *Id.* This fulfills the requirements imposed by Privacy Directive Article 14. *See* Privacy Directive, *supra* note 7, art. 14.

168. WP 128, *supra* note 11, at 19. This fulfills the requirements of Articles 10 and 11. *See* Privacy Directive, *supra* note 7, arts. 10-11.

169. WP 128, *supra* note 11, at 19. This fulfills the requirements of Articles 18-20. *See* Privacy Directive, *supra* note 7, arts. 18-20.

170. WP 128, *supra* note 11, at 18 ("It cannot be denied that SWIFT has a legitimate interest in complying with the subpoenas under U.S. law.").

reveals several options for simultaneous compliance with both sets of rules. Given that each compliance option possesses strengths and weaknesses, recommendations to parties in U.S.-EU trans-border litigation for constructing a strong, three-tiered compliance strategy are set forth below. Three tiers of compliance strategy are necessary because no single strategy has been used successfully with enough frequency to enable confidence in it alone. As a result, the strongest strategy for full compliance involves a plan in which the top tier is the best possible outcome and the third tier is an acceptable outcome. The strategies were placed in tier one, two, or three, depending on their history of success, projected cost, and projected time consumption.

Tier 1: Seek a Protective Order from the U.S. Court

Litigants facing U.S. discovery requests for which compliance requires violating the Privacy Directive should first seek a protective order from the U.S. court excusing noncompliance. This strategy has been successfully used by litigants facing a U.S. discovery-Privacy Directive conflict.[171] To succeed on a motion for a protective order, it is helpful if the litigant:

1. is resisting production of documents which would otherwise help their case or are at least neutral;[172]
2. demonstrates that the requested information originated in the foreign country and remains there;[173]
3. is supported in its motion by a statement from the foreign sovereign that compliance with the discovery request is on its face a violation of the Privacy Directive and its implementing legislation and undermines sovereign interests;[174] and
4. shows evidence of good-faith attempts to comply with the discovery request before seeking the protective order (such as seeking consent from the data subjects, providing alternative forms of the information that satisfies the request, etc.).[175]

171. *See* Salerno v. Lecia, Inc., No. 97-CV-973S(H), 1999 WL 299306, at *3 (W.D.N.Y. Mar. 23, 1999); Volkswagen, A.G. v. Valdez, 909 S.W.2d 900 (Tex. 1995).

172. Societe Internationale v. Rogers, 357 U.S. 197, 212-13 (1958). *See also* United States v. Vetco, Inc., 691 F.2d 1281, 1288 (9th Cir. 1981) (holding this factor against a party resisting production of documents that will likely hurt his case).

173. *Volkswagen*, 909 S.W.2d at 902.

174. *See id.* at 902-03; Alfadda v. Fenn, 149 F.R.D. 28, 34-35 (S.D.N.Y. 1993).

175. *Volkswagen*, 909 S.W.2d at 903l; *Alfadda*, 149 F.R.D. at 40; *In re* Sealed Case, 825 F.2d 494, 498 (D.C. 1987).

Tier 2: Rely on Privacy Directive Articles 26(1)(d) and 7(f) to justify full compliance with the U.S. discovery request.

If the protective order is denied, the litigant's second-tier strategy should be to use the exceptions to the Privacy Directive to fully comply with the U.S. discovery request. In particular the litigant should:

1. rely on Article 26(1)(d) to transfer personal data for the purpose of establishing, exercising, or defending a legal claim; and
2. rely on Privacy Directive Article 7(f) to lawfully process the transferred data to achieve the legitimate interests of the data controller in complying with a U.S. discovery request and avoiding U.S. sanctions for noncompliance.

Before proceeding with the transfer and processing in reliance on these Privacy Directive provisions, the litigant should detail a proposed method of transfer and processing and request approval from the relevant EU member state data protection authority. To obtain permission to proceed under Privacy Directive Articles 26(d)(1) and 7(f), the litigant should demonstrate to the data protection authority that:

1. reliance on Article 26(1)(d) is necessary for the purposes of the litigation because the U.S. court has already denied the protective order and failure to comply with the discovery request will result in severe sanctions;
2. the EU member state's obligations under the Hague Evidence Convention are satisfied by the proposed transfer and processing;[176]
3. compliance with a U.S. discovery order is analogous to compliance with a U.S. subpoena and is a legitimate interest under Article 7(f);
4. the interests of the data subjects are being protected to the highest possible extent so that their rights are not violated by the processing of the data in litigation;
5. the consequences for the data subjects are minimal, if any; and
6. Privacy Directive Articles 6 and 8 will be respected.[177]

---

176. An example of this would be that the request is pursuant to litigation that has already been filed so that Article 23 of the Hague Evidence Convention is not triggered.

177. Article 6 requires that personal data be

(a) processed fairly and lawfully;

Although the Working Party has indicated tentative approval of reliance on Article 7 for such purposes, it has not yet commented on the specific issue of the U.S. discovery-EU Privacy Directive conflict. As such, while this scheme theoretically satisfies the transfer and processing rules set down by the Working Party, it is uncertain whether the application of the rules in this context would be upheld. As a result, this compliance strategy is less favorable than Tier 1 and should be a litigant's second choice.

Tier 3: Petition the U.S. court for substitution of the Hague Evidence Convention for the Federal Rules of Civil Procedure.

If the relevant EU member state data protection authority declines to approve the proposed transfer and processing under Privacy Directive Articles 26(1)(d) and 7, the litigant's final attempt to comply with both U.S. discovery rules and the Privacy Directive should be to petition the U.S. court to substitute the Hague Evidence Convention procedures for the Federal Rules of Civil Procedure. With regard to this petition, the litigant should:

1. demonstrate the overly-broad nature of the discovery requested of it;
2. use the denial of its transfer and processing proposal under Tier 2 by the EU Member State data protection authority to demonstrate the foreign country's aversion to the discovery mechanisms used in this particular case; and

---

(b) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes. . . . ;

(c) adequate, relevant and not excessive in relation to the purposes for which they are collected. . .;

(d) accurate, and . . . ;

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

Privacy Directive *supra* note 7, art. 6.

Article 8 prohibits the processing of several "special catagories of data," namely, "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and . . . data concerning health or sex life." *Id.* art. 8. Privacy Directive Article 8, however, does provide three exceptions to its prohibition of processing sensitive data that would allow such processing during a lawsuit: (1) the data subject has given his specific consent, (2) "processing is necessary for the purposes of carrying out the obligations and specific rights of the controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards," and (3) "the processing relates to data which are manifestly made public by the data subject or is necessary for the establishment, exercise or defense of legal claims." *Id.* arts. 8(2)(a), 8(2)(b), 8(2)(e).

3. allege that no fact specific reason exists for the Hague Evidence Convention procedures to not be effective.

Once the U.S. court authorizes the use of the Hague Evidence Convention, the litigant must then go before the EU judicial authority executing the letter of request and either argue that only non-personal data should be provided via the letter of request because of the Privacy Directive (recommended if the discoverable material will likely hinder the litigant's case)[178] or the personal data requested should be provided via the letter of request despite the Privacy Directive (recommended if the discoverable material will likely help the litigant's case).[179] When making the decision as to which argument to advance before the EU executing authority, the litigant should keep in mind that if a U.S. court remains unsatisfied with the level of discovery achieved under the Hague Evidence Convention procedures, the court retains the right to order production under the Federal Rules of Civil Procedure.[180]

CONCLUSION

Ultimately, the U.S. discovery-EU Privacy Directive conflict remains difficult to navigate. Because the conflict is set within the larger context of the civil versus common legal system approach to evidence gathering, EU member states' data protection authorities have increasingly called for the Working Party to comment on the issue directly. Until the Working Party issues such comments, the three-tiered compliance strategy offers the best opportunity for a litigant facing the U.S. discovery-Privacy Directive conflict to comply with both sets of rules. The most favorable outcome for the litigant is to succeed in the first-tier strategy; however the second- and third-tier strategies are more favorable than risking sanctions either under the Federal Rules of Civil Procedure or the Privacy Directive.

178. *See supra* text accompanying notes 44-45.

179. *See supra* text accompanying notes 46-48.

180. *In re* Perrier Bottled Water Litig., 138 F.R.D. 348, 356 (D. Conn. 1991).