WGS℠

THE SEDONA CONFERENCE®

Framework for Analysis of Cross-Border Discovery Conflicts:

A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery

A Project of The Sedona Conference®
on International Electronic Information
Management, Discovery and Disclosure (WG6)

PUBLIC COMMENT VERSION

AUGUST 2008

The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts:

A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery

2008 Public Comment Version

A Project of The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6)

Editors-in-Chief:

M. James Daley
Kenneth N. Rashbaum

Senior Editors:

Quentin Archer
Moze Cowper
Paul Robertson
Kenneth J. Withers

Contributing Editors:

Amy H. Chung
Conor R. Crowley

The Editors would like to acknowledge the generous assistance of Andrew Cohen, Amor Esteban, Laura Gilbert, Melissa Klipp and Laurie Weiss.

Foreword

Welcome to *The Sedona Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and Discovery,* a project of The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6). The Sedona Conference® Working Group Series (WGS℠) is designed to bring together some of the world's finest attorneys, privacy and compliance officers, technical consultants, records managers, academics and jurists to address current problems in the areas of antitrust law, complex litigation, and intellectual property to use collaborative dialogue -- not debate -- to develop a consensus approach to important issues of law and policy.[1] (See Appendix F for further information about The Sedona Conference® in general, and the WGS℠ in particular.)

This is a companion publication to *The Sedona Overview of International E-Discovery, Data Privacy and Disclosure Requirements*, which provides an overview of the electronic discovery and data privacy landscape of selected countries. Together, these publications are designed to provide a framework for constructive dialogue regarding the resolution (or at least mitigation) of cross-border discovery conflicts. Both of these publications will be published in PDF format, with hyperlinks to the other. The *Overview* publication will also initially be published in Wikipedia format, managed by selected country editors that will provide a platform for collaboration and dialogue, as well as a process for keeping information current. Eventually, we expect that both publications will be made available via a secure Wikipedia, to aid in expanding their scope, and updating their content.

The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6) was conceived at the October 17, 2003 annual meeting of The Sedona Conference® Working Group on Electronic Documents Retention and Production (WG1) in Santa Fe, New Mexico. At that meeting, WG1 members M. James Daley, Tim Opsitnick, Paul Robertson and Susan Wortzman gave a presentation entitled *The International Dimensions of the Electronic Discovery Dilemma*, and addressed the question to WG1: "Why focus on international developments?"

After a spirited dialogue—the hallmark of The Sedona Conference®—a number of WG1 members, under the leadership of Executive Director Richard Braman, responded that The Sedona Conference® is uniquely suited to facilitate a dialogue about the international management and discovery of electronically stored information (ESI). They also responded that these issues are important and timely due to the rapid proliferation of cross-border litigation and regulatory investigations, the increasing interdependence of countries due to commerce and market expansion, and the rapid development of international records retention, e-discovery and e-disclosure rules.

On July 14-17, 2005, WG6 held its first international conference in England at Clare College, Cambridge University. Its second annual conference was held September 28-30, 2006 at the Euroforum in El Escorial, Spain. And the third annual conference was held December 6-7, 2007 at the Fairmont Hamilton in Bermuda. Along the way, on January 14, 2007, WG6 members conducted an Audio Update on International Issues, as well as a successful Webinar on January 24, 2007.

Both *The Sedona Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and Discovery* and *The Sedona Overview of International E-Discovery, Data Privacy and*

[1] Debate: assuming that there is a right answer and you have it; Dialogue: assuming that many people have pieces of the answer and that a solution can be crafted together; Debate: listening to find flaws and to counter; Dialogue: listening to understand meaning; Debate: defending one's views against those of others; Dialogue: conceding when another's thinking can improve on your own; Debate: seeking a conclusion that ratifies your opinion; Dialogue: agreeing upon options without closure. Adapted from Daniel Yankelovich, THE MAGIC OF DIALOGUE (2001).

Disclosure Requirements represent the collective input of 123 members of WG6 from countries as diverse as Australia, Barbados, Brazil, Canada, China, England & Wales, France, Germany, Japan, Netherlands, Spain, Switzerland, Sweden, United Kingdom and the United States, among others.[2]

We want to thank the entire Working Group 6 for all their hard work, and especially the combined Steering and Editorial Committees. We also want to note that WG6 sought and received considerable assistance from members of The Sedona Conference® Working Group 1 in the United States, which began a similar process in October 2002 and published the first U.S. public comment draft of *The Sedona Principles* in March 2003. That publication and the editions that followed have been well received by U.S. courts, both as resources cited in judicial opinions and as significant contributions to the process leading to the amending the Federal Rules of Civil Procedure in December 2006. We hope that *The Sedona Framework for Analysis of Cross-Border Discovery Conflicts* will make similarly positive contributions to the development of International law, policy and practice.

We also want to thank the Annual and Sustaining Sponsors of the Working Group Series; without their financial support our Working Groups could not accomplish their goals. They are listed at www.thesedonaconference.org/sponsorship.

The Sedona Conference® is a nonprofit law and policy think tank based in Sedona, Arizona, dedicated to the advanced study, and reasoned and just development, of the law in the areas of complex litigation, antitrust law and intellectual property rights. It established the Working Group Series (the "WGS^{SM}") to bring together some of the finest lawyers, consultants, academics and jurists to address current issues that are either ripe for solution or in need of a "boost" to advance law and policy.[3] WGS^{SM} output is first published in draft form and widely distributed for review, critique and comment. Following this public comment period, drafts are reviewed and revised, taking into consideration what has been learned during the peer review process. The Sedona Conference® hopes and anticipates that the output of its Working Groups will evolve into authoritative statements of law and policy, both as these are and ought to be.

To make suggestions or if you have any questions, or for further information about The Sedona Conference®, its Conferences or Working Groups, please go to www.thesedonaconference.org or contact us at tsc@sedona.net.

Richard Braman
Executive Director, The Sedona Conference®

Quentin Archer (UK)
M. James Daley (US)
Co-Chairs. The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6)

Steven C. Bennett (US)
Janet Lambert (UK)
Neil Mirchandani (UK)
Sandra Potter (AU)
Paul R. Robertson (US)
Kenneth J. Withers (US)
Steering Committee, The Sedona Conference® Working Group on International Electronic Information Management, Discovery and Disclosure (WG6)

[2] See Appendix E for a listing of active WG6 members as of March 2008.
[3] See Appendix G for further information about The Sedona Conference® in general and the WGS^{SM} in particular.

Table of Contents

Introduction

The "Catch-22" of Cross-Border Discovery

Cross-border discovery[4] represents a "Catch-22"[5] situation in which the need to gather relevant information from foreign jurisdictions often squarely conflicts with blocking statutes and data privacy regulations that prohibit or restrict such discovery—often upon threat of severe civil and criminal sanctions.[6] U.S. courts often have very little familiarity with foreign data privacy and protection regulations and often are skeptical of efforts to restrict the discovery of relevant information from a European parent or affiliate organization. Cross-border discovery has become a major source of international legal conflict, and there is no clear, safe way forward.[7] At the heart of these conflicts are vastly differing notions of discovery and data privacy and protection. And the frequency and intensity of these conflicts is heightened by an expanding global marketplace and the unabated proliferation of electronically-stored information ("ESI").[8]

Indeed, our way of working and communicating across borders has changed profoundly over the last two decades. Our *lingua franca* is digital. We communicate, collaborate and socialize faster and more globally than ever before. We socialize and transact business in electronic form over the Internet and private data lines via telephone, voice mail, e-mail, instant messaging and text messaging, and a host of current and emerging collaborative technologies such as blogs, wikis, and social networks. We exchange information instantaneously with a myriad of portable and wireless devices without regard to borders. The volume, pace and portability of information exchange is unparalleled. And in this "information age," where the primary evidence of our global conduct is almost solely electronic, litigation and regulatory investigations are a fertile ground for cross-border e-discovery.

The Purpose of this Paper

This paper outlines a practical framework for analysis of legal conflicts arising from cross-border discovery of ESI.[9] Although the specific focus of this framework is ESI, the principles outlined here apply generally to print and other tangible evidence as well. The intended audience for this paper includes individuals, corporations, legal counsel, regulators and the judiciary.

---

[4] The term "discovery" and "disclosure" are used interchangeably for the purpose of this paper, notwithstanding the technical distinction in some jurisdictions between these terms. Their related issues of the impact of legal holds and the application of records retention schedules on materials in a company's custody and control in foreign jurisdictions is outside the scope of this paper but will likely be explored in a further paper. *See Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 216 (S.D.N.Y. 2003).

[5] A "Catch-22," after the book of the same name written in 1955 by Joseph Heller, is a situation where there are only two options, and both lead to undesirable results. In the book, an Army bombardier, Yossarian, asks to be taken off dangerous missions. The only way to be relieved of combat duty is to be ruled insane under Section 8 of the Military Code. But Clause 22 of Section 8 stipulates that "A concern for one's own safety in the face of dangers that are real and immediate is the process of a rational mind." Thus, Yossarian's very request to be relieved of duty proves he is "rational" and disqualifies him from relief from combat duty, and he must keep flying. (Hence, "Catch-22"). Joseph Heller, CATCH-22 55 (Simon & Schuster 1955).

[6] *Id. See also* Wikipedia, *Catch-22*, http://en.wikipedia.org/wiki/Catch-22.

[7] RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 442 Reporters' Notes, n. 1 (1987).

[8] The term "electronically stored information" has been adopted as a term of art in the U.S. Federal Rules of Civil Procedure and several U.S. state court rules. Fed. R. Civ. P. 34(a)(1), 2006 Committee Note ("A common example often sought in discovery is electronic communications, such as email. The rule covers — either as documents or as electronically stored information — information "stored in any medium," to encompass future developments in computer technology. Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information, and flexible enough to encompass future changes and developments.").

[9] The impact of legal holds and records retention schedules on data privacy regulations and blocking statutes is outside the scope of this paper, but is an important area for further inquiry. *See Zubulake*, *infra* note 4 at 216.

The foundation of our practical framework is an examination of differing notions of data privacy and legal discovery. This paper also draws from an overview of specific data privacy, discovery and disclosure regulations and practices in selected countries found in a companion paper by Working Group 6 of The Sedona Conference.[10] Our goal is that the reader use this framework to help navigate the turbulent currents of cross-border conflicts between data privacy and discovery, informed by country-specific data privacy, discovery and disclosure rules and practices.

This paper was prepared by a global team of professionals. As such, we hope it offers a broad international perspective on current practices and proposed best practice models to resolve conflicts, which may arise in relation to cross-border transfer of information during discovery. And while much of the analysis arises from the European Union, given the EU Privacy Directives, we believe the framework presented is transferable to any cross-border discovery conflict, regardless of the jurisdictions involved. In the end, the best way to avoid the "Catch-22" of cross-border discovery conflicts is for countries to use the framework below to engage, communicate and collaborate in crafting measures that reinforce data protection and privacy while respecting the legitimate need for the discovery of information as an integral part of the judicial and regulatory process.

[10] *The Sedona Conference® Overview of International E-Discovery, Data Privacy and Disclosure Requirements* (Public Comment Draft 2008) (forthcoming).

II. A Practical Framework for Analysis of Cross-Border Discovery Conflicts

Framework Outline

The following is an outline of the Framework for Analysis of Cross-Border Conflicts.

I. Is there jurisdiction?

- A. Does the forum court have jurisdiction over the data?
  - 1. Does an affiliate of a party have custody/control/access?
    - a. Determine relationship between affiliate and party
      - i. Ascertain "control" of data: physical, contractual, corporate (be careful not to confuse access with control)
        - a. U.S. and E.U. definitions of "control" and "data controller" must be clearly understood
    - b. Is the data already in the forum nation?
      - i. What is the location of the data "at rest?"
      - ii. Are the data routinely accessed by personnel based in the forum nation?

- B. Which non-forum entity has jurisdiction?
  - 1. Determine whether there is jurisdiction over the activity (data processing/collection in the E.U.), the data and/or the parties
  - 2. Consider nationality factors
    - a. Nationality of person or subject of the data
    - b. Nationality of the person(s) controlling the data
    - c. How do particular jurisdictions determine nationality?
  - 3. Consider geographic factors
    - a. Where was the data created?
    - b. Location(s) of data at rest
    - c. Location of server(s)
    - d. Location of data controller(s)
    - e. Where is the data processed?
    - f. Location of the subject and author of the data

II. Determine whether the data is subject to a provision limiting cross-border transfer

- A. Consider the character of the data
  - 1. Is the data personal (e.g., identifying individuals; identifying race, gender, religion, etc.)?
  - 2. Is the data sensitive (technological, national security, certain financial/company data)?
  - 3. Is the data industry-specific (medical information; telecommunications)?

- B. Consider the jurisdiction of the limiting provisions
  - 1. Regional (E.U. Directives)
  - 2. Country privacy laws
    - a. E.U. Directives enabling statues

b. Provisions which are more restrictive than E.U. Directives
c. Provincial/local (e.g., German Länder; Canadian provinces)

3. Industry-specific (financial; anti-trust; technological)

C. Are there derogations or exceptions to the limiting provisions?
1. Information in the public domain (i.e., data filed with governmental entities)
2. Transfers to enable compliance with regional or local legal obligations
3. Transfer to establish, exercise or defend a legal claim (NB: rejection of this exception by most EU Data Commissioners for discovery related to U.S. litigation and investigations)

D. Can the data be made to fit the limitations of the provisions?
1. De-identification (stripping of identifiers)
2. Consent/Notice of data subjects/authors
3. Limitation of data request (proportionality)

III. Is there a blocking statute?

A. General
B. Industry-specific

IV. Is there a treaty, legislation or agreement between the parties which may provide a solution?

A. Is the Hague Convention available and useful?
B. May consent be obtained from a Data Commissioner?
C. Will a Protective Order satisfy the pertinent provisions and/or Data Commissioner?

III. E-Discovery and the Nature of ESI

What is Electronic Discovery?

Electronic discovery, commonly referred to as "e-discovery," is the process of identifying, collecting, filtering, searching, de-duplicating, reviewing and potentially producing ESI that relates to pending or reasonably anticipated litigation in the host or a foreign country. In addition to the civil litigation context, foreign parent companies and their affiliates are subject to expansive discovery in criminal and regulatory investigations and prosecutions in the United States and other countries. For example, the U.S. Department of Justice, working in tandem with the U.S. Securities and Exchange Commission is quite active in investigating and prosecuting violations of the Foreign Corrupt Practices Act,[11] the Sherman Antitrust Act,[12] and the Sarbanes-Oxley Act,[13] among others.

Intentional or even inadvertent loss or deletion of ESI may place officers and directors of foreign parent corporations and their affiliates at risk of criminal prosecution for obstruction of justice, as reflected by the recent prosecution of Arthur Andersen LLP. While the conviction of Arthur Andersen LLP was ultimately reversed, the catastrophic economic and reputational damage had already been done. And in the wake of Arthur Andersen and Enron, Sarbanes-Oxley was amended to make it a criminal offense to "corruptly or knowingly alter, destroy, mutilate, conceal or cover up information with the intent to impede or obstruct federal authorities."[14] Most commentators agree that criminal penalties for "data destruction" will likely increase in the future, exacerbating cross-border discovery conflicts.

The main focus of ESI discovery is the content and not the container. That is, any kind of relevant ESI in any computer system is fair game. This includes all forms of ESI (e-mail, word processing, spreadsheets, etc.) as well as all types of ESI systems (e-mail servers, file servers, database systems, etc.).[15] If ESI content is relevant to a dispute, then it is a potential target of discovery, regardless of format or location.

Why is ESI Different?

Commentators have noted six major qualitative and quantitative differences between ESI and printed information:

1. Volume and ease of replication
2. Persistence
3. Dynamic nature
4. Existence of hidden metadata
5. Hardware & software system dependence and obsolescence
6. Mobility, portability and searchability[16]

Volume and Ease of Replication

Experts estimate that well over ninety percent of all information is generated, received and stored electronically.[17] Murphy's law is well known, but in the computing world, the lesser-known "Moore's law" prevails. Moore's law, named after former Intel Co-Founder, Gordon E. Moore, generally stands for the proposition that the speed and

[11] Foreign Corrupt Practices Act of 1977, 15 U.S.C. §§ 78dd-1, *et seq*. (2004).
[12] Sherman Antitrust Act, 15 U.S.C. §§ 1-7 (2004).
[13] Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, 116 Stat. 745 (codified as amended in scattered sections of 15 U.S.C.).
[14] 18 U.S.C. §§ 1512 C & 1519 (2004).
[15] For readers less familiar with technical terms relating to e-discovery, please see *The Sedona Conference Glossary: E-Discovery & Digital Information Management*, *available at* www.thesedonaconference.org.
[16] *The Sedona Principles, Second Edition: Best Practices, Recommendations & Principles for Addressing Electronic Document Production*, pp. 3-8 (The Sedona Conference® Working Group Series, 2007).
[17] *Id.*

storage capacity of technology will double every two years.[18] In the computing world, Moore's law has been applied to a broad range of technological change such as processor speeds, RAM capacity, storage capacity of removable media and hard drive volumes. In the context of ESI, where volumes are increasing exponentially, Moore's law appears to be alive and well.

It is no wonder we are awash in ESI. Over the last 15 years, the declining cost of PC computing and server storage, combined with e-mail as a ubiquitous channel for distribution and replication of ESI has caused a strategic inflection point in records management where the majority of ESI is almost entirely unmanaged.[19] The resulting burden of this unmanaged ESI on corporations, counsel and courts is enormous.

Persistence

ESI is persistent. Even deleted electronic files can be completely or partially "resurrected" with today's forensic tools. Deletion is not destruction. Deleting ESI is not the functional equivalent of shredding or burning a paper document.

Dynamic Nature

ESI is dynamic and alterable. For example, databases are designed to facilitate adding, modifying and deleting records. Unless steps are taken to preserve certain database information, it can be permanently altered or deleted. Likewise, it is relatively simple to alter the content of electronic files. Even the simple act of accessing an electronic file can inadvertently change certain system metadata, such as the last modified and accessed date. Generally, forensic tools such as MD5 hash values[20] that create "digital fingerprints" are required to prove that the content of an electronic file is authentic and has not been altered.

Existence of Metadata

Metadata is simply "information about electronic information" that is stored in a computer system, or within an electronic file. For example, metadata includes the formulas and text notes that are embedded in a spreadsheet; the speaker's notes that are embedded in a PowerPoint presentation; and the track changes edits in a Microsoft Word document. Less common examples include the file's date and time stamp set by the systems internal clock, which is viewable using the "details" option in Microsoft XP or Vista. Or, in the case of Microsoft Outlook, it can be one of hundreds of hidden fields that track the date that e-mails were created, modified, sent, received, and acknowledged.

These application metadata fields are hidden from the ordinary user. Server administration rights or specialized forensic tools are required to view this information, which can help to answer the question asked in the Iran Contra "arms for hostages" scandal: [21] Who knew what and when?

System Dependence and Obsolescence

Printed documents only require human eyes for interpretation. Electronic documents require some kind of electronic system to interpret them, whether the file is in "native"[22] or a converted format.[23] And in the case of complex

---

[18] In 1965, Dr. Moore predicted that the number of transistors that can be inexpensively placed on an integrated circuit increases exponentially, doubling approximately every two years.

[19] The term, "inflection point," was coined by another Intel pioneer, former CEO Andrew Grove in "Only the Paranoid Survive" to describe Intel's failure to foresee the dramatic consequences of marketing Intel processors directly to consumers, rather than just computer manufacturers, when the early Pentium "bug" was identified.

[20] *See The Sedona Conference® Glossary: E-Discovery & Digital Management* (Second Edition, 2007), p. 25 ("Hash: A mathematical algorithm that represents a unique value for a given set of data, similar to a digital fingerprint. Common hash algorithms include MD5 and SHA.").

[21] *Armstrong v. Executive Office of the President*, 1 F.3d 1274 (D.C. Cir. 1993).

[22] "Native" format refers to the original format in which the file was created, such as a .doc file created by Microsoft Word.

relational databases and other specialized applications, the original hardware, software and "native" data files are required in able to sort, search, retrieve, and report information as was done in the ordinary course of business.

Mobility, Portability and Searchability

ESI is increasingly mobile – it can be replicated and stored on computers across continents with relative ease. It is extremely portable. A library's worth of sensitive data can be physically transported on a small USB thumb drive. And it is searchable. One of the major differences between electronic and printed information is the potential for finding the proverbial "needle in a haystack" through the use of increasingly powerful key word and concept-based search and retrieval technologies.

[23] Typical converted formats found in e-discovery include PDF (portable document format) and TIFF (tagged image file format).

IV. The Human Landscape: Differing Notions of Privacy

What is Data Privacy and Protection?

Too much of the developed world, data privacy is a fundamental human right.[24] This concept certainly is embraced by the 30 member states of the European Economic Area ("EEA") and a host of other developed nations, including Australia, Canada and Japan to name a few. These countries generally embrace a much broader view of "personal data" than the United States; for example, the 1995 EU Data Protection Directive[25] and similar data privacy legislation[26] protects against the unauthorized processing or transfer of "personal data," which includes any information relating to an identifiable individual.[27]

Yet in the United States, the concepts of "personal data" and "processing" of data are quite different; and this fact contributes to difficulties in cross-border communication and collaboration in this arena. [28] Indeed, the concept of "personal data" in the United States is restricted to specific types of personal and sensitive information, such as personal medical information,[29] social security information, and banking information. In the EU, this would be considered "personal sensitive data," which commands an even greater degree of protection.

In addition, in the EU Data Protection Directive, the concept of "processing" is broadly defined as "any operation or set of operations," whether manual or automated, including but not limited to "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."[30] In contrast, in the United States, "processing" is generally understood as only as relating solely to technical actions, such as conversion from one format to another, de-duplication, high-level filtering, indexing, sampling, and the like.[31]

In this sense, while the European Union and other countries take a global approach to protection of personal data, the United States takes a very segmented approach as to both the scope of personal data and processing of such data. It is critical to understand these semantic differences in any dialogue regarding these issues. Of course, it should be noted that in most third-world countries, data privacy is altogether non-existent.

---

[24] *See* data privacy legislative history discussion *available at* http://ec.europa.eu/justice_home/fsj/privacy.
[25] Directive 95/46/EC of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, *at* 31-50.
[26] The Data Protection Directive imposes obligations on Member States, which must implement the principles of the Directive in their national laws. These national laws, which can vary from State to State, in turn impose direct obligations on the individuals and organizations subject to their jurisdiction.
[27] European Commission, *Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN (2007), *available at* http://europa.eu.int.
[28] *See* Cate and Eisenhauer, "Between a Rock and Hard Place: The Conflict Between European Data Protection Laws and U.S. Civil Litigation Document Production Requirements," *Privacy & Security Law Report*, Vol. 6, No. 6, 02/25/2007.
[29] This is regulated by the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), Pub. L. 104-191 (1996). Sections 261 through 264 of HIPAA require the Secretary of HHS to publicize standards for the electronic exchange, privacy and security of health information.
[30] *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*, Official Journal L 281, 23/11/1995 P. 0031 – 0050, *available in English at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (visited August 26, 2008).
[31] Even personal data in the hands of third-party contractors and agents is included under the Data Protection Directive. *See also* M. James Daley, *Preservation of Electronic Records of Third-Party Contractors*, Practicing Law Institute, (Jan. 2007) (U.S. perspective).

The widespread collection and sale of personal information in the United States for commercial marketing purposes, and the disclosure of airline passenger lists and certain banking information under the U.S. Patriot Act[32] are understandably frightening developments for those who hold privacy as an inalienable right. And the significant number of security breaches of governmental, corporate and non-profit data repositories that have resulted in the compromise of sensitive personal information has led to a crisis of confidence in the ability of technology to protect this interest. Indeed, a non-profit privacy group, attrition.org, maintains a Data Loss Database that chronicles over 850 significant known information security breaches resulting in the loss of personal sensitive data since 2001.[33] Recent examples include:

21 March 2008	loss of 1 million customer personal and financial records from a stolen Compass Bank laptop computer;
17 March 2008	loss of 4.2 million credit card numbers from the Hannaford database;
12 March 2008	loss of 10,000 social security numbers and personal data from a Harvard University database;
27 February 2008	pubic disclosure of 103,000 social security numbers and patient medical information from Health Net Federal Services;
13 February 2008	loss of 321,000 health and financial records from missing Lifeblood laptops;
29 January 2008	loss of 38,000 social security numbers and other personal information from a hard drive stolen from Georgetown University;
18 January 2008	loss of 600,000 passport details, National Insurance numbers and medical records from a stolen laptop of the United Kingdom Ministry of Defence;
17 January 2008	loss of 650,000 credit card numbers and social security numbers of GE Money customers from a missing backup from an Iron Mountain facility.

Along with difference in the cultural appreciation of data privacy, confusion as to the scope abounds. That is, the EU Directive and similar legislation protects the privacy of all kinds of personal data. This would include any e-mails identifying an employee as an author or recipient, for example.[34] As noted above, in the United States, personal data would ordinarily be viewed as something very unique to a person, and data with a high degree of sensitivity, such as their medical records, their social security number, their personal address and telephone number, and their banking records.

In the discussion that follows as to differing notions of privacy in the context of cross-border discovery, certain jurisdictions are mentioned for illustrative purposes only. More detail concerning the data privacy and protection regimes in these and other countries will be included in the "living" companion publication: *The Sedona Conference® Overview of International E-Discovery, Data Privacy and Disclosure Requirements*, which is scheduled to be published for public comment in Fall 2008.

---

[32] USA PATRIOT Act, 18 USC § 2712, 31 USC § 5318A (2004). and European Commission, *Article 29 Working Party Opinion 5/2006 on the ruling by the European Court of Justice of 30 May 2006 in Joined Cases C-317/04 and C-318/04 on the transmission of Passenger Name Records to the United States*, *available at* http://europa.eu.int. The USA PATRIOT Act, commonly known as the "Patriot Act," is an Act of Congress that United States President George W. Bush signed into law on October 26, 2001. The acronym stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001."

[33] *See* http://attrition.org/dataloss/

[34] European Commission, *Article 29 Working Party Opinion 4/2007 on the Concept of Personal Data*, 01248/07/EN (2007), *available at* http://europa.eu.int.

What are Cross-Border Discovery Conflicts?

Cross-border transfers occur when documents that reside in one country are transported because they are subject to disclosure in another country. For example, when a United States court issues a discovery order that affects electronic data or files stored in France, counsel, clients and courts need to consider questions such as:

- Does jurisdiction exist?
- Is a blocking statute involved?
- What procedural discovery rules govern?
- Is the Hague Convention the exclusive means of cross-border discovery?
- Is personal data involved?
- Who controls the data?
- Is the personal data protected by a privacy law or other directive?
- What analytical test(s) should be applied by courts to determine if discovery can proceed, and the party is entitled to the information they have requested?

These are important and timely questions. In the past, parties often turned to international legal principles in order to answer the above questions.[35] The problem, though, is that these principles were not drafted with ESI in mind. For example, the Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (otherwise known as the "Hague Evidence Convention") is a multilateral treaty that was signed in 1970. The Restatement (First and Second) of Foreign Relations was originally drafted in 1962 and later revised in 1965. The Restatement (Third) of Foreign Relations was published in 1986. Finally, the Restatement (First) Conflict of Laws was originally drafted in 1934 and was later revised in 1971.

The Restatements offer important and valuable guidance on how attorneys and courts need to evaluate conducting discovery abroad. But they do not address the challenges faced in a global society where, for example, the most important piece of evidence may be an electronic file that was created by an employee in Berlin, which now sits on a server in Singapore, and was recently downloaded by a co-worker at a café in Paris. Technology has significantly changed, and the law must keep pace with such change.

What does this mean for business and the practice of law across borders? It means that worldwide, clients, counsel and courts are expected to understand how electronic information is created, stored and retrieved. It means they are expected to know and apply foreign standards and rules procedures for civil discovery. It means they are expected to appreciate and adhere to competing notions of data privacy. These seemingly irreconcilable notions venerate personal privacy as an inalienable human right on the one hand, and on the other reject any expectation of privacy in the workplace.

How does data privacy affect e-discovery in jurisdictions subject to the EU Directive?

One rationale for the distinction between the differing notions of pre-trial discovery or access to information in common law countries and civil jurisdictions is that the civil law regimes have vastly different notions of what is considered personal and private. The European data protection laws have their origins in the European Convention

[35] The Hague Evidence Convention offers optional procedures in the form of minimum standards with which contracting states agree to comply in order to facilitate the taking of evidence abroad. It "does not modify the law of any contracting state [including the Federal Rules of Civil Procedure], require any contracting state to use its procedures either in requesting evidence or in responding to requests, nor compel any contracting state to change its own evidence gathering procedures." *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522, 534 (1987) [hereinafter "A*érospatiale"*]. Under the Convention parties may seek a Letter of Request or Letter Rogatory be sent from the Convention authorities to a foreign court to compel production of evidence. However, this procedure may be "unduly time consuming and expensive, as well as less certain to produce needed evidence than direct use of the Federal Rules." *Id.* at 542.

on Human Rights of 1950 ("ECHR"), which is a treaty of the Council of Europe, Europe's oldest and largest inter-Governmental political institution. Article 8 of the ECHR contains the right to privacy:

> Article 8 – Right to respect for private and family life
>
> 1. Everyone has the right to respect for his private and family life, his home and his correspondence.
>
> 2. There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.[36]

The Council of Europe took its first steps towards data protection laws in the early 1970s.[37] The trigger for the Council's activities at that time was a fear that Article 8 did not cover computer-based data processing operations involving personal data, particularly as computer-based data processing was becoming increasingly prevalent within the private sector.[38] Thus, the Council's first data protection resolutions focused solely on protecting the privacy of personal information contained in public sector and private sector electronic data banks. By the time the Organization for Economic Co-operation and Development's Guidelines were published, however, a new concern regarding the protection of data had emerged; namely, the maintenance of cross-border transfers of personal data.

On October 24, 1995, the European Union's Data Protection Directive was published. Article 1 of the Data Protection Directive states:

> Article 1 – Object of the Directive
>
> 1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.
>
> 2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.[39]

It is important to understand, however, that each European Economic Area ("EEA") Member State has implemented the Data Protection Directive in different ways, and some Member States have chosen to give additional protection to personal data. Accordingly, it will be necessary in each case to consider the effect of the laws of the jurisdiction governing the processing of the personal data in question.

The transfer of personal data to countries outside the EEA is treated differently by the Data Protection Directive, with the starting point being that such transfers are prohibited unless the receiving country provides adequate

---

[36] European Conventional on Human Rights (English), p. 6, *available at* http://www.echr.coe.int/ECHR, under "Basic Texts" (visited August 26, 2008).

[37] *See* Council of Europe, *Resolution 721 (1980) on data processing and the protection of human rights*, available at http://assembly.coe.int/Mainf.asp?link=/Documents/AdoptedText/ta80/ERES721.htm (visited August 26, 2008) (relating the history of data protection activities by the Council of Europe).

[38] Article 8.2 refers to interferences in privacy by public authorities. At the beginning of data protection the Council of Europe concluded that this meant that private sector bodies were not bound by Article 8.1.

[39] *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*, Official Journal L 281, 23/11/1995 P. 0031 – 0050, *available in English at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:HTML (visited August 26, 2008).

protection for privacy. Furthermore, the Data Protection Directive distinguishes transfers of personal data between countries within the EEA from transfers to countries outside the EEA. As mentioned above, within the area of harmonization Member States cannot prohibit or restrict the free flow of personal data between themselves for privacy reasons and this includes transfers for discovery purposes. In distinction, transfers of personal data from the EEA to third countries that do not provide adequate protection for privacy are prohibited, subject to some limited derogations.

EU and European Economic Area

The European Economic Area ("EEA") consists of all 27 EU member states, as well as Norway, Iceland and Liechtenstein. In general, the law of the EEA country where the "data controller" is established will apply to the question of whether the relevant personal data can be legitimately "processed" under the EU Directive and local laws which implement the Directive. Many companies in a corporate group will each be a data controller in respect of certain types of personal data, and if they are established in different countries then many sets of laws may apply.

If the data controller is established outside the EEA then personal data will be subject to the law of the EEA member country where equipment is used to process the data, and not just to transport it. For example, if a company in the USA transfers data to an e-discovery vendor in the UK, then it will be subject to UK local data privacy law.

When a party receives a binding court order compelling disclosure of information to a destination outside the EEA, then it may be possible to successfully argue that both the processing of personal data for the purposes of the transfer, and its export outside the EEA, are "necessary" within the meaning of Article 7(c) or Article 26(d) of the Data Protection Directive. However, the provisions of the national law of the relevant Member State(s) will need to be researched to determine (a) whether any additional safeguards have been put in place by the Member State, and (b) how the provisions of the Directive relating to the "necessity" of processing will be interpreted.

Generally, local counsel in the country where the requested data is located should be consulted to determine whether consent from individual employees, Works Councils or other bodies is necessary before processing or transferring the data. Any processing needed to determine the relevance of the personal data should be done within the EU before any transfer. In suitable cases, such preliminary processing should be conducted in the presence of affected employee(s) to allay any suspicions about unauthorized processing of personal data. In some cases, certification by a notary public may be sufficient to provide evidence that processing has been properly undertaken.

Professionals undertaking data searches commonly conduct key word and date range searches to identify relevant personal data. The main requirement is to take all reasonable measures to ensure that only relevant material is collected, and that neither sensitive personal data (e.g., medical records) nor irrelevant private correspondence are reviewed or transferred outside the EEA.

In-person meetings with many of the privacy commissioners have indicated that these and other "in-country" measures are needed to provide adequate assurance that the scope of the data processing and transfer is proportional -- narrowly tailored to answer the legitimate information need. That is, some concrete actions will likely be needed before the EU or other states with strong data protection regulations will recognize that the "legitimate interests" or "legal requirements" exceptions to such regulations apply to processing and cross-border transfer of electronic information for the purpose, for instance, of US-based discovery.

The EU countries have almost unanimously determined that foreign corporation interests (even US parents of EU subsidiaries) are not enough of a nexus to local concerns to allow for processing and cross-border transfer of such information under the "legitimate interest" or "legal requirements" exceptions. The reasoning of the EU Commissioners is straightforward: if the processing and transfer were permitted every time a US corporate parent or

subsidiary divined a reason to do so for litigation or a regulatory or governmental investigation, these data protection and privacy laws would be trampled.

However, anecdotal evidence suggests that most EU Data Protection Authorities understand that without a proportional way forward, the US Courts will proceed to place US companies in untenable positions of violating EU privacy or violating US court orders—a persistent "catch 22" that serves no one's best interests. If (1) attempts are made to reduce the scope of the processing, to avoid a "fishing expedition;" and (2) if data is handled securely, if a protective order is used, then as noted below, it may be possible to tailor a way forward that would permit the processing of personal information for litigation purposes based on the "legitimate interest" exception to the data privacy regulations.

V. The Legal Landscape: Differing Notions of Discovery

How does discovery differ in civil code versus common law jurisdictions?

Common law jurisdictions generally differ from civil law jurisdictions in terms of overall litigation procedures, and pretrial discovery in particular. At the core of the difference is a fundamental disagreement as to how to most fairly administer justice. Common law jurisdictions contend that the active involvement of individual litigants within an adversarial system is most likely to achieve the fair administration of justice. In contrast, civil code jurisdictions contend that the state, through the active participation of an experienced judiciary is best suited to direct the litigant process in general, and discovery in particular.

Another relevant difference is that common law jurisdictions are based upon the principle of *stare decisis*, or legal precedent. An advantage of this approach is that it ensures the law can respond to cultural change. It also allows for flexible application of the law to the unique facts of a dispute. However, a disadvantage of this system is that it can lack consistency, uniformity and predictability.

In contrast, civil code jurisdictions are very uniform as to litigation procedure, as they are based on statutory law. This offers consistency and predictability, but often at the price of flexibility and adaptability. In addition, as noted above, it elevates the role of the court over private litigants in the discovery process. One rationale is that the state is better suited to respect and protect the privacy of individuals as an inalienable human right. Another rationale is that active court involvement prevents the judicial system from becoming the private refuge of the wealthy, who are the only ones who can afford unfettered pretrial discovery. That is, the state is better able than private litigants to ensure the "just, speedy and inexpensive"[40] administration of justice.

In the discussion that follows as to differing notions of discovery in the cross-border context, the laws of certain specific jurisdictions are highlighted for illustrative purposes only. More detail concerning the general and specific discovery schemes of these and other countries will be included in the "living" companion publication: *The Sedona Conference® Overview of International E-Discovery, Data Privacy and Disclosure Requirements*, which is scheduled to be published for public comment in Fall 2008.

A. Discovery in Common Law Countries

Although globally, civil code systems vastly outnumber common law jurisdictions, the superpower status of certain common law countries has sometimes created a different impression—especially in the minds of such superpowers. Invariably, the scope of permissible pretrial discovery differs dramatically between common law and civil code countries: for the reasons noted above, pre-trial discovery is much more accepted in common law jurisdictions than in civil code countries.

The scope of pretrial discovery in the United States is the most expansive of any common law country. It is the poster child for "full and searching" (and expensive) discovery. United States procedural law—which is primarily governed by the U.S. Federal Rules of Civil Procedure and its state procedural schemes—not only allows discovery of relevant information, but also discovery of information that will lead to the discovery of relevant information. Among the common law jurisdictions including Canada and the United Kingdom, the United States has the most expansive discovery system.

[40] *Cf.* Fed. R. Civ. P. 1 (U.S.) (articulating the same goals).

Specifically, Federal Rule of Civil Procedure 26, as recently amended, requires the parties to disclose certain relevant information "regarding any matter, not privileged" to the other parties, whether in print or electronic form.[41] Amended Rule 34 further allows each party to serve on the opposing party a request to produce additional information that is within the possession, custody or control of the party upon whom the request is served.[42] In short, so long as a litigant's request is reasonably calculated to lead to the discovery of admissible evidence, and does not comprise impracticable demands, a judge is likely to grant a party's request for discovery in a United States court.[43]

The recent amendments to the U.S. Federal Rules of Civil Procedure regarding electronic discovery have resulted in an increased reliance on discovery—often as a tactical sword against a large corporate adversary. And recent U.S. court decisions such as *Qualcomm v. Broadcom Corp.*[44] and *Columbia Pictures v. Bunnell*[45]—where clients as well as legal counsel were sanctioned for incomplete responses to electronic discovery requests—only highlighted the inherent tension between cross-border discovery and data privacy interests.

In addition, common law countries such as the United Kingdom and Canada have adopted liberal electronic discovery rules in their civil procedure rules, much like those in the United States.

United Kingdom

In the United Kingdom, parties must disclose (1) documents relied upon; (2) documents that adversely affect or support his or another party's case; and (3) documents required to produce by a practice direction.[46] In October 2005, the United Kingdom amended its Practice Direction to U.K. Civil Procedures ("Practice Direction") Rule 31 on Disclosure and Inspection. The amendments to this rule broadened the definition of "document" to include "electronic documents, including e-mail and other electronic communications, word processed documents and databases," documents stored on servers and back-up systems, "deleted" documents, and metadata.[47] While the term, "document," is inclusive of most electronically stored information, disclosure is limited to reasonableness.[48] Reasonableness is determined by, among other factors, the number of documents; the complexity of the proceeding; ease, accessibility, expense of retrieving documents; and the documents significance.[49] Under the Practice Direction, parties are encouraged to cooperate and discuss potential issues regarding searches and preservation of electronic documents, inspection methods, and format of documents to be turned over.[50]

Canada

Electronic documents are discoverable in Canada to the same extent as paper, and the discovery process is expansive. Under Canada's Rules of Civil Procedure, parties must disclose and produce "every document relating to any matter in issue in an action that is or has been in the possession, control or power of a party to the action."[51] The term,

---

[41] Fed. R. Civ. P. 26.
[42] *See* Fed. R. Civ. P. 34(a)(1).
[43] *See* M. James Daley & Ken Prine, *One Year After the Federal E-Discovery Amendments*, NATURAL RESOURCES & ENV'T, Vol. 22, No. 4, Spring 2008.
[44] *Qualcomm v. Broadcom Corp.,* 2008 WL 66932 (S.D. Cal. Jan. 7, 2008).
[45] *Columbia Pictures Inc. v. Bunnell*, 245 F.R.D. 443 (C.D. Cal. 2007)**.**
[46] CPR,31.6 (2007) (U.K.).
[47] CPR, PD 31, ¶ 2A.1 (2007) (U.K.).
[48] CPR, PD 31, ¶12A.4 (2007) (U.K.).
[49] *Id.*
[50] CPR, PD 31, ¶ 2A.2, 2A3 (2007) (U.K.)
[51] R. of Civ P 30.02(1)-(2) (2007) (Can.).

"document," is defined to include "data and information in electronic form."[52] Rule 30 provides that relevant electronic documents must be disclosed.

Case law does not detail how parties should store and produce electronic data. Therefore, practitioners should turn to provincial guidelines on procedure, such as the Guidelines for the Discovery of Electronic Documents in Ontario ("Ontario Guidelines") developed in 2005 and the most recent publication from Sedona Conference Working Group 7 ("Sedona Canada") for recommendations regarding the retention, preservation, and production of discoverable electronic documents. One important aspect of the Ontario Guidelines is that, unlike the United Kingdom's Practice Direction, they do not require parties to search for deleted or residual data.[53]

Just as privacy laws inform the way disclosure is handled in the EU, privacy laws affect how discovery must be conducted in Canada. The Personal Information Protection and Electronic Documents Act ("PIPEDA") governs the use of personal data in commercial businesses.[54] Foreign organizations receiving personal information from a Canadian business must comply with PIPEDA. In many ways, it is similar to the EU Privacy Directive. For example, entities must use "contractual or other means to provide a comparable level of protection while the information is being processed by a third-party,"[55] Although consent is usually required to transfer personal information across borders, PIPEDA provides exceptions for particular circumstances.[56]

B. Discovery in Civil Code Countries

Most civil code countries have no formal discovery process. Unlike common law pretrial practice, in which documents and data are discoverable if they are reasonably calculated to lead to admissible evidence, many civil law jurisdictions prohibit disclosure of evidence beyond what is needed for the scope of the trial.[57]

For example, the French system restricts disclosure to only those documents that are admissible at trial.[58] Further, document disclosure is supervised by the judge, who decides on the relevance and admissibility of the evidence proposed by parties.[59]

In Germany, litigants are not required to disclose documents to the other party. Instead, the parties need only produce those documents that will support its claims. These documents must be authentic, original, and certified, but the party seeking the document must appeal to the court to order the production of the document. Such appeal must be specific in the description of the document and must include the facts the document would prove and the justification for having the document produced.[60] If the document is in the possession of a third party, the document seeker must obtain permission from the third party. Otherwise, the seeker must commence proceedings against the holder of the documents.[61]

---

[52] R. of Civ. P 30.01(1)(a) (2007) (Can.).
[53] *Compare* Task Force on the Discovery Process in Ontario, Guidelines for the Discovery of Electronic Documents in Ontario, October 2005, at 11, *available at* http://www.commonwealthlegal.com/pdf/E-DiscoveryGuidelinesOct2005.pdf *with* CPR, PD 31, ¶ 1.2A1 (2007) (U.K.).
[54] Personal Information Protection and Electronic Documents Act, 2000 S.C., ch. 5 (Can.).
[55] *Id.* at Part 5, Schedule 1, Clause 4.2 .
[56] *Id.* at Div. 1, para 7(3)(a) .
[57] *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 442 cmt. a (1987) (stating that "[g]iven the difficulty in obtaining compliance, and the resistance of foreign states to discovery demands originating in the United States, it is ordinarily reasonable to limit foreign discovery to information necessary to the action. . . . Requests for admission for information that could lead to admissible evidence would not ordinarily be granted under this standard. . .").
[58] *See* Cynthia Day Wallace, *'Extraterritorial' Discovery: Ongoing Challenges for Antitrust Litigation in an Environment of Global Investment*, 5 J. INT'L ECON. L. 353, 365 (2002).
[59] *See id.*
[60] Zivilprozeßordnung [ZPO][German Civil Procedure Code] Oct. 1, 1879, Bundesgesetzblatt [BGBl] I P. 3202, as amended, § 424.
[61] *Id.*

C. The Impact of The Hague Convention and Blocking Statutes

What is The Hague Convention?

Several countries attempt to somewhat restrict common law-style pretrial discovery through Article 23 of the Hague Evidence Convention.[62] Very briefly, the Hague Convention instituted a uniform procedure for the issuance of "letters of request" (a/k/a "letters rogatory"). Letters of request are petitions from a court in one nation to a designated central authority in another, requesting assistance from that authority in obtaining relevant information located within its borders.[63] Even if a litigant requests information located abroad via a letter of request directed to the proper agency, there is no guarantee that the request will be honored. A State may ignore or deny such a request if it "considers that its sovereignty of security would be prejudiced" by executing the request.[64] In addition, a State may deny such a request if it believes it is restricted by the States' law of privilege, or a pertinent statute that "blocks" such requests.

In addition, Article 23 of the Hague Evidence Convention presents an even greater obstacle. Under this article, "a contracting State may at the time of signature, ratification or accession, declare that it will not execute letters of request issued for the purpose of obtaining pretrial discovery of documents known in common law countries.[65] Many signatory States, including France, Germany, Italy and Spain have filed such reservations under Article 23. This creates a situation where such States have declared that they will not allow discovery of any information, regardless of relevance, if the information is sought in relation to a foreign proceeding.[66]

As discussed in more detail below, U.S. courts have generally rejected the interests of civil law jurisdictions in protecting their data from U.S.-based discovery. In *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*, the United State District Court for the Northern District of Illinois held that the Federal Rules should apply despite Italy's express declaration against the "obtaining [of] pre-trial discovery of documents as known in Common law countries."[67] In *United States v. Vetco,*[68] the Ninth Circuit upheld a sanction against Vetco for not complying with an IRS summons, despite its argument that this would violate Swiss banking secrecy law. Similarly, in *Enron v. J.P. Morgan Securities Inc.*,[69] the Bankruptcy Court held that the threat of the French blocking statute did not warrant the invocation of the Hague Convention. Nor was the Hague Convention recognized as the exclusive means of discovery in *Columbia Pictures Industries v. Bunnell.*[70]

However, the District Court of Minnesota in the *In re Baycol Products Litigation* case held that the Italian courts should be afforded the opportunity to decide whether it would refuse letter requests since many countries have modified their Article 23 declarations to apply only to irrelevant requests that lack sufficient specificity.[71]

---

[62] Hague Evidence Convention on the Taking of Evidence Abroad in Civil or Commercial Matters, Mar. 18, 1970, 23 U.S.T. 2555, T.I.A.S. No. 7444, 847 U.N.T.S. 231 (1972) [hereinafter Hague Evidence Convention}.
[63] *See* Lowenfeld, *International Litigation and Arbitration*, 874 (West Group 2002).
[64] Hague Evidence Convention, Art. 12.,
[65] Hague Evidence Convention, Art. 23.
[66] *See* Soiret, *The Foreign Defendant: Overview of Principles Governing Jurisdiction, Venue, Extraterritorial Service of Process and Extraterritorial Discovery in U.S. Courts*, 28 TORT & INS. L.J. 533 (1993).
[67] *Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L.*, 2005 U.S. Dist. LEXIS 20049, at *14 (N.D. Ill. Sept. 12, 2005).
[68] *See United States v. Vetco*, 691 F.2d 1281 (9th Cir. 1981).
[69] *Enron v. J.P. Morgan Secur. Inc.*, No. 01-16034 (Bankr. S.D.N.Y. July 18, 2007).
[70] *Columbia Pictures Inc. v. Bunnell*, ; 245 F.R.D. 443 (C.D. Cal. 2007). *See also*, *Reino de Espana v. Am. Bureau of Shipping*, 2006 WL 3208579 (S.D.N.Y. Nov. 3, 2006); 2005 U.S. Dist. Lexis 15685 (S.D.N.Y. 2005).
[71] *In re Baycol Products Litigation*, 348 F.Supp.2d 1058 (D. Minn. 2004).

Blocking Statutes: Shields For Nationally Sensitive Data: Traps For Unwary Litigants; Conundrums For Courts

Some countries – mostly civil law jurisdictions, but also a few common law countries such as Australia– attempt to restrict cross-border discovery of information intended for disclosure in foreign jurisdictions by means of blocking statutes. These provisions are not at all uniform--either in origin, intent or effect. They have arisen in a variety of eras and contexts, and generally have been promulgated in an effort to protect the sovereignty, as well as commercial interests of particular states. Some prohibit the disclosure, copying, inspection or removal of documents from a specific country.[72] Others are designed to protect commercial interests of the citizens from cross-border interference by other States, such as in the case of U.S. Antitrust, SEC, and similar foreign regulations.[73]

Blocking statutes are frequently invoked in motions for protective orders with regard to discovery requests that would require cross-border transfer of electronic information. A party who discloses such information, even as part of a required investigation, may be guilty of violating blocking statutes of the country from which the data was released. Violations of some of these statutes may result in civil or criminal penalties.

A number of civil law countries have also enacted blocking statutes, as a consequence of the Hague Evidence Convention, to prevent the broad reach of discovery from the United States. For example, in 1980 France specifically enacted a section of its penal law that criminalizes discovery within France by private parties for litigation abroad. French Penal Law No. 80-538 provides:

> Subject to international treaties or agreements and laws and regulations in force, it is forbidden for any person to request, seek or communicate, in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature leading to the constitution of evidence with a view to foreign judicial or administrative procedures or in the context of such procedures.[74]

Switzerland

Another form of blocking statute proscribes specific types of information from disclosure to foreign authorities. Switzerland has enacted the Swiss Banking Act, which makes criminal the divulging of banking secrets, protects the financial assets of depositors from foreign governments. Article 47 states that "Whoever divulges a secret entrusted to him or of which he has become aware in his capacity as officer, employee, mandatory, liquidator or commissioner of a bank, as representative of the Banking Commission, officer or employee of a recognized auditing company and whoever tries to induce others to violate professional secrecy shall be punished by imprisonment for not more than six months or by a fine of not more than SFr. 50,000."[75] Further, Article 271 of the Swiss Penal Code prohibits the gathering of evidence in Switzerland for use in a foreign proceeding unless done through judicial assistance.[76] Article 273 of the Swiss Penal Code "may likewise have the effect of a blocking statute" as it prohibits "disclosing business

[72] For example, Germany, France, Switzerland and China have laws referenced as "blocking statutes" or "state/bank secrecy laws, as discussed below."
[73] *See* Business Records Protection Act, 1950 R.S.O., ch. 54 (Can.) (enacting the blocking statute in response to a1947 investigation by the U.S. of the Canadian newsprint industry).
[74] Section 1134 of the civil code, section 111-4 of the criminal code, 1bis of the law n° 68-678 dated July 26th, 1968 amended by the law n° 80-538 dated July 16th, 1980.
[75] Swiss Federal Banking Act of Nov. 8, 1934, Art. 47. *See also* Strafgesetzbuch [StGB] [Penal Code] Art. 273 (Switz.) (stating that revealing business secrets to foreign officials is a crime); *Société Internationale pour Participations Industrielles Et Commerciales, S. A. v. Rogers*, 357 U.S. 197, 200 (1958).
[76] *See e.g.*, the Hague Convention.

secrets of third parties residing in Switzerland to foreign states and foreign entities" (including affiliates and parent companies)[77]

China

China has a State Secrecy Law that has been raised in at least one case to prevent disclosure of information from abroad. In *Richmark Corp. v. Timber Falling Consultants*, the Ninth Circuit upheld a U.S. District Court sanction against a corporation from the People's Republic of China ("PRC") for failure to comply with discovery orders.[78] In that case, the plaintiff demanded discovery of the worldwide assets of a Chinese corporation. However, the corporation argued that the PRC's State Secrecy Laws prevented it from disclosing such information as the Ever Bright Group, an arm of the State Council, had deemed it a state secret. Disclosure of such information would subject the corporation to criminal prosecution.[79] The Ninth Circuit, however, held that the PRC's law would not excuse the corporation's failure to comply with the discovery orders.

United Kingdom

The United Kingdom allows discovery of documents unless an authority specifically precludes it.[80] Its provision does not impose a blanket block, but empowers the government to give directions in specific or general instances where the United Kingdom's trading interests appear to require it. An English court may refuse to assist a foreign court in obtaining evidence in instances where the request for production would infringe the United Kingdom's sovereignty.[81] An example of this is the general direction, issued by the British Secretary of State in 1984, to prohibit any person in the United Kingdom from complying with the United States District Court of the District of Columbia's order to produce commercial documents located in the nation for a civil anti-trust case against a United Kingdom airline.[82]

Australia

Australia has enacted similar blocking statutes as the United Kingdom, including: Foreign Proceedings (Prohibition of Certain Evidence) Act 1979, Foreign Antitrust Judgments (Restriction of Enforcement) Act 1979, and Foreign Proceedings (Excess of Jurisdiction) Act 1984.[83] Under the 1984 Act, which superseded and combined the 1976 and 1979 Acts, the Australian Commonwealth Attorney General may prohibit compliance with foreign discovery orders and judgments in foreign antitrust proceedings when Australian sovereignty is infringed or where the foreign court asserts jurisdiction which is considered to be contrary to international law or inconsistent with "international comity or international practice." [84]

---

[77] *See* David Rosenthal, *E-Discovery in Switzerland: How to Deal with DP Restrictions*, PRIVACY LAWS & BUSINESS INTERNATIONAL NEWSLETTER, October 2007.
[78] *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468 (9th Cir. 1992).
[79] *Id.* at 1474.
[80] United Kingdom's Protection of Trading Interests Act, 1980, ch. 11, § 2.
[81] *Id.* at § 2(2).
[82] House of Commons Hansard Debates for 12 Mar 1993.
[83] Foreign Proceedings (Excess of Jurisdiction) Act 1984 No. 3, 1984 (Mar. 21, 2004), *available at* http://www.comlaw.gov.au/comlaw/management.nsf/lookupindexpagesbyid/IP200403254?OpenDocument
[84] Foreign Proceedings (excess of Jurisdiction) Act 1984, s. 6.

South Africa

South Africa has also adopted provisions that prohibit the removal of documents or data unless permission is obtained. For example, its Protection of Business Act of 1978 specifically bars the disclosure of business operation information to foreign jurisdictions unless the Minister of Industries, Commerce and Consumer Affairs allows it.[85]

Canada

Canada adopted the Foreign Extraterritorial Measures Act in 1985.[86] This Act allows the government to restrict the "production of records" in instances in which a foreign court would infringe Canadian interests or sovereignty. The Canadian province of Quebec has enacted a blocking statute with respect to business documents in anti-trust litigation. For example, the Quebec Business Concerns Records Act prohibits the "removal from the province of documents of business concerns in Quebec that are required pursuant to judicial processes outside the province."[87] It was enacted to prevent the intrusion of U.S. courts in anti-trust actions and "other forms of foreign judicial interference."[88]

Is there any real threat of criminal enforcement of blocking statutes?

Until recently, as described below, there had not been any reported instances of any country invoking the criminal portion of their blocking statutes against parties asked to comply with an order for production of documents made by a foreign court. As such, blocking statues are sometimes viewed as being applied *in terrorem* as a point for negotiation rather than as a threat likely to come to pass. For example, in the *Heidberg* case, the court found that "where there was no evidence that any person had ever been prosecuted for breach of [the French blocking statute]," it was unreasonable for a litigant to fear prosecution under the statute for disclosing information that was protected under the statute.[89]

While the court in *Heidberg* noted that blocking statutes are enacted merely to strike fear into litigants and thus rarely enforced, practice may well dictate otherwise. French parties can indeed face criminal sanctions for disclosure of evidence in foreign proceedings, but, because much of the proceedings are cloaked with grand jury-like confidentiality, there are few records of the enforcement taking place and no published judicial decisions.[90]

Yet potential criminal sanctions, real or perceived, associated with blocking provisions can severely limit on access to and dissemination of corporate records. In *Lyondell-Citgo Refining, LP v. Petroleos de Venezuela, S.A.*, rather than violate Venezuela's Special Law Against Information Systems Crimes and face stiff criminal sanctions, the defendant, national oil company of Venezuela, refused to turn over its board meeting minutes and related documents to the plaintiff.[91]

The defendant submitted letters from the Venezuelan Minister of Mines explaining that the requested materials included classified and national security information.[92] However, the court held that the defendant had not provided specific reasons for asserting confidentiality or executive privilege and ordered defendant to turn over the documents. Rather than face the penalties associated with the disclosure of classified information, the defendant declined to

[85] Protection of Business Act, 1978 (Act No. 99 of 1978). (S. Afr.)
[86] Foreign Extraterritorial Measures Act, R.S.C., ch. F-29 (1985) (Can.).
[87] *Hunt v. T&N plc*, [1993] 4 S.C.R. 289. (Can)
[88] *Id.*
[89] *Heidberg v. Grosvenor*, [1993] Q. B, 324, 325 (U.K.).
[90] *But see Strauss v. Credit Lyonnais, S.A.,* 242 F.R.D. 199 (E.D.N.Y. May 25, 2007), discussed supra.
[91] *Lyondell-Citgo Refining, LP v. Petroleos de Venezuela, S.A*, 2005 WL 1026461 (S.D.N.Y. 2005).
[92] *See Lyondell-Citgo Refining, LP v. Petroleos de Venezuela, S.A*, 2005 WL 356808 at *3 (S.D.N.Y. 2005).

produce the data and accepted an adverse inference instruction from the magistrate judge in the Southern District of New York[93]

While it is unclear whether a corporation has ever been sanctioned for violation of Venezuela's Information Systems law, the threat--whether real or perceived--dictates how litigants respond to discovery requests. Switzerland, like Venezuela, holds out the prospect of strict enforcement as a means of compliance with its banking laws.[94]

Recent French Blocking Statute Conviction

On January 16, 2008, the Criminal Chamber of the French Supreme Court upheld a December 12, 2007 conviction and sentence of a French lawyer for violating the French Blocking Statute,[95] which prohibits "requesting, seeking, or disclosing in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature for the purposes of constituting evidence in view of foreign judicial or administrative proceedings."[96] Under this provision, a violation is punishable by six months in prison and/or a €18,000 fine). The French lawyer in question was fined €10,000, or about $15,000 US. This decision may alter the perception of U.S. courts as to the reality of enforcement of such statutes.

Some context for this decision is helpful. The events arose from decade-long dispute in a federal district court in California known as "The Executive Life Litigation." The California Insurance Commissioner alleged that the State had been defrauded by the Paris-based insurance company, MAAF, and other defendants into allowing the sale of the insurance business of Executive Life Insurance Company to foreign government-controlled banking interests in violation of California law. [97] The French attorney designated "Christopher X" by the court was alleged to have called a former Director of MAAF, identified as "Jean-Claude Y, " and stated, for the purpose of obtaining information by which the State could decide to call the former Director as a witness, that the Directors of MAAF had not been informed about the decision to purchase Executive Life, and that this decision had "been made in the hallways."[98] Jean-Claude Y denied the allegation, and MAAF filed a criminal complaint alleging a violation of the blocking statute; that is, that the statement was "a lie to get at the truth," as the court held, and thus was an attempt to elicit commercial information for the purpose of creating or facilitating evidence for use in a foreign judicial proceeding.[99] Christopher X was convicted and, upon appeal, contended that he did not, in fact, solicit information but, rather, approached Jean Claude Y to obtain consent for his testimony, and that Jean Claude Y's statement was given spontaneously. The court rejected these arguments, noting that Christopher X had "not approached the witness in a neutral manner so that his testimony could have been obtained in accordance with the requirements of the Hague Convention, but instead attempted to identify Jean-Claude Y as a witness for the plaintiff and to influence his questioning at trial.[100]

Prior to this case -- the first reported decision of a criminal conviction under France's blocking statute -- French defendants in *Straus v. Credit Lyonais* [101] cited the French blocking statute in motions for protective orders to limit discovery. The case was brought under the Terrorism Act of 1992, which permits citizens to sue as victims of

---

[93] *See Lyondell-Citgo Refining, supra* n. 90.
[94] Bonnie H. Weinstein, Diane Henkels, *International Legal Developments in Review: 2002*, 37 INT'L LAW. 389, 393 (2003) (stating that Switzerland refused to surrender to the European Union's pressure to "loosen the strict enforcement of its centuries old bank secrecy and non-disclosure laws").
[95] *In re Advocat "Christopher X"*, Cour de Cassation, French Supreme Court, December 12, 2007, Appeal n 07-83228 (English Translation).
[96] French Penal Law No. 80-538 (July 16, 1980).
[97] See Generally *Garamendi, et. al. v. Altus Finance, et. al,*2005 WL 3977994 (C.D.Ca.) .
[98] *In re Advocat "Christopher X"*, Cour de Cassation, French Supreme Court, December 12, 2007, Appeal n 07-83228 (English translation).
[99] *Id.*
[100] *Id.*
[101] 242 F.R.D. 199 (E.D.N.Y May 25, 2007)

terrorism and receive treble damages. The plaintiffs contended that the bank maintained records of a Hamas-related charity that was allegedly a front for terrorism. They sought access to bank records reflecting the accounts of the alleged charity, among other records. The U.S. court rejected the blocking statute as a basis for preclusion of the disclosure. It cited, as its principal point of analysis, the Restatement (Third) of Foreign Relations Law of the United States, § 442. Under that Section, a court may order a person subject to its jurisdiction to produce evidence even if the information is located outside the United States. Citing *Aerospatiale* and the Restatement, the court held that five factors need to be considered in determining whether to order disclosure:

> (1) the importance to the . . . litigation of the documents or other information requested;
> (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 compliance with the request would undermine the important interests of the state where the information is located.[102]

Citing *Minpeco*,[103] the court also considered two other factors: (1) The hardship of compliance on the party or witness from whom the discovery is sought, and (2) The good faith of the party resisting discovery.[104] The court held that the documents were crucial to the litigation, that the requests were narrowly tailored, and that the plaintiffs need not exhaust their remedies through the Hague Convention prior to recovering the documents. The court further concluded that the U.S. and France have a mutual interest in combating terrorism. Moreover, it rejected Credit Lyonnais' argument that it would face possible prosecution by French banking authorities, holding that there was, in fact, a low likelihood of actual prosecution. The court ordered the defendants to disclose records relating to the case within 30 days.[105]

While one cannot say with certainty that the decision in *Straus* would differ had it come after the *Christopher X* matter, the significance of this French decision is that it suggests that U.S. litigants and third parties have a criminal conviction to show U.S. courts that France does, indeed, enforce its blocking statute. Litigants in seeking cross-border discovery may, therefore, be well advised to reconsider the efficacy of using the Hague Convention as a means of discovery abroad.

[102] *Id.* at 210.
[103] *Supra* note 121.
[104] *Strauss*, 242 F.R.D. at 210-211.
[105] *Id. at* 228.

VI. The General Contours of Cross-Border Discovery Conflicts:

How Have Courts Addressed Cross Border Discovery Conflicts?

The landscape of cross-border discovery disputes is littered with judicial decisions holding that the discovery procedures of the presiding court control the litigation, regardless of the foreign domicile of one or more of the parties. And it is not just United States courts. For example, the Commercial Court of the Queen's Bench Division in *The Heidberg* stated "all matters of procedure are governed by the domestic law of the country to which the Court wherein any legal proceedings are taken belongs…."[106] In *Mackinnon v. Donaldson,* Justice Hoffmann indicated he was not concerned "with the discovery required by [Rules of the Supreme Court, Ordinance] 24 from ordinary parties to English litigation who happen to be foreigners. If you join the game you must play according to the local rules. . ."[107]

Some of the most urgent cross-border discovery issues giving rise to conflicts include:

1. Obtaining consents for the processing and transfer of personal data;
2. Ensuring the integrity and security of the collection of person data, and its handling and production;
3. Ensuring that the amount of personal data collected and the extent of its use in litigation is proportional to the actual issues in legitimate controversy, and not frivolous lawsuits;
4. Complying with cross-border data transfer rules to ensure the absence of unauthorized onward transfer or use of personal data.

[106] *Heidberg v. Grosvenor* , [1993] Q.B. 324, 325 (U.K.)
[107] *Mackinnon v. Donaldson,* [1986] Ch 482, 494. *See also Reino de Espana v. Am. Bureau of Shipping*, 2006 WL 3208579 (S.D.N.Y. Nov. 3, 2006); 2005 U.S. Dist. Lexis 15685 (S.D.N.Y. 2005).

How does the doctrine of "playing according to local rules" apply?

This guideline of playing by the local rules may lead a court to insist upon application of its own rules of procedure, even where an alternative procedure is available, as under the Hague Convention.[108] For instance, in *Morris v. Banque Arabe et Internationale D'Investissement*, the English High Court stated that where litigation was in the English Court and an order for inspection was made to a foreign party under English Civil Procedure Rules "the forum state had a legitimate interest in the conduct of its own judicial proceedings which should not be undermined by the encroachment of foreign law" although an opposing party's position could be taken into consideration by the English court in determining whether an order for inspection should stand.[109]

Likewise, litigation commenced in a United States forum found to have jurisdiction over the parties is guided by the U.S. Federal Rules of Civil Procedure ("FRCP") regardless of the countries of residence of the parties or the location of discoverable documents.[110] However, foreign law may be considered and certain limitations applied. For example, the FRCP may not be construed to authorize dismissal where failure to comply with a discovery order has been shown not to be due to "willfulness, bad faith, or any fault of petitioner" but rather where "the very fact of compliance by disclosure…will itself constitute the initial violation…." of domestic law.[111]

Yet, in *Aérospatiale,* the U.S. Supreme Court held that courts in the United States were not bound to utilize the Hague Convention, and that the convention did not preempt the FRCP with respect to discovery from foreign litigants. The court further described Hague Convention procedures as optional supplementary measures that did not need to be used where they would be "unduly time consuming and expensive, as well as less certain to produce needed evidence than direct use of the FRCP."[112] To determine whether to use the Federal Rules or the Convention, the Court in *Aerospatiale* considered: "(1) the intrusiveness of the discovery requests given the facts of the particular case, (2) the Sovereign interests involved and, (3) the likelihood that resort to the Convention would be an effective discovery device."[113]

Applying this analysis, the court in *Bodner v. Paribas*[114]declined to apply the Hague Convention to resolve a discovery conflict involving a French blocking statute. The court found the French blocking statute did not stand in the way of disclosure because discovery was limited in scope, the U.S. had significant interest in the outcome (return of money and assets to U.S. plaintiffs allegedly taken wrongfully by French banks during World War II) and the national interests of France in withholding the documents did not compel use of the blocking statute.

---

[108] *Morris v. Banque Arabe et Internationale D'Investissement* I.L.Pr. 37 at H6 (2001) (arguing success was not guaranteed under the Convention and defendant had not been cooperative in taking necessary steps.).
[109] *Id.* at H5.
[110] *Dietrich v. Bauer,* No. 95 Civ. 7051(RWS), 2000 WL 1171132 at *2 (S.D.N.Y. Aug. 16, 2000) ("the test for production of documents is control, not locations." (quoting *Marc Rich & Co., A.G. v. United States*, 707 F.2d 663, 667 (2d Cir. 1983)). *See also Reino de Espana,* 2007 WL 1686327 (S.D.N.Y. 2007).
[111] *Societe Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers,* 357 U.S. 197, 211 (1958) (Note: distinction is made between Swiss laws that carry criminal monetary and incarceration penalties against the disclosing party and are likely to be enforced as opposed to French Blocking Statutes for which the risk of criminal conviction is so low it "can't be seriously argued in good faith" and "no evidence [exists] that any person has ever been prosecuted for breach of Art. 1 bis." *Heidberg v. Grosvenor*, [1993] Q.B. 324, 332 (U.K.))*But see supra n*. 64, regarding confidentiality of French proceedings to enforce its blocking statute.
[112] *Aerospatiale,* 482 U.S. 522, 544 (1987) (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 442(1)(c) (1987) (In deciding whether to issue an order directing production of information located abroad, and in framing such an order, a court or agency in the United States should take into account the importance to the investigation or litigation of the documents or other information requested; the degree of specificity of the request; whether the information originated in the United States; the availability of alternative means of securing the information; and the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.)
[113] *In re Aircrash Disaster Near Roselawn, Indiana*, 172 F.R.D. 295, 309 (N.D. Ill. 1997). (citations omitted)
[114] *Bodner v. Paribas*, 202 F.R.D. 370,375 (N.D. Ill. 2000).

Some American courts have opted to chart a middle course. In *In re: Vitamins Antitrust Litigation*, the court upheld a Special Master's recommendation that merits discovery should proceed under the Federal Rules of Civil Procedures rather than under the Hague Convention,[115] but limited discovery by granting defendants' request to file a privacy log of documents protected from discovery by Swiss and German defendants' domestic privacy laws.[116] Plaintiffs were then given the chance to determine if the requested information was absolutely essential to their case or if there was a way to amend a protective order to safeguard defendants from liability in the production of this information.[117] Thus, production of the data rested on a balance of the relevance and harm to plaintiffs in not having this information against the burden and intrusiveness on defendants of requiring this discovery.[118]

In other circumstances, courts have been persuaded that the threat of criminal sanctions is real, and this has tipped the balance. In *Société Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers*[119] the court held that dismissal of the case was not justified where the plaintiff Swiss bank failed to comply with pretrial production, in that its failure was "not due to inability fostered by its own conduct or by circumstances within its control but because production of documents might violate Swiss laws…" that included criminal penalties (monetary and possible incarceration) and where plaintiff had shown good faith by attempting "all which a reasonable man would have undertaken in the circumstances to comply with the order."[120]

Since *Rogers*, courts have evaluated requests for production of documents from a foreign entity in light of good faith efforts by the respondent under a standard of reasonableness.[121] Increasingly, perhaps as a consequences of the increasing globalization of business and the frequency with which these issues arise, cross-border discovery matters, these cases turn on their facts rather than preconceived notions of the whether the local discovery scheme should prevail.[122]

Attempts to harmonize notions of discovery and national interests have been extant since *Aerospatiale* in which the Supreme Court endorsed the five factor test from the Restatement, holding that it should, in fact, be applied before a court decides whether or not to compel production from a foreign source. This court found the test "relevant to any comity analysis" and identified it as being "perfectly appropriate for courts to use when no treaty has been negotiated to accommodate the different legal systems. It would also be appropriate if the [Hague] Convention failed to resolve the conflict.…"[123]

The court in *Minpeco v. Conticommodity Services, Inc.* decided two weeks after *Aerospatiale*, did not cite directly to the Restatement (Third) balancing factors but it identified three additional factors to consider:

1. The competing interest of the nations whose laws are in conflict;
2. The hardship of compliance on the party from whom discovery is sought;
3. The importance to the litigation of the information and documents requested.[124]

---

[115] *See In Re Vitamins Antitrust Litigation*, No. 99-197TFH, 2001 WL 1049433 (D.D.C. June 20, 2001) (citing balancing factors from *Aerospatiale*, 482 U.S. at 544).
[116] *See id*. at *1
[117] *See id.* at *9.
[118] *See id.* at *14.
[119] *Société Internationale Pour Participations Industrielles et Commerciales, S.A. v. Rogers,* 357 U.S. 197 (1958).
[120] *Id.* at 201.
[121] *See id*; *Bodner v. Paribas,* 202 F.R.D. 370, 374 (E.D.N.Y. 2000) (citing *Aérospatiale* 482 U.S. at 545-46: "The exact line between reasonableness and unreasonableness in each case must be drawn by the trial court, based on its knowledge of the case and of the claims and interests of the parties and the governments whose statutes and policies they invoke.").
[122] *See U.S. v. First National City Bank,* 396 F.2d 897, 901 (2d Cir. 1968); *In re Vitamins Antitrust Litigation*, No. 99-197TFH, 2001 WL 1049433 at *14 (D.D.C. June 20, 2001) (Burden of discovery on the foreign producer is to be evaluated in the context of the court's "knowledge of the case and claims and interests of the parties and the governments whose statutes and policies they invoke." (citing *Aérospatiale* 482 U.S. at 546)).
[123] *See Aerospatiale,* 482 U.S. at 544.
[124] *Minpeco, S.A. v. Conticommodity Servs., Inc.*, 116 F.R.D 517, 522 (S.D.N.Y. 1987).

Application of these factors let the Texas Supreme Court in *Volkswagen, A.G., Relator v. Valdez* to hold, in a case where Texas discovery rules conflicted with the German Federal Data Protection Act, that information held by the German parent company of the U.S. subsidiary party should not be produced. In overruling the trial court's denial of a writ of mandamus to protect personal data from discovery, the Texas court held that the trial court failed to balance the competing interests of the parties including relevant German law.

A few courts, a minority to be sure, have held that parties must first utilize the procedures under the Hague Convention before resorting to the Federal Rules. In *Husa v. Laboratoires Servier SA*, the New Jersey court held in a personal injury claim against a French pharmaceutical company that the "Convention should be utilized unless it is demonstrated that its use will substantially impair the search for truth, which is at the heart of all litigation, or will cause unduly prejudicial delay."[125]

Some federal courts have also held that the Hague Evidence Convention should be used. *In re Perrier Bottled Water Litigation* involved the application of the *Aerospatiale* in a product liability action against a French company. The Connecticut District Court held that the Convention should be applied because the discovery requests were (1) intrusive and not narrowly tailored to target material information; (2) the Federal Rules would breach French sovereignty; and (3) the Convention's procedures would not prove ineffective.[126]

While *Husa* and *In Re Perrier* are minority holdings, the recent decision of the French Supreme Court that affirmed the conviction of a French attorney for violating the French blocking statute in the context of discovery relating to the *Strauss v. Credit Lyonnais* case may, in appropriate cases, tip the balance applied by courts in favor of playing to rules of the jurisdictions from which the data is sought.

[125] *Husa v. Laboratoires Servier SA*, 326 N.J. Super. 150, 156 (App. Div. 1999).
[126] *See In re Perrier Bottled Water Litig.*, 138 F.R.D. 348 (D. Conn. 1991).

VII. Trends and Future Directions

"Catch-22" Revisited

The most prevalent recent trend is to restrict cross-border discovery through the application of blocking statutes and data privacy regulations. The recently published decision of the French Supreme Court affirming the criminal conviction of a French attorney for violating the French Blocking Statute casts in doubt a great deal of U.S. case law precedent on the issue of cross-border discovery. Prior U.S. court decisions ordering cross-border discovery over the objections such discovery violates foreign blocking statutes is expressly premised on the heretofore absence of any **public** enforcement of such statutes.

Historically, the attitude of the U.S. Supreme Court and U.S. federal and state courts at all levels has been that the threat of such prosecution is, in reality, just a minor factor in the type of proportionality analysis called for by the Restatements of Law. The U.S. courts in these cases almost uniformly reason that in the absence of enforcement of foreign blocking statutes, the Hague Convention cannot be considered the exclusive means of cross-border discovery. This is, if blocking statutes have teeth but no bite, then cross-border discovery should be ordered, albeit with some restrictions based upon the type of case, and uniqueness and relevance of the information sought.

Indeed, U.S. courts inferred that the real intent of blocking statutes was just to ensure an arms-length negotiation leading to an outcome that respects and recognizes legitimate data privacy concerns. Certainly, prior reported decisions clearly articulate the belief that under principles of comity, a foreign state would allow a balancing of relevant litigation and privacy interests.

The recent French blocking statute conviction now suggests that parties should consider, more thoughtfully than ever, whether they should resort in the first instance to the Hague Convention. Certainly, prior precedent that held that the Hague Convention is not the exclusive means of obtaining cross-border discovery is now squarely in doubt, at least in France. The circumstances of publication of the French decision almost one year later, and its grand jury-like proceedings begs the question whether there have been prior such unpublished decisions.

Now that the logical syllogism upon which prior U.S. case law is based is broken, the stage is set for U.S. Courts to reconsider whether the Hague Convention procedures are indeed the exclusive means of cross-border discovery, at least in France. And it suggests that parties should more thoughtfully than ever weigh the civil and criminal consequences in their jurisdictions of not conducting relevant cross-border discovery with the civil and criminal consequences in other jurisdictions. The stakes of this "Catch-22" are higher than ever before. And the situation cries out for a collaborative framework in which cross-border legal disputes can effectively be resolved.

Global Trend toward Increased Data Privacy and Protection

Even in countries like the United States—which historically has placed commercial marketing and national defense interests ahead of data privacy concerns—information privacy is experiencing a renaissance. This has been in large part fueled by a consumer backlash against the unrestricted sale and use of personal data for marketing purposes. The flood of information security breaches of large private and public databases of personal information has brought these concerns into focus. And the increase in the frequency and severity of identity theft from such breaches and others has energized the global privacy movement, and its advocates in the United States.

The above framework, combined with appropriate use of unambiguous consents, Safe Harbor registration, Model contract provisions and Corporate Binding Rules can help ameliorate, but not entirely remove this "Hobson's choice." Rather, additional proactive steps can be taken to help reduce legal risk, time and cost of cross-border

discovery, and the private sector has played a significant role in this regard. For example, Eli Lilly, a U.S. based, publicly traded pharmaceutical corporation with operations in 50 countries, is forging a dialogue with the Data Commissioners throughout the European Union. Some of these steps include:

1. Engaging in dialogue with the Data Protection Authorities (DPAs) and focusing on common interests in the free flow of data for commercial and judicial purposes;

2. Developing a uniform confidentiality designation and legend, such as EU Confidential for any personal data involved in cross-border discovery;

3. Exploring EU-approved training for those involved in the investigation, collection, filtering, review and production of EU Confidential data;

4. Developing specific EU provisions for federal and state protective orders and for Case Management Orders; such provisions would restrict further transfer of such data, and otherwise provide additional procedural protections against unauthorized disclosure, alteration, use or retention of such data, beyond its specified purpose or time. They would also allow the data owner access to inspect the data, and would require certified destruction or return of personal data when the specified purpose was fulfilled;

5. Add cross-border discovery training to Federal Judicial Center's curriculum;

6. Invite the participation of Data Protection Officials to partake in collaborative dialogue through such groups as WG6, and particularly in conferences such as the Annual WG6 Conference in The Hague in September 2008;

7. Develop EU approved protocols and processes for pre-filtering of personal data in the host country to ensure that only relevant personal data is transferred for cross-border discovery purposes.

VIII. A Potential Way Forward

Ideally, determining the scope of cross-border discovery obligations should be based on a balancing of the needs, costs and burdens of the discovery with the interests of each jurisdiction in protecting the privacy rights and welfare of its citizens. The following factors should be considered in this balancing:

1. The nature of the data privacy obligations in the jurisdiction where the information is located;

2. The obligations of the responding party to preserve and produce relevant information in the jurisdiction where the dispute is filed and the jurisdiction where the data is located;

3. The purpose and degree of custody and control of the responding party over maintaining the requested information;

4. The nature and complexity of the proceedings;

5. The amount in controversy;

6. The importance of the discovery to resolving critical issues; and

7. The ease and expense of colleting, processing, reviewing and producing relevant information, taking into account:
    a. the accessibility of the relevant information;
    b. the volume of the relevant information;
    c. the location of the relevant information;
    d. the likelihood that the integrity and authenticity of the information will be impaired by the discovery process; and
    e. the ability to identify information that is subject to foreign privilege and work product protection from disclosure.

Cross-border discovery involves not only the interests and needs of the litigants, but also the interests of the involved nations in protecting privacy rights within their borders. Cross-border discovery disputes generally involve the privacy rights of employees, secured as a constitutional and/or contractual right.

The first factor seeks to identify the specific privacy obligations of the countries involved. As mentioned, this is a very case-specific analysis, because data privacy requirements differ from country to country.

The second and third factors examine the purpose and intent of the responding party in locating its information in a particular country. If the placement of the information in a particular country is based upon a good faith, legitimate business reason, then the requesting party should give great deference to the ruling by the presiding court where the action is filed. However, if the placement of the information in a particular jurisdiction is with the intent to circumvent the privacy rights of an individual or group, then an order from the presiding court to disclose such information is entitled to less weight when balanced against the state interest in protecting the privacy of its citizens.

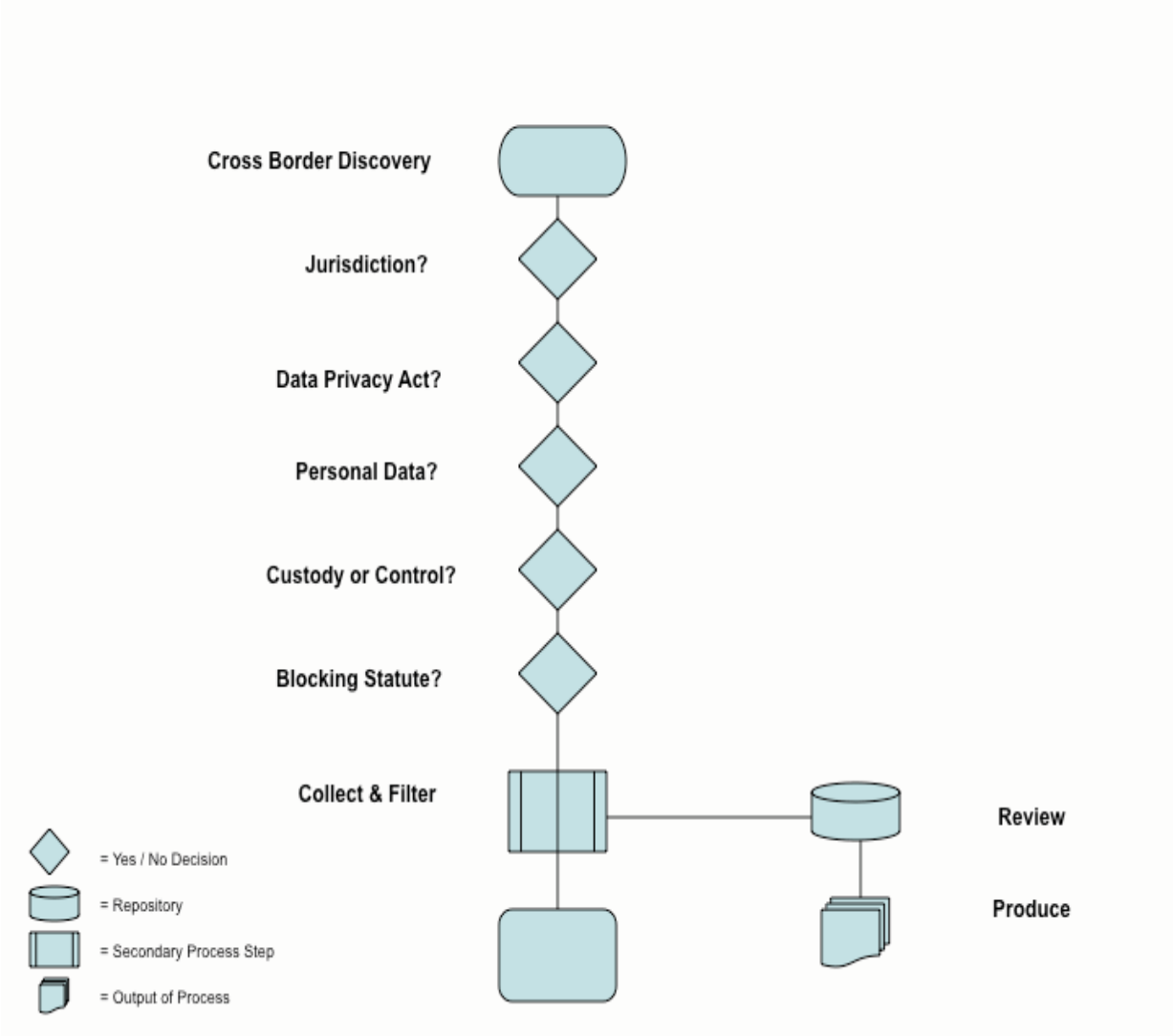
The remaining factors reflect the United States and UK approach to balancing the proportionate interests of the parties requesting and responding to the requested discovery.

Although not yet tested by U.S. and non-U.S. courts, the above framework offers a starting point for analysis, communication and collaboration regarding ways to resolved cross-border discovery conflicts. If, in the spirit of true Sedona dialogue, all concerned parties seek a way forward in good faith, then there is good reason to be optimistic that a mutually acceptable solution can be forged. Indeed, the practical requirements of global commerce will likely demand such a solution. A solution that fairly balances legitimate privacy interests with the need for relevant information relating to foreign-based litigation and investigations. And a solution that can, above all, resolve the current "Catch-22" of cross-border discovery conflict

Appendix A: Table of Authorities

[NOTE: This is deferred until receipt of all comments and edits]

Appendix B: High Level Analytical Framework for Cross-Border Discovery Conflicts



Appendix C: Application of the Framework for Cross-Border Discovery Conflicts to Selected Hypothetical Case Studies

Hypothetical Case Study No. 1

Multinational Corporation X is sued in a state court in the United States. The party that brought the action requests information through the discovery/disclosure process from the parent corporation which is located in a foreign jurisdiction. The privacy laws of the foreign jurisdiction where the parent corporation is located protect the information sought. The parent corporation refuses to provide the information sought stating that to do so would be to subject it to civil liability, imprisonment, or fine under their nondisclosure or privacy law. The requesting party files a motion to compel the disclosure of the information in the state court.

Analysis for Hypothetical Case Study No. 1

When information is requested through the discovery/disclosure process in one jurisdiction but is subject to the privacy laws in another foreign jurisdiction, the Court should balance the interests of the foreign entity, which is subject to the privacy laws with those of the requesting party in determining whether a party is entitled to the discovery/disclosure.

Restatement (Third) of Foreign Relations Law Section 442(2)(a) states:

If disclosure of information located outside the United States is prohibited by a law, regulation, or order of a court or other authority of the state in which the information or prospective witness is located, or of the state of which a prospective witness is a national:

A. a court or agency in the United States may require the person to whom the order is directed to make a good faith effort to secure permission from the foreign authorities to make the information available;

B. a court or agency should not ordinarily impose sanctions of contempt, dismissal, or default on a party that has failed to comply with the order for production, except in cases of deliberate concealment or removal of information or of failure to make a good faith effort [to secure permission to make the information available].

A trial court should balance the following factors in deciding whether a requesting party is entitled to information sought in the discovery or disclosure process where that information is subject to the privacy laws in another foreign jurisdiction:

1) the significance of the discovery/disclosure to issues in the case;

2) the degree of specificity of request;

3) whether the information originated in the jurisdiction from which it is being requested;

4) the availability of alternative means of securing the information sought in the discovery/disclosure request; and

5) the extent to which noncompliance would undermine the foreign sovereign's interest in the information requested.

See Restatement (Third) of Foreign Relations Law Section 442(1)(c) (1987); The United States Supreme Court invoked these criteria in *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa,* 482 U.S. 522, 534 (1987). *See also Volkswagen, A.G. v. Valdez*, 909 S.W.2d 900 (Tex. 1995). Yet, the earlier discussion referenced herein indicates that a majority of U.S. courts have declined to place the interests of the foreign state over the exigencies of the U.S. litigation.

In balancing the competing interests of two foreign States, a U.S. court may also consider the risk of civil liability that a party might face should it not comply with the local law. For example, a U.S. district court found, that the risk of civil liability in Germany was "speculative" where a federal grand jury in New York issued a subpoena to a New York bank requiring production of documents relating to transactions of its customers located both at its head office in New York and at its branch in Frankfurt, West Germany. The bank refused to produce documents from its West German branch. The court concluded that the bank had not made a good faith effort to comply with the subpoena and held the relevant bank officer in contempt. The Court of Appeals for the Second Circuit affirmed -- finding the importance of antitrust enforcement to the United States to be greater than the bank secrecy doctrine in Germany. *In Re United States v. First National City Bank*, 396 F.2d 897 (2d Cir. 1968).

More recently, however, the Criminal Chamber of the French Supreme Court upheld the conviction of a French lawyer for violating the French blocking statute, which prohibits "requesting, seeking, or disclosing in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature for the purposes of constituting evidence in view of foreign judicial or administrative proceedings." The lawyer was fined €10,000, or about $15,000 US, for his attempt to obtain discovery for a civil action in a U.S. federal court. *In re Advocat "Christopher X"*, Cour de Cassation, French Supreme Court, December 12, 2007, Appeal n 07-83228. This decision may alter the perception of U.S. courts as to the reality of enforcement of such statutes.

In balancing the competing interests of two foreign States, a court may also consider each State's interest in requesting or protecting the information. *See In Re United States v. Field*, 532 F.2d 404 (5th Cir.1976), *cert. denied*, 429 U.S. 940, 97 S.Ct. 354, 50 L.Ed. 2d 309 (1976). *See also United States v. Bank of Nova Scotia, I,* 691 F.2d 1384 (11th Cir. 1982), *cert. denied*, 462 U.S. 1119, 103 S.Ct. 3086, 77 L.Ed.2d 1348 (1983) (the Courts of Appeals for the Fifth and Eleventh Circuits held that the interest of the United States in upholding the grand jury's power to investigate crime outweighed the interests of the Cayman Islands and the Bahamas in bank secrecy laws). *See also United States v. Vetco, Inc.*, 691 F.2d 1281 (9th Cir.) *cert. denied*, 454 U.S. 1098, 102 S.Ct. 671 (1981) (the court held that the strong United States interest in collecting taxes and prosecuting tax fraud by its nationals outweighed Switzerland's interest in preserving business secrets of Swiss subsidiaries of American corporations.)

As discussed in the section entitled "How Does the Notion of 'playing according to local rules' apply?," U.S. courts are not unanimous in applying the Restatement guidelines or the *Aerospatiale* criteria. Reference to the most recent case law in this area in the pertinent jurisdiction is strongly advised. Similarly, state courts in the U.S. are not bound to follow the precedent of the federal jurisdiction cited above.

Hypothetical Case Study No. 2

Company A, a Delaware corporation, is sued in U.S. District Court in New York by Company B, a corporation under the laws of Germany that does business in New York. Company A has followed the practice for the last 10 years of storing certain electronic information extremely relevant to the U.S. litigation in Country XYZ, a jurisdiction with minimalist records management and preservation of evidence obligations, contrary to Company A's obligations if it were to store the records in the U.S. Company B seeks

to obtain electronic information from Company A's XYZ operations, as it has found such information lacking in Company A's domestic U.S. records and contends that Company A is deliberately shielding its information by maintaining it in Country XYZ.

Analysis for Hypothetical Case Study No. 2

If there is no legitimate business need to maintain data in Country XYZ, placement of company information in a country from which it would be difficult to extricate same in the event of litigation would not be looked upon kindly by most courts.

Several factors are involved in the analysis of this issue. For example, the initial analysis would look to the purpose and intent of the responding multi-national in locating its business information in a particular jurisdiction. If the placement of business information in a particular jurisdiction is based on good faith legitimate business reasons, the placement of the information in the particular jurisdiction should have the respect of the court in the jurisdiction where the matter is filed. However, if the placement of the data in a particular jurisdiction is with the intent to subvert the preservation or privacy obligations of the home jurisdiction, this too should be taken into account in the balancing of interests and determining the applicability of the privacy directives involved.

Yet, one must also look to identification the specific privacy obligations of the jurisdictions involved, in the interest of international comity; while most privacy standards are similar in intent, the implementing requirements may well be different from one country to another and may affect the analysis in a given situation (for a discussion of balancing these interests, as articulated by U.S. courts, please see the discussion in Hypothetical 1 above and the section of this Paper entitled "How Does the Notion of 'playing according to local rules' apply?," Each situation must be looked at on a case by case basis, with particular attention to the case law of the particular venue and, where pertinent, opinions of the subject data protection authorities.

Hypothetical Case Study No. 3

Company X., headquartered in the US, has multiple business units, including subsidiaries located in Madrid and Sydney. As part of its training on international warehousing and logistics, Company X has seconded two trainees from its Detroit office; one to Spain and the other to Australia.

While in their respective host country, each employee continues to use the same email address and e-mail system they used in Detroit. Likewise, because Company X and its subsidiaries share many of the same data systems, each seconded employee is able to continue to utilize the same data platforms and to store information to the same shared drive as when they worked in Detroit.

In the US, company X permits its employees to use the company electronic data systems (such as email) for personal use, so long as it does not interfere with the operations of the company and so long as the employee acknowledges that all information contained on the company data systems belongs to the company. Each seconded employee has extensive electronic files that they maintain on company data systems, including "private" files containing personal exchanges with family and friends, banking and credit card information, medical information, and the like.

During the cross-border training period, Company X is required to respond to discovery in US litigation calling for the production of certain e-mails and other electronic documents created and received by the seconded employees during the time each was working in Detroit. The discovery requests are broad enough, however, to also call for the production of emails and other electronic documents the seconded employees authored or received while on assignment overseas.

May Company X, through its Detroit computer facilities, search, collect and review the electronic data of each seconded employee for purposes of the ongoing litigation without regard to the data protection laws of Spain and Australia?

Analysis for Hypothetical Case Study No. 3

In the case of a seconded employee, the data protection privacy law of the host nation will apply to the extent it is made expressly applicable to the seconded employee. Where the law of the host nation does not specifically apply to the seconded employee, the determination is made by balancing those factors indicative of whether the seconded employee is predominantly then employed by the business unit in the host country or by the business unit in the country of origin, and by whether the seconded employee predominantly uses the data systems of the business unit in the host country or that of the business unit in the country of origin.

The data protection privacy law of the host country applies if it is expressly made applicable to the seconded employee, notwithstanding that the seconded employee predominantly continues in the employ of the business unit located in the country of origin.

Under the EC Data Protection Directive, any processing of personal data within the EEA is likely to fall within the terms of the Directive, and so the relevant national law (in this case Spain, in relation to the processing in Madrid) should be consulted in order to determine whether a transfer of the personal data to the US would be lawful.

If the data protection privacy law of the host country does not expressly apply to the seconded employee, it would be prudent to assume that the law should nevertheless apply to the seconded employee if a balancing of factors indicates that the seconded employee is predominantly employed by the business unit located in the host country, and if the employee predominantly utilized the data systems of the host business unit.

The factors to consider include:

i. Whether the host business unit directly compensates the seconded employee;

ii. Whether the host business unit directly provides benefits to the seconded employee such as pension, health and life insurance and worker's compensation, and the like;

iii. Whether the host business unit provides direction to and supervision over the seconded employee;

iv. Whether the term of the assignment in the host country is lengthy or undefined;

v. Whether the documents to be searched were authored or received by the seconded employee in the host country; and

vi. Whether the seconded employee uses and stores information on the data systems administered and maintained by the business unit in the host country.

International businesses often move employees from one business unit to a business unit in a different country, temporarily, for training or business purposes. Questions arise as to whether the seconded employee's data is subject to the host country's data protection laws, particularly where the term of the new employment is relatively short in duration or where the seconded employee continues to use the data systems of the business unit in the country of origin. The issue becomes most prominent when litigation in the host country compels the search, collection, review and production of the seconded employee's electronic data.

Whether the data of a seconded employee is subject to the host country's privacy law should be determined by first looking to text of those laws. In most instances the privacy protection statute will specify the scope of the law and the factors that trigger its application. Where the law of the host nation specifically applies to the seconded employee's data, those laws should be followed.
In other circumstances, the data privacy law of the host nation may not specifically address whether it applies to the data of a temporary employee. The employer is thus left without clear guidance as to whether application of the host nation's data privacy protection law is obligatory or whether the employer should or may continue with the data processing practices of the country of origin. Where the data protection law of the host nation does not specifically apply to the seconded employee, the law should still be followed if a balancing of factors dictates that the seconded employee is predominantly in the employ of the business unit located in the host country and predominantly uses the data systems of the host business unit.

There are a number of factors that help determine the status of a borrowed employee. Direct compensation from the business unit in the host country is a strong indictor that the employment relationship has shifted, albeit temporarily. Other strong indicators include whether the host business unit directly provides benefits such as life and health insurance, whether the host business unit exercises direct supervision over the seconded employee and the length of the anticipated duration of the assignment.

Appendix D: 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

23. 11. 95 EN Official Journal of the European Communities No L 281/31

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

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty establishing the European Community, and in particular Article 100a thereof,

Having regard to the proposal from the Commission [1],

Having regard to the opinion of the Economic and Social Committee [2],

Acting in accordance with the procedure referred to in Article 189b of the Treaty [3],

(1) Whereas the objectives of the Community, as laid down in the Treaty, as amended by the Treaty on European Union, include creating an ever closer union among the peoples of Europe, fostering closer relations between the States belonging to the Community, ensuring economic and social progress by common action to eliminate the barriers which divide Europe, encouraging the constant improvement of the living conditions of its peoples, preserving and strengthening peace and liberty and promoting democracy on the basis of the fundamental rights recognized in the constitution and laws of the Member States and in the European Convention for the Protection of Human Rights and Fundamental Freedoms;

(2) Whereas data-processing systems are designed to serve man; whereas they must, whatever the nationality or residence of natural persons, respect their fundamental rights and freedoms, notably the right to privacy, and contribute to economic and social progress, trade expansion and the well-being of individuals;

(3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one Member State to another, but also that the fundamental rights of individuals should be safeguarded;

(4) Whereas increasingly frequent recourse is being had in the Community to the processing of personal data in the various spheres of economic and social activity; whereas the progress made in information technology is making the processing and exchange of such data considerably easier;

(5) Whereas the economic and social integration resulting from the establishment and functioning of the internal market within the meaning of Article 7a of the Treaty will necessarily lead to a substantial increase in cross-border flows of personal data between all those involved in a private or public capacity in economic and social activity in the Member States; whereas the exchange of personal data between undertakings in different Member States is set to increase; whereas the national authorities in the various Member States are being called upon by virtue of Community law to collaborate and exchange personal data so as to be able to perform their duties or carry out tasks on behalf of an authority in another Member State within the context of the area without internal frontiers as constituted by the internal market;

(6) Whereas, furthermore, the increase in scientific and technical cooperation and the coordinated introduction of new telecommunications networks in the Community necessitate and facilitate cross-border flows of personal data;

(7) Whereas the difference in levels of protection of the rights and freedoms of individuals, notably the right to privacy, with regard to the processing of personal data afforded in the Member States may prevent the transmission of such data from the territory of one Member State to that of another Member State; whereas this difference may therefore constitute an obstacle to the pursuit of a number of economic activities at Community level,

---

[1] OJ No C 277, 5. 11. 1990, p. 3 and OJ No C 311, 27. 11. 1992, p. 30.

[2] OJ No C 159, 17. 6. 1991, p 38.

[3] Opinion of the European Parliament of 11 March 1992 (OJ No C 94, 13. 4. 1992, p. 198), confirmed on 2 December 1993 (OJ No C 342, 20. 12. 1993, p. 30); Council common position of 20 February 1995 (OJ No C 93, 13. 4. 1995, p. 1) and Decision of the European Parliament of 15 June 1995 (OJ No C 166, 3. 7. 1995).

distort competition and impede authorities in the discharge of their responsibilities under Community law; whereas this difference in levels of protection is due to the existence of a wide variety of national laws, regulations and administrative provisions;

(8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of individuals with regard to the processing of such data must be equivalent in all Member States; whereas this objective is vital to the internal market but cannot be achieved by the Member States alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the Member States and the need to coordinate the laws of the Member States so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas Community action to approximate those laws is therefore needed;

(9) Whereas, given the equivalent protection resulting from the approximation of national laws, the Member States will no longer be able to inhibit the free movement between them of personal data on grounds relating to protection of the rights and freedoms of individuals, and in particular the right to privacy; whereas Member States will be left a margin for manoeuvre, which may, in the context of implementation of the Directive, also be exercised by the business and social partners; whereas Member States will therefore be able to specify in their national law the general conditions governing the lawfulness of data processing; whereas in doing so the Member States shall strive to improve the protection currently provided by their legislation; whereas, within the limits of this margin for manoeuvre and in accordance with Community law, disparities could arise in the implementation of the Directive, and this could have an effect on the movement of data within a Member State as well as within the Community;

(10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community;

(11) Whereas the principles of the protection of the rights and freedoms of individuals, notably the right to privacy, which are contained in this Directive, give substance to and amplify those contained in the Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data;

(12) Whereas the protection principles must apply to all processing of personal data by any person whose activities are governed by Community law; whereas there should be excluded the processing of data carried out by a natural person in the exercise of activities which are exclusively personal or domestic, such as correspondence and the holding of records of addresses;

(13) Whereas the acitivities referred to in Titles V and VI of the Treaty on European Union regarding public safety, defence, State security or the acitivities of the State in the area of criminal laws fall outside the scope of Community law, without prejudice to the obligations incumbent upon Member States under Article 56 (2), Article 57 or Article 100a of the Treaty establishing the European Community; whereas the processing of personal data that is necessary to safeguard the economic well-being of the State does not fall within the scope of this Directive where such processing relates to State security matters;

(14) Whereas, given the importance of the developments under way, in the framework of the information society, of the techniques used to capture, transmit, manipulate, record, store or communicate sound and image data relating to natural persons, this Directive should be applicable to processing involving such data;

(15) Whereas the processing of such data is covered by this Directive only if it is automated or if the data processed are contained or are intended to be contained in a filing system structured according to specific criteria relating to individuals, so as to permit easy access to the personal data in question;

(16) Whereas the processing of sound and image data, such as in cases of video surveillance, does not come within the scope of this Directive if it is carried out for the purposes of public security, defence, national security or in the course of State activities relating to the area of criminal law or of other activities which do not come within the scope of Community law;

(17) Whereas, as far as the processing of sound and image data carried out for purposes of journalism

or the purposes of literary or artistic expression is concerned, in particular in the audiovisual field, the principles of the Directive are to apply in a restricted manner according to the provisions laid down in Article 9;

(18) Whereas, in order to ensure that individuals are not deprived of the protection to which they are entitled under this Directive, any processing of personal data in the Community must be carried out in accordance with the law of one of the Member States; whereas, in this connection, processing carried out under the responsibility of a controller who is established in a Member State should be governed by the law of that State;

(19) Whereas establishment on the territory of a Member State implies the effective and real exercise of activity through stable arrangements; whereas the legal form of such an establishment, whether simply branch or a subsidiary with a legal personality, is not the determining factor in this respect; whereas, when a single controller is established on the territory of several Member States, particularly by means of subsidiaries, he must ensure, in order to avoid any circumvention of national rules, that each of the establishments fulfils the obligations imposed by the national law applicable to its activities;

(20) Whereas the fact that the processing of data is carried out by a person established in a third country must not stand in the way of the protection of individuals provided for in this Directive; whereas in these cases, the processing should be governed by the law of the Member State in which the means used are located, and there should be guarantees to ensure that the rights and obligations provided for in this Directive are respected in practice;

(21) Whereas this Directive is without prejudice to the rules of territoriality applicable in criminal matters;

(22) Whereas Member States shall more precisely define in the laws they enact or when bringing into force the measures taken under this Directive the general circumstances in which processing is lawful; whereas in particular Article 5, in conjunction with Articles 7 and 8, allows Member States, independently of general rules, to provide for special processing conditions for specific sectors and for the various categories of data covered by Article 8;

(23) Whereas Member States are empowered to ensure the implementation of the protection of individuals both by means of a general law on the protection of individuals as regards the processing of personal data and by sectorial laws such as those relating, for example, to statistical institutes;

(24) Whereas the legislation concerning the protection of legal persons with regard to the processing data which concerns them is not affected by this Directive;

(25) Whereas the principles of protection must be reflected, on the one hand, in the obligations imposed on persons, public authorities, enterprises, agencies or other bodies responsible for processing, in particular regarding data quality, technical security, notification to the supervisory authority, and the circumstances under which processing can be carried out, and, on the other hand, in the right conferred on individuals, the data on whom are the subject of processing, to be informed that processing is taking place, to consult the data, to request corrections and even to object to processing in certain circumstances;

(26) Whereas the principles of protection must apply to any information concerning an identified or identifiable person; whereas, to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable; whereas codes of conduct within the meaning of Article 27 may be a useful instrument for providing guidance as to the ways in which data may be rendered anonymous and retained in a form in which identification of the data subject is no longer possible;

(27) Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; whereas, in particular, the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c), the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set,

may be laid down by each Member State; whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive;

(28) Whereas any processing of personal data must be lawful and fair to the individuals concerned; whereas, in particular, the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed; whereas such purposes must be explicit and legitimate and must be determined at the time of collection of the data; whereas the purposes of processing further to collection shall not be incompatible with the purposes as they were originally specified;

(29) Whereas the further processing of personal data for historical, statistical or scientific purposes is not generally to be considered incompatible with the purposes for which the data have previously been collected provided that Member States furnish suitable safeguards; whereas these safeguards must in particular rule out the use of the data in support of measures or decisions regarding any particular individual;

(30) Whereas, in order to be lawful, the processing of personal data must in addition be carried out with the consent of the data subject or be necessary for the conclusion or performance of a contract binding on the data subject, or as a legal requirement, or for the performance of a task carried out in the public interest or in the exercise of official authority, or in the legitimate interests of a natural or legal person, provided that the interests or the rights and freedoms of the data subject are not overriding; whereas, in particular, in order to maintain a balance between the interests involved while guaranteeing effective competition, Member States may determine the circumstances in which personal data may be used or disclosed to a third party in the context of the legitimate ordinary business activities of companies and other bodies; whereas Member States may similarly specify the conditions under which personal data may be disclosed to a third party for the purposes of marketing whether carried out commercially or by a charitable organization or by any other association or foundation, of a political nature for example, subject to the provisions allowing a data subject to object to the processing of data regarding him, at no cost and without having to state his reasons;

(31) Whereas the processing of personal data must equally be regarded as lawful where it is carried out in order to protect an interest which is essential for the data subject's life;

(32) Whereas it is for national legislation to determine whether the controller performing a task carried out in the public interest or in the exercise of official authority should be a public administration or another natural or legal person governed by public law, or by private law such as a professional association;

(33) Whereas data which are capable by their nature of infringing fundamental freedoms or privacy should not be processed unless the data subject gives his explicit consent; whereas, however, derogations from this prohibition must be explicitly provided for in respect of specific needs, in particular where the processing of these data is carried out for certain health-related purposes by persons subject to a legal obligation of professional secrecy or in the course of legitimate activities by certain associations or foundations the purpose of which is to permit the exercise of fundamental freedoms;

(34) Whereas Member States must also be authorized, when justified by grounds of important public interest, to derogate from the prohibition on processing sensitive categories of data where important reasons of public interest so justify in areas such as public health and social protection - especially in order to ensure the quality and cost-effectiveness of the procedures used for settling claims for benefits and services in the health insurance system - scientific research and government statistics; whereas it is incumbent on them, however, to provide specific and suitable safeguards so as to protect the fundamental rights and the privacy of individuals;

(35) Whereas, moreover, the processing of personal data by official authorities for achieving aims, laid down in constitutional law or international public law, of officially recognized religious associations is carried out on important grounds of public interest;

(36) Whereas where, in the course of electoral activities, the operation of the democratic system requires in certain Member States that political parties compile data on people's political opinion, the processing of such data may be permitted for reasons of important public interest, provided that appropriate safeguards are established;

(37) Whereas the processing of personal data for purposes of journalism or for purposes of literary of artistic expression, in particular in the audiovisual field, should qualify for exemption from the requirements of certain provisions of this Directive in so far as this is necessary to reconcile

the fundamental rights of individuals with freedom of information and notably the right to receive and impart information, as guaranteed in particular in Article 10 of the European Convention for the Protection of Human Rights and Fundamental Freedoms; whereas Member States should therefore lay down exemptions and derogations necessary for the purpose of balance between fundamental rights as regards general measures on the legitimacy of data processing, measures on the transfer of data to third countries and the power of the supervisory authority; whereas this should not, however, lead Member States to lay down exemptions from the measures to ensure security of processing; whereas at least the supervisory authority responsible for this sector should also be provided with certain ex-post powers, e.g. to publish a regular report or to refer matters to the judicial authorities;

(38) Whereas, if the processing of data is to be fair, the data subject must be in a position to learn of the existence of a processing operation and, where data are collected from him, must be given accurate and full information, bearing in mind the circumstances of the collection;

(39) Whereas certain processing operations involve data which the controller has not collected directly from the data subject; whereas, furthermore, data can be legitimately disclosed to a third party, even if the disclosure was not anticipated at the time the data were collected from the data subject; whereas, in all these cases, the data subject should be informed when the data are recorded or at the latest when the data are first disclosed to a third party;

(40) Whereas, however, it is not necessary to impose this obligation of the data subject already has the information; whereas, moreover, there will be no such obligation if the recording or disclosure are expressly provided for by law or if the provision of information to the data subject proves impossible or would involve disproportionate efforts, which could be the case where processing is for historical, statistical or scientific purposes; whereas, in this regard, the number of data subjects, the age of the data, and any compensatory measures adopted may be taken into consideration;

(41) Whereas any person must be able to exercise the right of access to data relating to him which are being processed, in order to verify in particular the accuracy of the data and the lawfulness of the processing; whereas, for the same reasons, every data subject must also have the right to know the logic involved in the automatic processing of data concerning him, at least in the case of the automated decisions referred to in Article 15 (1); whereas this right must not adversely affect trade secrets or intellectual property and in particular the copyright protecting the software; whereas these considerations must not, however, result in the data subject being refused all information;

(42) Whereas Member States may, in the interest of the data subject or so as to protect the rights and freedoms of others, restrict rights of access and information; whereas they may, for example, specify that access to medical data may be obtained only through a health professional;

(43) Whereas restrictions on the rights of access and information and on certain obligations of the controller may similarly be imposed by Member States in so far as they are necessary to safeguard, for example, national security, defence, public safety, or important economic or financial interests of a Member State or the Union, as well as criminal investigations and prosecutions and action in respect of breaches of ethics in the regulated professions; whereas the list of exceptions and limitations should include the tasks of monitoring, inspection or regulation necessary in the three last-mentioned areas concerning public security, economic or financial interests and crime prevention; whereas the listing of tasks in these three areas does not affect the legitimacy of exceptions or restrictions for reasons of State security or defence;

(44) Whereas Member States may also be led, by virtue of the provisions of Community law, to derogate from the provisions of this Directive concerning the right of access, the obligation to inform individuals, and the quality of data, in order to secure certain of the purposes referred to above;

(45) Whereas, in cases where data might lawfully be processed on grounds of public interest, official authority or the legitimate interests of a natural or legal person, any data subject should nevertheless be entitled, on legitimate and compelling grounds relating to his particular situation, to object to the processing of any data relating to himself; whereas Member States may nevertheless lay down national provisions to the contrary;

(46) Whereas the protection of the rights and freedoms of data subjects with regard to the processing of personal data requires that appropriate technical

and organizational measures be taken, both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorized processing; whereas it is incumbent on the Member States to ensure that controllers comply with these measures; whereas these measures must ensure an appropriate level of security, taking into account the state of the art and the costs of their implementation in relation to the risks inherent in the processing and the nature of the data to be protected;

(47) Whereas where a message containing personal data is transmitted by means of a telecommunications or electronic mail service, the sole purpose of which is the transmission of such messages, the controller in respect of the personal data contained in the message will normally be considered to be the person from whom the message originates, rather than the person offering the transmission services; whereas, nevertheless, those offering such services will normally be considered controllers in respect of the processing of the additional personal data necessary for the operation of the service;

(48) Whereas the procedures for notifying the supervisory authority are designed to ensure disclosure of the purposes and main features of any processing operation for the purpose of verification that the operation is in accordance with the national measures taken under this Directive;

(49) Whereas, in order to avoid unsuitable administrative formalities, exemptions from the obligation to notify and simplification of the notification required may be provided for by Member States in cases where processing is unlikely adversely to affect the rights and freedoms of data subjects, provided that it is in accordance with a measure taken by a Member State specifying its limits; whereas exemption or simplification may similarly be provided for by Member States where a person appointed by the controller ensures that the processing carried out is not likely adversely to affect the rights and freedoms of data subjects; whereas such a data protection official, whether or not an employee of the controller, must be in a position to exercise his functions in complete independence;

(50) Whereas exemption or simplification could be provided for in cases of processing operations whose sole purpose is the keeping of a register intended, according to national law, to provide information to the public and open to consultation by the public or by any person demonstrating a legitimate interest;

(51) Whereas, nevertheless, simplification or exemption from the obligation to notify shall not release the controller from any of the other obligations resulting from this Directive;

(52) Whereas, in this context, *ex post facto* verification by the competent authorities must in general be considered a sufficient measure;

(53) Whereas, however, certain processing operation are likely to pose specific risks to the rights and freedoms of data subjects by virtue of their nature, their scope or their purposes, such as that of excluding individuals from a right, benefit or a contract, or by virtue of the specific use of new technologies; whereas it is for Member States, if they so wish, to specify such risks in their legislation;

(54) Whereas with regard to all the processing undertaken in society, the amount posing such specific risks should be very limited; whereas Member States must provide that the supervisory authority, or the data protection official in cooperation with the authority, check such processing prior to it being carried out; whereas following this prior check, the supervisory authority may, according to its national law, give an opinion or an authorization regarding the processing; whereas such checking may equally take place in the course of the preparation either of a measure of the national parliament or of a measure based on such a legislative measure, which defines the nature of the processing and lays down appropriate safeguards;

(55) Whereas, if the controller fails to respect the rights of data subjects, national legislation must provide for a judicial remedy; whereas any damage which a person may suffer as a result of unlawful processing must be compensated for by the controller, who may be exempted from liability if he proves that he is not responsible for the damage, in particular in cases where he establishes fault on the part of the data subject or in case of *force majeure*; whereas sanctions must be imposed on any person, whether governed by private of public law, who fails to comply with the national measures taken under this Directive;

(56) Whereas cross-border flows of personal data are necessary to the expansion of international trade; whereas the protection of individuals guaranteed in the Community by this Directive does not stand in the way of transfers of personal data to third

countries which ensure an adequate level of protection; whereas the adequacy of the level of protection afforded by a third country must be assessed in the light of all the circumstances surrounding the transfer operation or set of transfer operations;

(57) Whereas, on the other hand, the transfer of personal data to a third country which does not ensure an adequate level of protection must be prohibited;

(58) Whereas provisions should be made for exemptions from this prohibition in certain circumstances where the data subject has given his consent, where the transfer is necessary in relation to a contract or a legal claim, where protection of an important public interest so requires, for example in cases of international transfers of data between tax or customs administrations or between services competent for social security matters, or where the transfer is made from a register established by law and intended for consultation by the public or persons having a legitimate interest; whereas in this case such a transfer should not involve the entirety of the data or entire categories of the data contained in the register and, when the register is intended for consultation by persons having a legitimate interest, the transfer should be made only at the request of those persons or if they are to be the recipients;

(59) Whereas particular measures may be taken to compensate for the lack of protection in a third country in cases where the controller offers appropriate safeguards; whereas, moreover, provision must be made for procedures for negotiations between the Community and such third countries;

(60) Whereas, in any event, transfers to third countries may be effected only in full compliance with the provisions adopted by the Member States pursuant to this Directive, and in particular Article 8 thereof;

(61) Whereas Member States and the Commission, in their respective spheres of competence, must encourage the trade associations and other representative organizations concerned to draw up codes of conduct so as to facilitate the application of this Directive, taking account of the specific characteristics of the processing carried out in certain sectors, and respecting the national provisions adopted for its implementation;

(62) Whereas the establishment in Member States of supervisory authorities, exercising their functions with complete independence, is an essential component of the protection of individuals with regard to the processing of personal data;

(63) Whereas such authorities must have the necessary means to perform their duties, including powers of investigation and intervention, particularly in cases of complaints from individuals, and powers to engage in legal proceedings; whereas such authorities must help to ensure transparency of processing in the Member States within whose jurisdiction they fall;

(64) Whereas the authorities in the different Member States will need to assist one another in performing their duties so as to ensure that the rules of protection are properly respected throughout the European Union;

(65) Whereas, at Community level, a Working Party on the Protection of Individuals with regard to the Processing of Personal Data must be set up and be completely independent in the performance of its functions; whereas, having regard to its specific nature, it must advise the Commission and, in particular, contribute to the uniform application of the national rules adopted pursuant to this Directive;

(66) Whereas, with regard to the transfer of data to third countries, the application of this Directive calls for the conferment of powers of implementation on the Commission and the establishment of a procedure as laid down in Council Decision 87/373/EEC [1];

(67) Whereas an agreement on a *modus vivendi* between the European Parliament, the Council and the Commission concerning the implementing measures for acts adopted in accordance with the procedure laid down in Article 189b of the EC Treaty was reached on 20 December 1994;

(68) Whereas the principles set out in this Directive regarding the protection of the rights and freedoms of individuals, notably their right to privacy, with regard to the processing of personal data may be supplemented or clarified, in particular as far as certain sectors are concerned, by specific rules based on those principles;

(69) Whereas Member States should be allowed a period of not more than three years from the entry into force of the national measures transposing this Directive in which to apply such new national rules progressively to all processing operations already under way; whereas, in order to facilitate their cost-effective implementation, a further period

[1] OJ No L 197, 18. 7. 1987, p. 33.

expiring 12 years after the date on which this Directive is adopted will be allowed to Member States to ensure the conformity of existing manual filing systems with certain of the Directive's provisions; whereas, where data contained in such filing systems are manually processed during this extended transition period, those systems must be brought into conformity with these provisions at the time of such processing;

(70) Whereas it is not necessary for the data subject to give his consent again so as to allow the controller to continue to process, after the national provisions taken pursuant to this Directive enter into force, any sensitive data necessary for the performance of a contract concluded on the basis of free and informed consent before the entry into force of these provisions;

(71) Whereas this Directive does not stand in the way of a Member State's regulating marketing activities aimed at consumers residing in territory in so far as such regulation does not concern the protection of individuals with regard to the processing of personal data;

(72) Whereas this Directive allows the principle of public access to official documents to be taken into account when implementing the principles set out in this Directive,

HAVE ADOPTED THIS DIRECTIVE:

CHAPTER I

GENERAL PROVISIONS

Article 1

Object of the Directive

1. In accordance with this Directive, Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.

2. Member States shall neither restrict nor prohibit the free flow of personal data between Member States for reasons connected with the protection afforded under paragraph 1.

Article 2

Definitions

For the purposes of this Directive:

(a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity;

(b) 'processing of personal data' ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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;

(c) 'personal data filing system' ('filing system') shall mean any structured set of personal data which are accessible according to specific criteria, whether centralized, decentralized or dispersed on a functional or geographical basis;

(d) 'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law;

(e) 'processor' shall mean a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller;

(f) 'third party' shall mean any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data;

(g) 'recipient' shall mean a natural or legal person, public authority, agency or any other body to whom data are disclosed, whether a third party or not; however, authorities which may receive data in the framework of a particular inquiry shall not be regarded as recipients;

(h) 'the data subject's consent' shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed.

Article 3

Scope

1. This Directive shall apply to the processing of personal data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a filing system or are intended to form part of a filing system.

2. This Directive shall not apply to the processing of personal data:

— in the course of an activity which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security (including the economic well-being of the State when the processing operation relates to State security matters) and the activities of the State in areas of criminal law,

— by a natural person in the course of a purely personal or household activity.

Article 4

National law applicable

1. Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where:

(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;

(b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;

(c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community.

2. In the circumstances referred to in paragraph 1 (c), the controller must designate a representative established in the territory of that Member State, without prejudice to legal actions which could be initiated against the controller himself.

CHAPTER II

GENERAL RULES ON THE LAWFULNESS OF THE PROCESSING OF PERSONAL DATA

Article 5

Member States shall, within the limits of the provisions of this Chapter, determine more precisely the conditions under which the processing of personal data is lawful.

Appendix E: Options for Cross Border Data Transfers

Option 1: Consent

A data transfer can be made on the condition that the data subject, or the person to whom the data pertains, has given unambiguous consent to the transfer. This is an attractive option if the data solely pertains to a few people, such as e-mail communications between select board members. In order for the consent to be considered valid, it must be: (1) given before the transfer; (2) unambiguous; (3) specific to the transfer or category of transfers; (4) freely given; and (5) informed.[1]

For extremely limited data, this can be a relatively simple and inexpensive process. If that limited data is commingled with other data, however, this option may not be feasible. For example, if e-mails among a few board members can only be found on backup tapes that also contain detailed customer information, consent is ineffective, as shipping a backup tape or any single piece of media, is an "all or nothing" proposition. If required, the data controller must be able to prove to the relevant E.U. Member State's Data Protection Authority ("DPA") that the valid consent of each data subject was obtained. It must be noted that in certain countries, a Consent given by an employee to an employer is considered *per se* involuntary.[2] In addition, it must also be shown that the consent was given on the basis of precise information, such as an explanation of the risks associated with sending data to a third country lacking adequate data privacy protection and the purpose of the transfer.[3]

Option 2: Safe Harbor.

The U.S. Department of Commerce, in consultation with the European Commission, has developed a "Safe Harbor" framework that provides predictability and continuity for those organizations that consistently send personal information to the United States. This approach allows personal data to flow between the E.U. and U.S. without the need for consent or another acceptable arrangement. Should an organization decide to operate under this framework, it must either join a self-regulatory privacy program or develop its own self-regulatory privacy policy that conforms to the requirements of Safe Harbor.

It is important to mention that an organization is required to annually self-certify to the Department of Commerce in writing that it is following the requirements of Safe Harbor. Self-certifying organizations must provide a contact person or persons to handle questions, complaints, and access requests; establish an independent recourse mechanism to investigate unresolved complaints, and have procedures in place for verifying compliance. These requirements assure E.U. privacy organizations that the organization provides "adequate" privacy protection.[4]

The advantage of this approach is that organizations which participate in Safe Harbor will be deemed to provide adequate data privacy protection by all countries in the E.U. and data flows to those organizations will continue unabated. Prior approval from each DPA for data transfers will either be

[1] The EU Privacy Directive, Articles 2(h) and 26(a).
[2] European Commission Article 29 Working Party. Opinion 8/2001 on the Processing of Personal Data in the Employment Context. (5062/01/EN/Final) (2001). http://europa.eu.int.
[3] Article 29 Data Protection Working Party, *Working Paper*: *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC*, WP114 (Nov. 25, 2005) (citing WP 48) and *Working Party Opinion on Protection of Individuals with Regard to the Processing of Data*, DG XV D/5025/98, WP12 (July 24, 1998).
[4] U.S. Department of Commerce, "Safe Harbor," available at http://www.export.gov/safeharbor/index.html.

waived or automatically granted. Subject to limited exceptions, claims brought by European citizens against U.S. organizations will be heard in the United States.

The risk in this approach is that only organizations that fall under the jurisdiction of the U.S. Federal Trade Commission or Department of Transportation can participate in Safe Harbor. Telecommunications and financial services companies are not eligible. This means there is a threat of U.S. government enforcement action should the organization fail to abide by its commitment to implement the Safe Harbor principles. If a need for an onward transfer (disclosure to a third party)[5] arises (such as in litigation, or in the case of a transfer that is not covered by the Safe Harbor agreement), organizations must notify the data subjects as to the purposes of the transfer and give them the opportunity to opt-out.[6] If this is not possible, the organization has the option of entering into a written agreement with the third party to provide the same level of privacy. This can be done with a contract incorporating Model Contractual Clauses.

Option 3: Model Contractual Clauses.

It took years of negotiations with regulatory agencies, international organizations, and trade associations for the European Commission to adopt a set of standard contractual clauses that will ensure adequate safeguards for international transfers of personal data. This scheme allows the transfer of data outside the E.U. where both parties agree to be bound by a set of clauses that comply with provisions equivalent to the main aspects of the Directive.[7] There are two types of clauses available.[8]

1. Controller to Controller (two versions) – transfer of data between entities where each is able to control and decide the manner in which data is processed. The first version created joint and several liability for the data exporter, which has now been removed [9] and the second, more business friendly, version bases liability on fault.[10]

2. Controller to Processor – transfer of data between an exporting entity which is outsourcing the process to a data processor while still maintaining control over the data and the manner in which it is to be processed.

Model Contractual Clauses are a good option for organizations not eligible or not certified under Safe Harbor. Unlike Safe Harbor, the clauses allow for the transfer of personal data to any country in the world, not just the United States. Distinct from Binding Corporate Rules, as discussed below, under Safe Harbor the details of the company's privacy policies need not be published. Additionally, this is a good option for organizations that do not need day-to-day transfer of personal data from the E.U. but are occasionally required to do so for litigation.

The difficulty with this approach is that contracts incorporating Model Contractual Clauses must follow the provisions of Commission 2002/16/EC scrupulously, and be carefully structured and drafted in a manner that will anticipate every possible data transfer and use or they will be outdated and the organization will be subject to enforcement actions by the relevant DPA or a data subject.[11] The Controller to Controller Clauses

---

[5] *Id.*
[6] Commission Decision 2000/520/EC (OJ L215, 25.8.2000).
[7] The Directive, Article 26(2).
[8] Commission Decision 2001/497/EC (OJ L181, 4.7.2001).
[9] *Id.*
[10] Commission Decision 2004/915/EC (OJ L385, 29.12.2004).
[11] Commission Decision 2002/16/EC (OJ L6, 10.1.2002). Since December 27, 2004, the European Commission has recognized a set of standard contractual clauses proposed by seven international business organizations to be an adequate alternative to the Model Contractual Clauses. This alternative set imposes due diligence requirements on the importer and exporter of the data and exposes parties to liability for only those damages that the party has caused. Commission Decision 2004/915/EC (O.J. L385/74, 29.12.2004).

require jurisdiction to be accepted in the data exporter's country of establishment should a data subject, as a third-party beneficiary, seek recourse against any party.[12] Most importantly, thorough research must be done to determine if prior approval is required by the relevant DPA before data is transferred.

Option 4: Binding Corporate Rules (BCRs).

For many businesses with limited global data transfers it may be sufficient to utilize either Safe Harbor or the E.U. Model Contractual Clauses, but for others with complex corporate structures and a web of cross-border data transfers, another option may be considered as a long-term solution. Personal data can be transferred outside of the E.U. but within a group of companies in a manner that ensures adequacy by the adoption of binding codes of corporate conduct by the organization or binding corporate rules ("BCRs").[13] To date, the only corporations who have had their BCRs approved by a DPA are General Electric (UK), Philips (Denmark) and Daimler-Chrysler (Germany).[14] However, no company has yet achieved full approval by all relevant DPAs.

BCRs detail what information is collected, how it is processed, used and stored, and who may access this data. They are binding on all E.U. affiliates and must give employees the right to enforce the code of conduct directly against the organization. The rules provide for the creation of independent ombudsman teams whose job it is to address data privacy concerns. Once approved by the relevant E.U. regulators, this proactive scheme allows for seamless transfer of data between the offices of multi-national organizations.

Similar to the U.S. Safe Harbor program, BCRs can offer a safety zone within an organization between corporate groups. Once put in place, they offer the most comprehensive compliance framework for multinational organizations. Additionally, BCRs can dispose of the need for recurring research on privacy laws in each E.U. country, and save resources needed for drafting Model Contractual Clauses or obtaining consent from every data subject.

BCRs, however, create a safety zone for transfers between corporate groups, they do not create the same for transfers outside the corporate group. This means information subject to "onward transfer" for litigation will not be protected without additional safeguards. Implementing BCRs will necessitate a lot of upfront time and expense. Each organization that transfers data must provide for a detailed and uniform compliance system backed up by an audit. Then it must nominate a lead regulator from within the European Union whose role it is to broker its BCRs to its counterparts across the EU. Undoubtedly, many revisions to the BCRs will be required in order to comply with the laws of each country's DPA.[15]

---

[12] *Id.*

[13] Article 29 Data Protection Working Party, *Working Paper: 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*, MARKT/11639/02/EN, WP74 (June 3, 2003).

[14] General Electric Website: http://www.ge.com/en/citizenship/govcomp/dataprivacy.htm and The Official Guernsey Government Website: http://www.gov.gg/ .

[15] The process may have recently become easier. Previously, organizations had to submit different application forms to each E.U. member state when asking data protection authorities to approve their BCRs. However, on January 10, 2007, the E.U. Data Protection Working Party took a step towards simplifying this complex process by adopting a new Model Application for the submission of an organization's BCRs to any DPA. Article 29 Data Protection Working Party, Working Paper: Co-Operation Procedure for Issuing Common Opinions as Adequate Safeguards Resulting From "Binding Corporate Rules" 05/EN, WP107 (April 14, 2005) and Working Paper: Establishing a Model Checklist Application for Approval of Binding Corporate Rules, 05/EN, WP108 (April 14, 2005).

Appendix G: The Sedona Conference® Working Group Series℠ & WGS℠ Membership Program

"DIALOGUE DESIGNED TO MOVE THE LAW FORWARD IN A REASONED AND JUST WAY"

The Sedona Conference® Working Group Series℠ ("WGS℠") represents the evolution of The Sedona Conference® from a forum for advanced dialogue to an open think-tank confronting some of the most challenging issues faced by our legal system today.

The WGS℠ begins with the same high caliber of participants as our regular season conferences. The total, active group, however, is limited to 30-35 instead of 60. Further, in lieu of finished papers being posted on the website in advance of the Conference, thought pieces and other ideas are exchanged ahead of time, and the Working Group meeting becomes the opportunity to create a set of recommendations, guidelines or other position piece designed to be of immediate benefit to the bench and bar, and to move the law forward in a reasoned and just way. Working Group output, when complete, is then put through a peer review process, including where possible critique at one of our regular season conferences, hopefully resulting in authoritative, meaningful and balanced final papers for publication and distribution.

The first Working Group was convened in October 2002, and was dedicated to the development of guidelines for electronic document retention and production. The impact of its first (draft) publication—The Sedona Principles; Best Practices Recommendations and Principles Addressing Electronic Document Production (March 2003 version)—was immediate and substantial. The Principles was cited in the Judicial Conference of the United State Advisory Committee on Civil Rules Discovery Subcommittee Report on Electronic Discovery less than a month after the publication of the "public comment" draft, and was cited in a seminal e-discovery decision of the Federal District Court in New York less than a month after that. As noted in the June 2003 issue of Pike & Fischer's Digital Discovery and E-Evidence, "The Principles...influence is already becoming evident."

The WGS℠ Membership Program was established to provide a vehicle to allow any interested jurist, attorney, academic or consultant to participate in Working Group activities. Membership provides access to advance drafts of Working Group output with the opportunity for early input, and to a Bulletin Board where reference materials are posted and current news and other matters of interest can be discussed. Members may also indicate their willingness to volunteer for special Project Team assignment, and a Member's Roster is included in Working Group publications.

We currently have active Working Groups in the areas of 1) electronic document retention and production; 2) protective orders, confidentiality, and public access; 3) the role of economics in antitrust; 4) the intersection of the patent and antitrust laws; (5) Markman hearings and claim construction; (6) international e-information disclosure and management issues; and (7) e-discovery in Canadian civil litigation. See the "Working Group Series" area of our website www.thesedonaconference.org for further details on our Working Group Series and the Membership Program.

Appendix H: Working Group Participants Member & Observers (as of August 1,2008)

E. Regan Adams
Goldman, Sachs & Co.

Reza Alexander
DLA Piper UK LLP

Sharon Alexander-Gooding
University of the West Indies

Thomas Y. Allman

Keith Altman
Finkelstein & Partners LLP

Neil Andrews
Cambridge University Faculty of Law

Hon. Leonard B. Austin
Supreme Court of the State of New York
Observer

John Bace
Gartner, Inc.

Denise E. Backhouse
Morgan Lewis & Bockius LLP

Theodore S. Barassi
Symantec Corp.

Jerry F. Barbanel
Attorney & Consultant

Kara L.B. Barrow
Faegre & Benson LLP

Courtney Barton
Crowell & Moring

Cynthia Bateman
Georgia Pacific Corporation

Steven C. Bennett
Jones Day

Karin A. Bentz
Law Offices of Karin A. Bentz

Amanda Miller Bettinelli
Hughes Hubbard & Reed LLP

Sanjay Bhandari
Ernst & Young LLP

Daniel Blair
Bank of America

Andrew Bowyer
KPMG

Paul Brabant
Epiq Systems Inc.

Richard G. Braman
The Sedona Conference
Ex Officio

Jonathan Brewer
LexisNexis Applied Discovery

Greg Buckles
Reason-Ed LLC

Patrick Burke
Guidance Software, Inc.

Megan Butler

William P. Butterfield
Cohen, Milstein, Hausfeld & Toll, PLLC

Jacob Cameron
Shell International

Justice Colin L. Campbell
Superior Court of Justice, Ontario
Observer

Jonathan S. Campbell
Capital One Services, Inc.

Craig Carpenter
Recommind, Inc.

Kevin Carr
InterLegis

Timothy Carson
Crowell & Moring

Roger Chadderdon
Renew Data

Andrew M. Cohen
EMC Corporation

Clark R. Cordner
Orrick, Herrington & Sutcliffe LLP

Andrew Cosgrove
Redgrave Daley Ragan & Wagner LLP

Christopher V. Cotton
Shook Hardy & Bacon LLP

Moze Cowper
Amgen Inc.

Stan Crosley
Eli Lilly and Company

Conor R. Crowley
Conor Crowley Consulting

M. James Daley
Daley & Associates LLP

Olivier Debouzy
August & Debouzy

Radi Dennis
Sentry Consulting Group

Robert W. Dibert
Frost Brown Todd LLC

Mark Dingle
Simmons & Simmons

R. David Donoghue
DLA Piper

Torsten Duwenhorst
Ernst & Young LLP

James Dykes
Exxon Mobil

Craig Earnshaw
FTI Consulting

Marc Eisner
SPi

V. Scott Ellis
Protiviti

Grant J. Esposito
Morrison & Foerster LLP

Amor A. Esteban
Shook, Hardy & Bacon, LLP

Kelly F. Farmer
Latham & Watkins LLP

Diana Fasching
Redgrave Daley Ragan & Wagner LLP

Jeffrey C. Fehrman
Onsite3

Carmen Oveissi Field
Daylight Forensic & Advisory LLC

Hon. Kenneth Fields
Superior Court of Arizona (Retired)
Observer

Eric R. Finkelman
Ciba Specialty Chemicals Corporation

Thomas Belitz Franca
Veirano Avaogados

Clive Freedman
3 Verulam Buildings, Gray's Inn

Eric M. Friedberg
Stroz Friedberg LLC

Kelly Friedman
Ogilvy Renault LLP

Christine Gabitass
Latham & Watkins LLP
David J. Galbenski
Lumen Legal

Aoife Gaughan
A & L Goodbody

Barbara K. Geier
King & Spalding LLP
Atlanta, GA

Steven S. Gensler
University of Oklahoma College of Law

Michael A. Gold
Jeffer Mangels Butler & Marmaro LLP

Richard Gomes
Citigroup

Richard Graham
Pension Benefit Guaranty Corporation

Matthew Grant
LexisNexis

David Gray
McCarthy Tétrault LLP

Peter Gronvall
AdamsGrayson

Maura R. Grossman
Wachtell, Lipton, Rosen & Katz

Jvo Grundler
Ernst & Young LLP

Mira GurAire
Federal Judicial Center
Observer

David H. Haines
Exterro

Julie Anne Halter
K&L Gates

Jennifer Hamilton
Deere & Company

William F. Hamilton
Holland & Knight LLP

Matthew S. Harman
King & Spalding LLP

Dominic Hartley
Department for Constitutional Affairs, UK
Observer

Hope Haslam
Epiq Systems

Gary Hayden
Ann Arbor Consulting LLC

Ronald J. Hedges
Nixon Peabody LLP

Janet Heins
Merck & Co., Inc.

William Herr
Coherent Discovery Solutions, Inc.

Michael Heyrich
Citigroup Inc.

Dr. Mark C. Hilgard
Mayer Brown LLP

Trevor Horwitz
Ernst & Young LLP

Oleh Hrycko
H & A Computer Forensics

Brian Ingram
Solomon Page Group LLC

Anders Isgren
Baker & MacKenzie

David K. Isom
Greenberg Traurig LLP

Harvey Jang
Symantec Corp.

Martin J. Jaron
Holland & Knight LLP

John Jennings

John H. Jessen
Electronic Evidence Discovery, Inc.

Glenn Johnson
King & Spalding LLP

Andrew Jones
Clifford Chance LLP

Judy Juhnke
Faegre & Benson LLP

Cierniak Jurgen

Dr. Hironao Kaneko
Tokyo Institute of Technology

Roger B. Kaplan
Greenberg Traurig LLP

Conrad S. Kee
Jackson Lewis LLP

Jerami D. Kemnitz
Redgrave Daley Ragan & Wagner LLP

David J. Kessler
Drinker Biddle & Reath LLP

Dr. Georg Kirsch
Bayer AG

Melissa L. Klipp
Drinker Biddle & Reath LLP

Joshua Kubicki
Solomon Page Group LLC

Christopher Kuner
Hunton & Williams LLP

Janet Kwuon
Reed Smith LLP

Janet Lambert
Barlow Lyde & Gilbert

Paul Lewis
Protiviti

Hon. Jim D. Lovett
Texas Sixth District Court
Observer

Cecilia Loving
Patterson Belknap Webb & Tyler LLP

Cecil Lynn
Ryley Carlock & Applewhite

Heidi Maher
Renew Data Corp.

Jean M. Mahon
CA Inc.

Michelle Mahoney
Mallesons Stephen Jaques

Carrie Mallen
Gilead Sciences, Inc.

Marisa Marinelli
Holland & Knight LLP

Greg Martin
SABMiller PLC

Ann-Marie Mason
Metropolitan Life Insurance Co.

Stephen Mason

Mark Maurice-Jones
Kimberly Clark Corp.

David McCartney
Mayer Brown LLP

Paul A. Meyer
Watson Wyatt Worldwide

Neil Micklethwaite
Bingham McCutchen LLP

Gary Milner-Moore
Herbert Smith

Neil Mirchandani
Lovells

David Moncure
Fulbright & Jaworski, LLP

Robert Moody
Berenfeld, Spritzer, Shechter & Sheer LLP

Tim Moorehead
BP America, Inc.

Thomas Mueller
Morrison & Foerster LLP

Sheila Murphy
Metropolitan Life Insurance Co.

Paul J. Neale Jr.
DOAR Litigation Consulting

Hon. Lord Justice David Neuberger
Royal Courts of Justice
Observer

Mollie Nichols
First Advantage

John Oakley
Berenfeld, Spritzer, Shechter & Sheer LLP

Patrick Oot
Verizon Communications Inc.

Deidre Paknad
PSS Systems Inc.

Thomas Pasternak
DLA Piper

George L. Paul
Lewis & Roca LLP

Anthony (Tony) Polk
Electronic Evidence
Discovery, Inc.

Sandra Potter
Potter Farrelly

Jason Priebe
Seyfarth Shaw LLP

Charles R. Ragan
Redgrave Daley Ragan &
Wagner LLP

Melody Rajsky
Merck & Co., Inc.

Kenneth Rashbaum
Sedgwick, Detert, Moran &
Arnold

Jonathan Redgrave
Redgrave Daley Ragan &
Wagner LLP

Sean Regan
Symantec Corp.

Daniel L. Regard
Intelligent Discovery
Solutions, Inc.

Anthony Reid
Deloitte & Touche

John T. Ritter
Bank of America

Paul M. Robertson
Redgrave Daley Ragan &
Wagner LLP

Ernesto Rojas
Forensic & Security
Services Inc.

John J. Rosenthal
Howrey LLP

Charles Rothman
H & A Computer Forensics

Jane K. Rushton
Prudential Financial

Jay G. Safer
Locke Lord Bissell &
Liddall LLP

Stuart K. Sammis
Corning Incorporated

Ed Sautter
Mayer Brown LLP

Eric J. Schwarz
Ernst & Young LLP

Samuel B. Sebree
Altria/Philip Morris Int'l

Stephen Shapiro
SAB Miller PLC

Jackson Sharman III
Lightfoot Franklin & White

James D. Shook
EMC Corporation

Mark Sidoti
Gibbons P.C.

Julie Sinor
PricewaterhouseCoopers

Jessica Cullen Smith
McDermott Will & Emery
LLP

Paul Smith
Conyers Dill & Pearman

Manuel Soudant
Shell International

Carolyn Southerland
Huron Consulting Group

Dr. Axel Spies
Bingham McCutchen LLP

David Sporkin
Protiviti

Judith Starr
Pension Benefit Guaranty
Corporation

Oliver Strub
Ciba Specialty Chemicals
Corporation

Richard Susskind
Advisor to Lord Chief
Justice
Observer

Ariana J. Tadler
Milberg LLP

Jeane A. Thomas
Crowell & Moring LLP

Hon. Samuel A. Thumma
Arizona Superior Court
Observer

Jason Velasco
Merrill Corporation

Vincent Walden
Ernst & Young LLP

Simon Walsh
Faegre & Benson LLP

Hon. Ira B. Warshawsky
Supreme Court of NY
Commercial Division
Observer

Hon. David Waxse
U.S. District Court, Kansas
Observer

Laurie A. Weiss
Fulbright & Jaworski, LLP

Robert N. Wickstrom
Sullivan & Cromwell LLP

Sally M. Wiese
Wachovia Bank

Robert B. Wiggins
Morgan Lewis & Bockius
LLP

Ashley P. Winton
White & Case LLP

Kenneth J. Withers
The Sedona Conference
Ex Officio

Susan B. Wortzman
Wortzman Nickle
Professional Corporation

Frank Wu
Protiviti

Christian Zeunert