IMPORTANT NOTICE:
This Publication Has Been Superseded by the January 2017 Transitional Edition

See the Most Current Publication at

https://thesedonaconference.org/publication/International_Litigation_Principles

THE SEDONA CONFERENCE® WORKING GROUP SERIES℠

WGS℠

THE SEDONA CONFERENCE®

International Principles on Discovery, Disclosure & Data Protection:

Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation

A Project of The Sedona Conference® Working Group 6
on International Electronic Information Management,
Discovery & Disclosure (WG6)

EUROPEAN UNION EDITION
PUBLIC COMMENT VERSION
DECEMBER 2011

The Sedona Conference® International Principles on Discovery, Disclosure & Data Protection:

Best Practices, Recommendations & Principles for Addressing the Preservation & Discovery of Protected Data in U.S. Litigation

A Project of The Sedona Conference® Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6)

EUROPEAN UNION EDITION
2011 PUBLIC COMMENT VERSION

Editor-in-Chief:
Amor A. Esteban

Senior Editors:
Moze Cowper
M. James Daley
John K. Rabiej
Daniel L. Regard
Kenneth J. Withers
Christian Zeunert

Contributing Editors:
Quentin Archer
Steven C. Bennett
Richard J. Hood
Patrick Kos
Marni Magowan Otjen
Sandra Potter

The Editors would like to especially acknowledge the comments of Dr. Alexander Dix, LL.M., Berlin Commissioner for Data Protection and Freedom of Information, and Hon. Shira A. Scheindlin, United States District Judge for the Southern District of New York, to earlier drafts of this publication.

We thank all of our Working Group Series[SM] Sustaining and Annual Sponsors, whose support is essential to our ability to develop Working Group Series[SM] publications. For a listing of our sponsors, click on the "Sponsors" navigation bar on the homepage of our website.

The opinions expressed in this publication, unless otherwise attributed, represent consensus views of the members of The Sedona Conference® Working Group 6. They do not necessarily represent the views of any of the individual participants or their employers, clients, or any other organizations to which any of the participants belong nor do they necessarily represent official positions of The Sedona Conference®.

REPRINT REQUESTS:
Requests for reprints or reprint information should be directed to Kenneth J. Withers, Director of Judicial Education, The Sedona Conference®, at kjw@sedonaconference.org or 1-866-860-6600.

Foreword

In 2005, The Sedona Conference® ("TSC") formally launched the Working Group on International Electronic Information Management, Discovery, and Disclosure ("Working Group 6"). The group's mandate was an important one: bring together some of the most experienced attorneys, judges, privacy and compliance officers, technology-thought leaders, and academics from around the globe to dialogue about the international management, discovery, and disclosure of electronically stored information ("ESI") involved in cross-border disputes.

This group recognized that the world is changing. For example, the rapid proliferation of electronic information and the increasing interdependence amongst individuals, multi-national companies, and governments arising from a global marketplace present novel and unique legal challenges that previously did not exist. These challenges have made us re-think deeply held notions of privacy, personal freedom, and how we resolve legal conflicts. More specifically, Working Group 6 recognized that one of the challenges in this new "flat world" is the conflict that arises when a party is obligated to disclose information in one forum (e.g., a United States federal court) but that information is located outside the United States (e.g., typically in the European Union) and is protected by a data-protection law or "blocking statute," which prohibits its disclosure.

The German-born theologian Thomas à Kempis once wrote, "the loftier the building, the deeper must the foundation be laid." Similar to great faith, great ideas also need a solid foundation. Therefore, in 2007, Working Group 6 decided that recognizing and analyzing conflicts of laws were necessary steps to trying to resolve them. This understanding led to the creation of a "framework for analysis" of cross-border discovery conflicts. The goal was three-fold: (1) to examine the differing notions of data privacy and differing notions of legal discovery between common law countries and civil law countries; (2) to understand the current legal mechanisms for cross-border transfer of ESI and examine the obstacles inherent in those mechanisms; and (3) to offer a way to think through the problem while acknowledging that there was not one solution or an easy fix to the problem. A year later, 2008, *The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts* ("Framework for Analysis") was published, laying the foundation for further work.

With the publication of the *Framework for Analysis*, Working Group 6 felt it was appropriate to start working on a set of principles to guide parties as they attempt to navigate the challenges of cross-border conflicts. We met in 2009 in Barcelona, Spain, in 2010 in Washington, D.C., and in 2011 in Lisbon, Portugal, in order to develop and test the idea of a set of international principles that parties, data privacy authorities, and courts might turn to for guidance when faced with these cross-border issues. Each of these meetings was extended beyond the ranks of Working Group 6 to invited data protection and data privacy thought leaders from around the world. Beginning in 2009, Working Group 6 also engaged in an active dialogue with the Article 29 Working Party in order to share ideas and develop a solution to this cross-border conundrum.

Now, after more than six years, Working Group 6 has drafted *The Sedona Conference® International Principles on Discovery, Disclosure and Data Protection* ("International Principles"). The *International Principles* sets forth a three-stage approach to addressing cross-border conflicts while also providing useful commentary. The previously published *Framework for Analysis* will serve as an appendix to the *International Principles*, providing a strong foundation. The *International Principles* demonstrates that data protection and discovery are not at intellectual or practical odds.

Finally, as part of the *International Principles*, Working Group 6 has developed a model protective order and a model data process and transfer protocol for use by parties and courts to better protect litigation-related data subject to data protection laws within the ambit of traditional U.S. litigation and court discovery practices. *The Sedona Conference® Model Protected Data Protective Order* ("Protective Order") combines the conventional protective order restrictions on disclosure and use of "confidential" information with additional specific protections for certain classes of information (e.g., personal information) because of international and domestic data protection laws. *The Sedona Conference® Cross-Border Data Safeguarding Process + Transfer Protocol* ("Protocol") outlines a practical, baseline approach to protecting data at the preservation and collection levels, rather than attempt to reconcile differences in data protection and privacy schemes among countries and multinational companies.

The *International Principles*, together with the *Framework for Analysis*, the *Protective Order,* and the *Protocol*, demonstrate that through cooperation and dialogue, and the collective experiences of hundreds of commentators, problems that were once thought to be insurmountable are, in fact, manageable and solvable.

This version of the *International Principle*s is subtitled "European Union Edition." Other editions of the *International Principles* are planned for publication by Working Group 6 that will focus on sovereign countries or regions other than the EU and the intersection of their data protection laws and U.S. preservation and discovery requirements. It is expected that lawyers, data protection authorities, and the courts will find this European Union Edition helpful until more specific editions may become available. As stated in the definition of Data Protection Laws, the European Union Edition of the *International Principles*, "[a]lthough focused principally on the relationship between U.S. preservation and discovery obligations and the EU Data Protection Directive . . . is intended to apply broadly wherever Data Protection Laws, regardless of national origin, conflict with U.S. preservation and discovery obligations, whether those laws take the form of blocking statutes, privacy regulations, or trade secret protections and whether those laws are enacted by EU member states, other countries, or the United States . . . .").

This version of the *International Principles* is also subtitled a "Public Comment Version." We welcome your suggestions. To submit comments, if you have any questions, or to learn more about The Sedona Conference®, please go to www.thesedonaconference.org or contact us at info@sedonaconference.org.

Quentin Archer (UK)
M. James Daley (US)

Co-Chairs, The Sedona Conference® Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6)

Steven C. Bennett (US)
Moze Cowper (US)
Amor A. Esteban (US)
Richard J. Hood (US)
Sandra Potter (AU)
Cecilia Alvarez Rigaudias (ES)
Christian Zeunert (CH)

Steering Committee, The Sedona Conference®. Working Group 6 on International Electronic Information Management, Discovery, and Disclosure (WG6)

The Sedona Conference® International Principles on Discovery, Disclosure & Data Protection

1. With regard to data that is subject to preservation, disclosure, or discovery, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.

2. Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.

3. Preservation or discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.

4. Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.

5. A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.

6. Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

Preface

Among the challenges inherent in the global marketplace is the cross-border disclosure and transfer of confidential, personal, privileged, or otherwise protected information sought for disclosure or discovery in U.S. litigation. Discovery requests that seek information from sources outside the United States bring to light international differences in the use of certain data deemed worthy of protections by the sovereign laws of other countries. The frequency and complexity of these requests have significantly increased over the last several years, undoubtedly driven, by a dramatic expansion in the volume of data created and stored in an electronic format, commonly referred to as Electronically Stored Information ("ESI") – which now accounts for virtually all business information. Indeed, the volume of stored electronic data and number of ESI transmissions grows exponentially each year.[1]

This unprecedented explosion in information owes in large part to ubiquitous, mobile, and easily-replicatable nature of ESI. Today, an employee from a Toronto company can conduct business from a cafe in Paris, while sending electronic messages to customers in Dubai that attach documents from "cloud" servers located in Singapore, Dallas, and Amsterdam. The ease with which electronic data is created, replicated, transmitters, and stored – unconstrained by traditional geographic borders – places profound stress on existing international treaties regarding discovery of information for purposes of cross-border litigation. In short, agreements among nations concerning cross-border discovery, made in the age before personal computers and the Internet, are now severely outdated. Indeed, the rapid pace of technological change, as reflected by increased use of cloud computing and social networking platforms, have blurred traditional legal notions of "custody and control" – the touchstone for traditional analysis of preservation and production obligations.[2]

The purpose of *International Principles* is to provide guidance to public and private parties, counsel, data protection authorities, and the judiciary regarding the management of conflicts that may arise when there is an obligation in one jurisdiction to preserve or produce information from a second jurisdiction in circumstances where the laws of the second jurisdiction limit the preservation, processing, or transfer of such information. These encounters frequently involve requests by a party to U.S. litigation for data from another party that is restricted in the disclosure or dissemination of that data by the laws of a member state of the European Union. All EU member states have implemented the Data Protection Directive, [3] which imposes restrictions on the use and dissemination of personal information. Most challenging to navigate are the restrictions relating to

---

[1]George L. Paul and Jason R. Baron, *Information Inflation: Can the Legal System Adapt?* 13 RICH. J.L. & TECH. 10 (2007) at 9.

[2]M. James Daley, *Information Age Catch 22: The Challenge of Technology to Cross-Border Disclosure and Data Privacy*, 12 SEDONA CONF. J. 121 (2011).

[3]The Data Protection Directive is more formally known as *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. See* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT.

the processing and transfer of personal information to the United States, which is deemed by the EU as a country that does not have privacy protections that satisfy EU standards.

Given the frequency of disputes involving data located in Europe, the *International Principles* is naturally influenced by conflicts of law that arise because of processing and transfer restrictions imposed by the EU Data Protection Directive. Nonetheless, TSC's intent is for the *International Principles* to transcend parochial treatment and instead apply broadly to any data protection law in conflict with U.S. preservation, disclosure, or discovery, regardless of the law at issue or the nation that enacted it. Similarly, while thematically centered on data in electronic form, the *International Principles* is intentionally written to apply equally to protected data in any form, whether recorded electronically, on paper, or on some other media or whether the protected information sought is capable of being conveyed orally.

The *International Principles* was prepared by attorneys from around the globe who specialize in cross-border discovery and data privacy. In formulating the *International Principles*, Working Group 6 has gained the perspective of and would like to thank the many recognized authorities on the subject, including government and compliance enforcement personnel from many countries, as well as members of the Article 29 Working Party, the EU body that provides formal guidance concerning application of the Data Protection Directive. It is through these various sources and many years of study that TSC provides this work to advance the law in an area often thought of as so complex and confounding that it has been largely ignored.

Table of Contents

I. Introduction

Today, litigation transcends geographical boundaries. In the past, when cross-border disputes were less frequent and complex, general international rules for "obtaining evidence abroad" provided sufficient guidance to the parties, counsel, and the courts. Today's commercial globalization has given rise to a complicated matrix of legal, technology, and compliance requirements. This complex international interconnectivity is naturally manifested in international disputes, whether in the context of litigation, arbitration, or regulatory activity. The difficulty in sorting out applicable and sometimes conflicting national laws is one of the most challenging aspects of litigation pertaining to multinational corporations. Nowhere is the tension greater than in discovery for purposes of litigation in the United States, which often conflicts with the significantly narrower scope permitted in other countries, particularly concerning information deemed confidential or subject to data protection laws.

Discovery, generally speaking, is the formal procedure set forth in the Federal Rules of Civil Procedure by which parties to litigation exchange information in order to better understand the facts of the case and the evidence that may be introduced at trial. State courts employ similar rules, many of which have been patterned after the federal rules. Fed. R. Civ. P. 34 applies where one party seeks documents and ESI from another party to the litigation.[1] There are a number of factors that determine the appropriateness of a request for documents under Fed. R. Civ. P. 34. The material sought, for example, must be relevant to a claim or defense in the action.[2] Likewise, the material sought should not be cumulative or duplicative, and it should be available from the source that is most convenient, least burdensome, and least expensive.[3]

[1]The scope of the definition of "document" and "electronically stored information" is quite broad. Fed. R. Civ. P. 34(1)(A) provides for production of "any designated documents or electronically stored information — including writings, drawings, graphs, charts, photographs, sound recordings, images, and other data or data compilations — stored in any medium from which information can be obtained either directly or, if necessary, after translation by the responding party into a reasonably usable form."

[2]Fed. R. Civ. P. 26(b)(1) ("Unless otherwise limited by court order, the scope of discovery is as follows: Parties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense — including the existence, description, nature, custody, condition, and location of any documents or other tangible things and the identity and location of persons who know of any discoverable matter. For good cause, the court may order discovery of any matter relevant to the subject matter involved in the action. Relevant information need not be admissible at the trial if the discovery appears reasonably calculated to lead to the discovery of admissible evidence. All discovery is subject to the limitations imposed by Rule 26(b)(2)(C).")

[3]Fed. R. Civ. P. 26(b)(2)(C) ("On motion or on its own, the court must limit the frequency or extent of discovery otherwise allowed by these rules or by local rule if it determines that: (i) the discovery sought is unreasonably cumulative or duplicative, or can be obtained from some other source that is more convenient, less burdensome, or less expensive; (ii) the party seeking discovery has had ample opportunity to obtain the information by discovery in the action; or (iii) the burden or expense of the proposed discovery outweighs its likely benefit, considering the needs of the case, the amount in controversy, the parties' resources, the importance of the issues at stake in the action, and the importance of the discovery in resolving the issues.")

In the U.S., parties to litigation have a corresponding obligation to preserve information that is relevant to the litigation.[4] The preservation obligation makes it unlawful for any party to destroy, hide, or render unusable information that is relevant to a claim or defense. The preservation obligation arises when a party first learns of the litigation or can be said to have reasonably anticipated it – not merely when litigation is "possible." The purpose of the preservation obligation is to compel a party to maintain and safeguard information that is likely to be requested through discovery, even if that information may be harmful to the party having possession, custody or control over it. Failing to preserve documents and ESI that fall within the scope of the preservation obligation is punishable by the court. The punishment can range from monetary sanctions up to and including a dispositive judgment. The case law recognizes, however, limits to the duty to preserve and that it does not require preservation of every possible piece of data that might be relevant.[5]

Conflicts between U.S. discovery and preservation obligations, on the one hand, and non-U.S. data protection laws, on the other, can arise in several ways. On many occasions, the information requested in U.S. discovery is in the hands of the responding party but subject to the data protection laws of another country. Frequently, however, information that is subject to discovery may be in the hands of another entity that is not a party to the litigation, such as an agent, corporate affiliate or joint venture partner of the litigant, and also subject to the data protection laws of another country. The court, under those circumstances, must first determine whether the responding party has sufficient "control" over the agent or corporate affiliate, or has sufficient "control" over the information sought to require its production in the United States.[6]

Importantly, U.S. courts have the authority to order the production of the information sought even if it is located outside the United States or disclosure is restricted or prohibited by the law of another country. To determine whether to exercise that authority, U.S. courts weigh a number of factors

[4] *Rimkus Consulting Grp., Inc. v. Cammarata*, 688 F.Supp.2d 598, 612–13 (S.D. Tex. 2010) ("Generally, the duty to preserve extends to documents or tangible things (defined by [Fed. R. Civ. P.] 34) by or to individuals 'likely to have discoverable information that the disclosing party may use to support its claims or defenses.'" (quoting *Zubulake v. UBS Warburg LLC (Zubulake IV)*, 220 F.R.D. 212, 217–18 (S.D.N.Y. 2003)); *Victor Stanley, Inc. v. Creative Pipe, Inc.*, 269 F.R.D. 497, 522 (D.Md. 2010) (it "'includes an obligation to identify, locate, and maintain, information that is relevant to specific, predictable, and identifiable litigation,'" quoting The Sedona Conference®, *The Sedona Conference® Commentary On Legal Holds: The Trigger And The Process (August 2007 Public Comment Version)* 3 (2007), (*available at* http://www.thesedonaconference.org/content/miscFiles/Legal_holds.pdf)).

[5] *See, e.g., In re Nat'l Century Fin. Enters.*, 2009 WL 2169174, at *11 (S.D.Ohio July 16, 2009) ("'[A] corporation, upon recognizing the threat of litigation, need not preserve 'every shred of paper, every email or electronic document, and every backup tape.'"')(quoting *Consul. Aluminum Corp. v. Alcoa, Inc.*, 244 F.R.D. 335, 339 (M.D. La. 2006)); *Consol. Aluminum*, 244 F.R.D. at 339 (quoting *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003)); *Danis v. USN Communications, Inc.,* 2000 WL 1694325, at *32 (N.D.Ill. Oct. 23, 2000) ("To be sure, the duty to preserve does not require a litigant to keep every scrap of paper in its file.") (citations omitted); *In re KMART Corp.*, 371 B.R. 823, 842 (Bankr. N.D.Ill. 2007) ("While the scope of the preservation duty is broad, the 'duty to preserve potentially discoverable information does not require a party to keep every scrap of paper' in its file.") (internal citations omitted) (quoting *Danis*, 2000 WL 1694325, at *32).

[6] *Dexia Credit Local v. Rogan*, 231 F.R.D. 538, 541 (N.D.Ill. 2004) (citing *In Re Uranium Antitrust Litig.*, 480 F. Supp. 1138, 1145 (N.D.Ill. 1979)).

pursuant to guidance provided by the U.S. Supreme Court.[7] And, while it is one of the factors that a court should consider before ordering cross-border production, the fact that a party is subject to civil or even criminal sanctions in the foreign jurisdiction may not alone prevent the U.S. court from ordering the production. This means that parties to U.S. litigation may find themselves compelled to preserve and produce information because of U.S. litigation while doing so would violate the law of another country.

The Sedona Conference® Three-Stage Approach for Harmonization of U.S. Discovery and Data Protection Laws.

The *International Principles* is based on the belief that through cooperation, lawyers, parties, judges, and data protection authorities often can avoid conflicts of law concerning discovery before they arise and resolve them when the conflict is unavoidable. Cooperation, in fact, is a hallmark of TSC, as reflected in its much-heralded *Cooperation Proclamation* published in July 2008.[8] The *Cooperation Proclamation* calls upon adversaries to work collaboratively during the discovery phase of litigation as a means of reducing costs and delays.

Here, TSC advances its position that data protection and discovery must co-exist. Data Protection Laws, after all, are not inherently antithetical to U.S. preservation and discovery efforts. U.S. courts and parties often provide protections for personal, confidential, and sensitive information through the use of confidentiality agreements and protective orders. Courts, in fact, have denied discovery in circumstances where privacy rights are deemed more important than the discovery sought by litigants.[9]

To this end, the *International Principles* envisions a three-stage approach for parties seeking to avoid or minimize the conflict that might otherwise arise: (1) a stipulation by the parties or an order from the U.S. court to extend special protections to data covered by data protection laws; (2) a scheduling order by the U.S. court that phases discovery to permit time to implement data protection processes and to determine whether the same or substantially similar information is available from non-protected sources; and (3) implementation of a legitimization plan by the parties to maximize simultaneous compliance with the foreign data protection law and the U.S. discovery obligation. The *International Principles* includes six definitions, six Principles, and a comment section under each Principle to elucidate the purpose of the Principle and provide references to supporting treaties,

[7] *Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa*, 482 U.S. 522 (1987) (approving factors identified in Restatement of Foreign Relations Law of the United States (Revised) § 437(1)(c) (Tent. Draft No. 7, 1986) (approved May 14, 1986)).

[8] The *Sedona Conference® Cooperation Proclamation* has been cited in more than twenty federal court opinions and is formally endorsed by more than one hundred U.S. state and federal judges. It is available without charge at http://www.thesedonaconference.org/content/tsc_cooperation_proclamation. *See also*, The Sedona Conference®, *The Case for Cooperation*, 10 SEDONA CONF. J. 339 (2010 Supp).

[9] *See e.g.*, *Salerno v. Lecia*, 1999 WL 299306 (W.D.N.Y. Mar. 23, 1999) (production of severance package information and personnel files precluded by Directive 95/46/EC and by the German Act on Data Protection); *Volkswagen AG, Relator v. Valdez*, 909 S.W.2d 900, 902 n. 14 (Tex. 1995) (denying request to produce company telephone book protected by German Federal Data Protection Act, BGB1. I, 2954, because production would undermine interests of Germany but no interest of the United States would be undermined if it was not produced, particularly where alternative methods of discovery of same information were available).

case law, and other authorities. TSC believes it is time for a new roadmap, and it is our hope that the *International Principles* will help chart the new course.

II. Definitions

The following definitions apply to the Principles, Commentary, and associated guidance:[10]

1. "Data Controller" is the natural or legal person, public authority, agency, or any other body which alone or jointly with others determines the purposes and means for the processing and transfer of Protected Data.

2. "Data Protection Laws" include any law or regulation that restricts the usage or disclosure of data which requires safeguarding data or imposes obligations in the event of compromises to the security or confidentiality of data. Although focused principally on the relationship between U.S. preservation and discovery obligations and the EU Data Protection Directive, the *International Principles* is intended to apply broadly wherever Data Protection Laws, regardless of national origin, conflict with U.S. preservation and discovery obligations, whether those laws take the form of blocking statutes, privacy regulations, or trade secret protections and whether those laws are enacted by EU member states, other countries or the United States (such as privacy protections afforded by The Health Insurance Portability and Accountability Act (HIPAA) of 1996 (P.L.104-191), a major goal of which is to assure that individuals' health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public's health and well being).[11]

3. "Data Subject" is any person or entity whose Protected Data is or may be processed, transferred, or disclosed.

4. "Processing" includes any operation, activity, use, or application performed upon Protected Data by automatic or other means, such as collection, recording, storage, alteration, retrieval, disclosure, or transfer.

5. "Protected Data" is any data irrespective of its form (e.g., paper, ESI, images, etc.) that is subject to Data Protection Laws.[12]

---

[10]Many of the definitions used in the *International Principles* parallel the terms used in the EU Data Protection Directive. We use these definitions intentionally in order to achieve and maintain a common platform of understanding. It should be noted, however, that the *International Principles* is agnostic relative to the national origin of any Data Protection Law and our usage of similar terminology should not be construed as recognition or acceptance of any particular interpretation given to those terms by others, either now or in the future.

[11]*See e.g.,* U.S. Department of Health and Human, Summary of HIPAA Privacy Rule, available at http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html.

[12]The use of the word "data" in the *International Principles* is intended to convey that the Principles, Commentary, and associated guidance apply to all data, from its lowest level of abstraction to any assembly into information and its recordation on any media.

6. "U.S. Litigation" includes civil and criminal proceedings, government investigations and certain formal audits requiring the discovery of relevant information whether in federal, state, or other U.S. fora. "U.S. Litigation" does not include – and these International Principles are not intended to apply – in criminal proceedings or government investigations governed by a Mutual Legal Assistance treaty.

III. The Sedona Conference® International Principles on Electronic Discovery, Disclosure & Data Protection

Principle 1

With regard to data that is subject to preservation, disclosure, or discovery, courts and parties should demonstrate due respect to the Data Protection Laws of any foreign sovereign and the interests of any person who is subject to or benefits from such laws.

Comment

Principle No. 1 requires the recognition of two fundamental tenets in circumstances where Data Protection Laws are advanced as justification for limitation of preservation or discovery. The first, recognized by the U.S. Supreme Court in *Aérospatiale*,[13] is that international comity[14] compels "due respect" for the laws of other nations and their impact on parties in U.S. litigation subject to, or entitled to benefits under, those laws.[15] The notion of comity is traditionally supported by the U.S. judiciary as presumptively applicable and necessary for the functioning of the international legal system.[16] It has been described as the "the mortar which cements together a brick house."[17] The "due

---

[13] *Supra*, note 11.

[14] As stated by the Restatement (Third) of Foreign Relations Law:

> Comity has been variously conceived and defined. A well-known definition is: 'Comity, in the legal sense, is neither a matter of absolute obligation, on the one hand, nor of mere courtesy and good will, upon the other. But it is the recognition which one nation allows within its territory to the legislative, executive or judicial acts of another nation, having due regard both to international duty and convenience and to the rights of its own citizens or of other persons who are under the protection of its laws.'

Restatement (Third) of Foreign Relations Law § 101 cmt. e (1987) (quoting *Hilton v. Guyot*, 159 U.S. 113, 163-64, 16 S.Ct. 139, 143, 40 L.Ed. 95 (1895)).

[15]

> [W]e have long recognized the demands of comity in suits involving foreign states, either as parties or as sovereigns with a coordinate interest in litigation . . . . American courts should therefore take care to demonstrate due respect for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state.

Aérospatiale, 482 U.S. at 546 (footnote omitted). *Aérospatiale* therefore prohibits U.S. courts from simply disregarding foreign Data Protection Laws; instead, a balancing of domestic and foreign interests is required. *See, e.g., In re Auto. Refinishing Paint Antitrust Litig.*, 358 F.3d 288, 305 n. 20 (2d. Cir. 2004) (noting that subordinate courts are bound to respect international comity and apply *Aérospatiale* balancing test); *Am. Home Assur. Co. v. Société Commerciale Toutélectric*, 128 Cal.Rptr.2d 430, 446 (Cal. Ct. App. 2002) ("We believe California courts will protect these [foreign and domestic] interests when performing the *Aérospatiale* comity analysis, which requires careful consideration of the 'sovereign interests' and other 'important interests' of both jurisdictions."); *Knight v. Ford Motor Co.*, 615 A.2d 297, 302 n. 12 (N.J. Super. 1992) (observing that *Aérospatiale* establishes "the minimum standard of deference to foreign interests" for states and suggesting that states could be even more deferential to foreign law).

[16] *See Laker Airways Ltd. v. Sabena, Belgian World Airlines*, 731 F.2d 909, 937 (D.C. Cir. 1984) and cases cited therein ("'Comity' summarizes in a brief word a complex and elusive concept — the degree of deference that a domestic forum

respect" standard advanced by Principle 1 applies this presumption while recognizing that comity is not without limits.[18] The second tenet, consistent with Fed. R. Civ. P. 11, is that Data Protection Laws should not be advanced for improper purposes or to delay preservation or discovery absent good faith belief that Data Protection Laws conflict with U.S. preservation or discovery requirements.[19]

---

must pay to the act of a foreign government not otherwise binding on the forum. Since comity varies according to the factual circumstances surrounding each claim for its recognition, the absolute boundaries of the duties it imposes are inherently uncertain. However, the central precept of comity teaches that, when possible, the decisions of foreign tribunals should be given effect in domestic courts, since recognition fosters international cooperation and encourages reciprocity, thereby promoting predictability and stability through satisfaction of mutual expectations. The interests of both forums are advanced — the foreign court because its laws and policies have been vindicated; the domestic country because international cooperation and ties have been strengthened. The rule of law is also encouraged, which benefits all nations").

[17] *Id.*

[18] *Id.* at 938. ("However, there are limitations to the application of comity. When the foreign act is inherently inconsistent with the policies underlying comity, domestic recognition could tend either to legitimize the aberration or to encourage retaliation, undercutting the realization of the goals served by comity. No nation is under an unremitting obligation to enforce foreign interests which are fundamentally prejudicial to those of the domestic forum. Thus, from the earliest times, authorities have recognized that the obligation of comity expires when the strong public policies of the forum are vitiated by the foreign act. Case law on the subject is extensive and recognizes the current validity of this exception to comity.")

[19] *See* Fed. R. Civ. P. 11(b):

> By presenting to the court a pleading, written motion, or other paper . . . an attorney. . . certifies that . . . (1) it is not being presented for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; (2) the claims, defenses, and other legal contentions are warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law or for establishing new law; (3) the factual contentions have evidentiary support or, if specifically so identified, will likely have evidentiary support after a reasonable opportunity for further investigation or discovery; and (4) the denials of factual contentions are warranted on the evidence or, if specifically so identified, are reasonably based on belief or a lack of information.

see also, Société Internationale Pour Participations v. Rogers, 357 U.S. 197 (1958) (holding that good faith of the party resisting discovery is a key factor when determining if that party should be sanctioned for failure to comply with discovery requests when foreign law prohibits the requested discovery); Restatement (Third) of Foreign Relations Law § 442 cmt. h (1987) ("Parties to litigation . . . may be required to show that they have made serious efforts before appropriate authorities of states with blocking statutes to secure release or waiver from a prohibition against disclosure. Evidence that parties or targets have actively sought a prohibition against disclosure, or that the information was deliberately moved to a state with blocking legislation, may be regarded as evidence of bad faith and justification for sanctions ….") (Reporter's Note citation omitted); Andrea Patzak, Mark C. Higard & Tim Wybitul, *Cross Border Data Transfer in E-Discoveries in the U.S. and the European and German Privacy Laws*, COMPUTER L. REV. INT'L, (Jan. 2011) at 17 ("By suggesting ways to obey [U.S. discovery orders] while remaining compliant with German data privacy laws, the [U.S.] court may see that the party uses his or her best endeavors to cooperate with the court. That may lead to the court abstaining from sanctions against the company. This holds true even if the company does not disclose the required information if this was discussed with the opposing party in a discovery conference.").

Principle 2

Where full compliance with both Data Protection Laws and preservation, disclosure, and discovery obligations presents a conflict, a party's conduct should be judged by a court or data protection authority under a standard of good faith and reasonableness.

Comment

Where a conflict exists preventing complete and concurrent compliance with Data Protection Laws and U.S. preservation, disclosure, and discovery obligations presents a conflict, this Principle provides guidance to parties who must attempt to meet both obligations, and to courts and data protection authorities that may later be required to evaluate the actions taken by the parties. In both situations, standards of good faith and reasonableness must be applied, particularly when guidance is unavailable, vague, or inconsistent. In the first instance, Data Controllers and parties seeking data for use in legal proceedings must recognize the legitimate interests that both non-U.S. and U.S. obligations serve and seek to minimize friction between the two. When conflicting obligations do arise, Data Controllers and other parties should make good faith and reasonable efforts to respond to those obligations recognizing that full compliance with all obligations may be impracticable. Conversely, when called upon to evaluate the actions and responses, data protection authorities and courts should consider the conflicting obligations and base their judgments in consideration of the Data Controller's or other parties' reasonable and good faith efforts made under the circumstances that existed at the time proportionate to the matters at issue.

For example, a Data Controller must necessarily make determinations regarding the applicability of Data Protection Laws, the country of origin of any Protected Data, and what data is actually protected. Furthermore, the Data Controller must ultimately make determinations about how to effectuate the processing and potential transfer of the Protected Data. Often these determinations may need to be made early, upon "reasonable anticipation" of litigation, before there is an opportunity to know much about the circumstances of the litigation or for consultation with opposing parties, the court, or the appropriate data protection authority.[20] Under Principle 2, the parties' actions – and later judgment of those actions – should be governed by a good faith and reasonableness standard.

Standards of good faith are often invoked in the U.S. in relation to preservation and discovery compliance. However, efforts to define good faith usually involve trying to identify what it is not.[21] That is, if an action is not in "bad faith," then it must be in "good faith," Fed. R. Civ. P. 37(e), for example, protects against certain sanctions if a party is unable to produce ESI because it was lost as a

[20]Under U.S. law, the duty to preserve relevant information arises when litigation is "reasonably anticipated." The Sedona Conference®, *The Sedona Conference® Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265, 269 (2010)("A reasonable anticipation of litigation arises when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation.").

[21]*See* Robert Summers, *'Good Faith' in General Contract Law and the Sales Provisions of the Uniform Commercial Code*, 54 VA. L. REV. 195 (1968). *See also* Robert Summers, *The General Duty of Good Faith – Its Recognition and Conceptualization*, 67 CORNELL L. REV. 810 (1982).

result of the routine, *good faith* operation of an electronic information system.[22] As noted by the Advisory Committee, the term "good faith" in Fed. R. Civ. P. 37(e) is intended to represent a middle ground between negligence, which afforded too little protection to be considered a "safe harbor," and recklessness or intentional misconduct, which might be impossible to establish.[23] The Advisory Committee did not otherwise define good faith except to suggest that good faith may require a party to take affirmative steps to suspend the routine operation of electronic information systems subject to litigation hold and that the nature of the steps taken will bear on the good faith determination.[24]

Courts often assess good faith to determine exemptions from liability or to assess rights and obligations outside the context of discovery.[25] Courts interpreting federal statutes, for example, traditionally have interpreted "good faith" to encompass a subjective standard and "reasonableness" to encompass an objective standard.[26] In defining the two-fold requirement of good faith and reasonableness to avoid liquidated damages under a federal act, one court described the dual standards as such:

> The good faith requirement of the Portal-to-Portal defense requires that the employer have an honest intention to ascertain and follow the dictates of the Act. The additional requirement that the employer have reasonable grounds for believing that his conduct complies with the Act imposes an objective standard by which to judge the employer's behavior. Moreover, an employer may not rely on ignorance alone in meeting the objective test.[27]

What is reasonable for one set of circumstances may not be in another. In the analogous tort context, the California Supreme Court has stated: "Because application of [due care] is inherently situational, the amount of care deemed reasonable in any particular case will vary, while at the same

[22] "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good faith operation of an electronic information system." Fed. R. Civ. P. 37(e). This provision, originally Fed. R. Civ. P. 37(f), was adopted in 2006 and renumbered as Fed. R. Civ. P. 37(e) in 2007.

[23] Judicial Conference of the United States, Committee on Rules of Practice and Procedure, *Report of the Civil Rules Advisory Committee* (Aug. 2004), *available at* http://www.uscourts.gov/RulesAndPolicies/rules/comment2005/CVAug04.pdf at 110-111.

[24] Judicial Conference of the United States, *Report of the Judicial Conference Committee on Rules and Practice and Procedure* (September 2005), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2005.pdf at 34.

[25] *See* Thomas Y. Allman, *Rule 37(f) Meets Its Critics: The Justification for a Limited Preservation Safe Harbor for ESI*, 5 NW. J. TECH. & INTELL. PROP. 1, 3 (2006).

[26] *See Rossi v. Motion Picture Ass'n of America*, 391 F.3d 1000, 1004 (9th Cir. 2004) (interpreting "good faith" as a subjective analysis under the Digital Millennium Copyright Act of 1998, 17 U.S.C. Sec. 512(c)(3)(A)(v) and extensively analyzing similar interpretation under various federal statutes).

[27] *Marshall v. Brunner*, 668 F.2d 748, 753 (3d Cir.1982)(citations and internal quotes omitted).

time the standard of conduct itself remains constant, i.e., due care commensurate with the risk posed by the conduct taking into consideration all relevant circumstances."[28]

Central to the concept of reasonableness is proportionality – the balancing of competing factors to achieve a practical compromise. U.S. courts and data protection authorities should consider a responding party's burdens and complications added by Data Protection obligations when judging compliance using the standard of good faith and reasonableness. Proportionality in discovery is already embodied in the Federal Rules of Civil Procedure. Courts are required to apply the rules to achieve the "just, speedy, and inexpensive determination of every action and proceeding."[29] For example, courts are obliged to restrict discovery where it is unreasonably cumulative; can be obtained from sources that are less expensive; or if the burden of discovery outweighs its likely benefit, considering the needs of the case, the resources of the parties, the importance of the issues at stake, or the importance of the discovery in resolving the issues.[30] Similarly, parties must certify that their discovery requests are not unreasonable, unduly burdensome, or expensive in proportion to the issues or the amount at stake in the litigation.[31] Recent Commentaries published by other TSC Working Groups in the U.S. and Canada have expounded on the application of proportionality to common law discovery.[32]

In the *Aérospatiale* decision, the U.S. Supreme Court, citing the Restatement (Third) of Foreign Relations Law §442(1)(a), stated that U.S. courts, when faced with requests for discovery of information protected by the laws of a foreign sovereign, must use proportionality considerations in framing an appropriate discovery order to balance domestic discovery obligations with the interests of that foreign sovereign. Among the considerations are the importance to the investigation or litigation of the documents or other information requested, the degree of specificity of the request, and the availability of alternative means of securing the information.[33] Principle 2 urges that these same considerations should be used by Data Controllers and parties when they must make decisions concerning conflicting legal obligations, and that courts and data protection authorities use these factors if they are called upon later to evaluate the parties' actions in that regard.

---

[28] *Flowers v. Torrance Memorial Hosp. Med. Ctr.* 8 Cal. 4th 992, 997 (1994).

[29] *See* Fed. R. Civ. P. 1

[30] Fed. R. Civ. P. 26(b)(2)(C)(iii)

[31] Fed. R. Civ. P. 26(g)(1)((B)(iii) *See also, Mancia v. Mayflower Textile Servs. Co.*, 253 F.R.D. 354, 359 (D.Md. 2008)("[T]he failure to engage in discovery as required by [Fed. R. Civ. P.] 26(g) is one reason why the cost of discovery is so widely criticized as being excessive to the point of pricing litigants out of court.")

[32] The Sedona Conference®, *The Sedona Conference® Commentary on Proportionality in Electronic Discovery*, 11 SEDONA CONF. J. 289 (2010); The Sedona Conference®, *The Sedona Canada℠ Commentary on Proportionality in Electronic Disclosure and Discovery* (October 2010)(available at http://www.thesedonaconference.org/dltForm?did=Canadian__Proportianality.pdf); *see also* The Sedona Conference®, *The Sedona Conference® Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265 at 265, 269 (2010).

[33] *Aérospatiale*, 482 U.S. at 544 (citing Restatement (Third) of Foreign Relations Law §442(1)(a)).

Principle 3

Preservation, disclosure, and discovery of Protected Data should be limited in scope to that which is relevant and necessary to support any party's claim or defense in order to minimize conflicts of law and impact on the Data Subject.

Comment

It is beyond the scope of the *International Principles* to define the contours of the duty to preserve, disclose, or produce Protected Data under U.S. law. Principle 3 does not attempt to define or modify these obligations. Principle 3 instead recognizes that the Data Controller (who usually is the responding party), the requesting party, and the court all have obligations to protect the rights of Data Subjects and to minimize conflicts with Data Protection Laws. Both goals can be achieved through cooperation and stipulation or court order.

The Federal Rules of Civil Procedure, for example, call for the disclosure of certain information early in the proceedings and without awaiting formal discovery requests. Fed. R. Civ. P. 26(a)(1)(A)(ii) requires disclosure of a copy of, or a description by category and location of, all documents, ESI, and tangible things in the possession, custody, or control of the party *and that the disclosing party may use to support its claims or defenses*, unless solely for impeachment. Principle 3 does not purport to expand or restrict the scope of early disclosure requirements under Fed. R. Civ. P. 26(a)(1) but emphasizes that a greater degree of scrutiny is necessary in order to protect the rights of the Data Subject and to minimize conflicts of law.

If it is questionable whether the Protected Data should be disclosed – for example, if the same or equivalent information may be available from a domestic source – the Data Controller should seek to prevent disclosure, at least as an interim measure, by means of a stipulation or court order until the matter can be conclusively determined. Conversely, Protected Data that clearly does not fall within the scope of early disclosure should not be produced even though, for example, there may be a strategic advantage for the Data Controller to do so. Protected Data that clearly must be disclosed under a rule like Fed. R. Civ. P. 26(a)(1)(A) should be disclosed only after appropriate measures are taken to comply with the applicable Data Protection Laws, which likely will include measures to restrict distribution and maintain confidentiality, which often can be achieved through the use of stipulations and court orders, as described later in the *International Principles*.

This same heightened level of scrutiny is necessary at the preservation and discovery stages of litigation. Principle 3 recognizes that discovery of Protected Data should be limited initially to that which is "relevant and necessary to support any party's claim or defense." Though frequently asserted erroneously by lawyers – and sometimes wrongly relied on by judges – the scope of Fed. R. Civ. P. 26(b)(1) discovery obligation *only* extends to information which appears to be reasonably calculated to lead to the discovery of admissible evidence *if it is first relevant*.[34] Courts especially emphasize this

[34]Discovery is not unlimited in U.S. litigation. The Federal Rules of Civil Procedure have been amended several times in order to correct perceived abuses of discovery. One of the most significant changes occurred in 2000 when Fed. R. Civ. P. 26(b)(1) was modified to create a "two-tiered" approach to the scope of discovery. Prior to the 2000 amendment, the Rule permitted discovery of all information "relevant to the subject matter involved in the pending actions." As the Rule currently reads, a party is only entitled, initially, to information that is relevant to any party's claim or defense in the case,

point when it comes to Protected Data, requiring proof that the information sought is *necessary, vital, or crucial* to a claim or defense before compelling production, in light of comity concerns.[35] Narrowing the focus of preservation and discovery through stipulations and court orders can have the same effect.

This heightened level of scrutiny aligns with the approach taken by of the Article 29 Working Party toward EU data privacy obligations in the context of U.S. discovery, which notes:

> There is a duty upon the data controllers involved in litigation to take such steps as are appropriate (in view of the sensitivity of the data in question and of alternative sources of the information) to limit the discovery of personal data to that which is objectively relevant to the issues being litigated. There are various stages to this filtering activity including determining the information that is relevant to the case, then moving on to assessing the extent to which this includes personal data. Once personal data has been identified, the data controller would need to consider whether it is necessary for all of the personal data to be processed, or for example, could it be produced in a more anonymised or redacted form. Where the identity of the individual data [subjects] is not relevant to the cause of action in the litigation, there is no need to provide such information in the first instance. However, at a later stage it may be required by the court which may give rise to another 'filtering' process. In most cases it will be sufficient to provide the personal data in a pseudonymised form with individual identifiers other than the data subject's name.[36]

There are many opportunities for parties and courts to put Principle 3 into practice, thereby avoiding or at least minimizing conflicts of laws and damage to the rights of Data Subjects, as the following examples demonstrate:

A. Limit the scope of the request

It is the responsibility of the parties to work together to limit the scope of preservation, processing, and production to that which is relevant and necessary to support a claim or defense. Absent an agreement between the parties, the court has authority to limit the scope of the inquiry and should do so when appropriate. The scope of document requests can be narrowed in a variety of ways. Two particular ways include (1) using requests with greater specificity and (2) restricting the breadth of requests to fewer, more relevant custodians, allowing an iterative process to extend the request, if needed.

---

as stated in the pleadings. Any other information relevant to the broader subject matter of the dispute is not properly within the scope of discovery without the prior permission of the court after the requesting party has demonstrated "good cause" for the information sought.

[35] *See e.g., In re Vitamins Antitrust Litig.*, No. 99-197, 2001 WL 1049433, at *10 n.20 (D.D.C. June 20, 2001); *Strauss v. Credit Lyonnais, S.A.*, 249 F.R.D. 429 (E.D.N.Y. 2008).

[36] Article 29 Data Protection Working Party, *Working Document 1/2009 on pre-trial discovery for cross-border civil litigation*, 00339/09/EN, WP 158, p. 10 (adopted Feb. 11, 2009) (describing possible methods to produce documents containing personal data in U.S. litigation in a manner that does not violate the EU Directive).

B. Discovery with specificity

In the United States, a requesting party often makes broad requests for disclosure and production of relevant information. Phrases such as "any and all" still appear in such requests, despite the best efforts of courts to encourage targeted discovery.[37] Most courts have required that production of materials that implicate foreign Data Protection Laws must be relevant and also necessary or vital to the litigation.[38]

A more narrowly tailored request that clarifies the particular scope of documents requested for a particular claim or defense, however, more closely comports with the spirit and the letter of most Data Protection Laws.

During the course of discovery, Data Controllers should discuss with the requesting party, where possible, narrowing the scope of discovery, especially with respect to inclusion of Protected Data. To the extent that the parties fail to reach consensus on the narrowing of discovery requests, the judiciary should act in the interests of minimizing the conflicts of laws by endorsing a narrowing of broad discovery requests.[39]

C. Phased discovery

A second consideration is the breadth of a request. In litigation many, if not most, of the claims and defenses can be resolved with discovery of a few highly relevant custodians as opposed to a large number of custodians who may possess data or information of only marginal relevance. Structuring disclosure and production on key players initially can significantly minimize the volume and breadth of Protected Data at issue, as well as the impact on Data Subjects, while preserving the ability to delve deeper into particular claims and defenses in later requests and productions, if necessary.[40]

---

[37]More recently, however, particularly following the amendments to Fed. R. Civ. P. 26, there has been broader oversight by courts requiring more tailored discovery. These early glimpses may telegraph a paradigm shift in judicial thinking whereby "fishing expeditions" will be a thing of the past.

[38]*See Aérospatiale*, 482 U.S. at 542 (noting that district courts must closely supervise the proceedings when "necessary to seek evidence abroad" and noting that foreign documents at issue were "vital" to the litigation); *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1475 (9th Cir. 1992) (noting unwillingness to override foreign laws unless outcome of litigation stands or falls on the discovery order); *Volkswagen, A.G. v. Valdez*, 909 S.W.2d 900, 903 (Tex. 1995) (holding that corporate phone book need not be produced if protected by German law and where evidence bore "little importance to the present litigation").

[39]*See Aérospatiale*, 482 U.S. at 542 ("When it is necessary to seek evidence abroad . . . the district court must supervise pretrial proceedings particularly closely to prevent discovery abuses"); *Devon Robotics v. De Viedma,* 2010 WL 3985877 (E.D.Pa. Oct. 8, 2010) (ordering production despite potential conflict with Italian data protection law, and citing the "specifically tailored" nature of the discovery requests as well as other factors as the basis for ruling); *Bodner v. Paribas*, 202 F.R.D. 370, 376-77 (E.D.N.Y. 2000) (quoting directive from *Aérospatiale* to the district courts to "exercise special vigilance" with respect to foreign discovery and noting that "discovery has, at this time, been significantly narrowed, and will continue only under the close supervision of this court").

[40]Andrea Patzak, Mark C. Hilgard & Tim Wybitul, *Cross Border Data Transfer in E-Discoveries in the U.S. and the European and German Privacy Laws*, COMPUTER L. REV. INT'L at 18 (Jan. 2011) (recommending that litigants urge U.S. courts to reduce the amount of Protected Data subject to disclosure to "only certain necessary data.").

Phased Discovery is contemplated by the second stage of the three-stage approach advanced by the *International Principles*, which recommends the use of a scheduling order whereby parties agree on —or the court orders—deadlines and sequencing for completion of discovery. The primary purpose of the scheduling order is to ensure sufficient time to "legitimize" the processing and transfer of Protected Data (legitimization is the third stage of the approach). Scheduling or phasing also serves to demonstrate respect for Data Protection Laws because, by phasing, information that is not subject to Data Protection Laws can be identified, collected, processed, and produced first, thereby minimizing the likelihood that the same or similar information will be required from sources subject to Data Protection Laws.[41]

A chronological phasing included in a scheduling order might be sequenced as follows:

1. Data from U.S. sources that are probably not subject to Data Protection Laws;

2. As necessary, data from U.S. sources that are potentially subject to Data Protection Laws (typically U.S. Data Protection Laws such as Gramm–Leach–Bliley and HIPAA);

3. Data from foreign sources that are probably not subject to Data Protection Laws; and

4. As necessary, data from foreign sources that are potentially subject to Data Protection Laws.

In the development of the scheduling order, each Data Protection Law and the ease or complexity of processing and transferring Protected Data thereunder would be considered separately, recognizing that different timetables will require flexibility.

D. Minimize the production of protected data

After the scope of the request is considered, Data Controllers may take steps to further minimize conflicts of law and potential impact on Data Subjects. These additional steps include the filtering of data, substitution of alternative data, and limitations on the format of production. Examples of filtering include the use of simple or complex search terms, statistical sampling, semantic clustering, voting systems, neural networks, linguistic analysis, natural language queries, or human review.[42] Culling, when using any of these techniques to minimize the production of Protected Data, is generally best undertaken as early in the process as possible to gain the greatest efficiencies. The Article 29 Working Party has expressed a preference that "filtering" (culling) and similar treatment

[41] It should be noted, however, that consistent with the second tenet of Principle No. 1, phasing of discovery should not be advanced for an improper purpose or to delay preservation or discovery.

[42] A neural network is a mathematical model usually defined by nodes (inputs and outputs) and connectors. A set of training data is run through the system with defined outputs. The system develops weights for the nodes and connectors based on the training set, and then uses the weights to calculate likely outputs for new data. Voting is the application of multiple predictive models to the same set of documents and then choosing the most likely answer based on how the various systems classified a given document (e.g., relevant or non-relevant). Both neural networks and voting are usually "supervised learning," which means that a sample of pre-categorized documents is used to train the system(s) that then predict the classification(s) of the remaining documents.

to Protected Data take place in the EU to minimize the exposure of non-relevant and unnecessary Protected Data to disclosure risks.[43]

E. Substitution of data

The substitution of one data source for another, or one data element for another, may be appropriate in a particular production to minimize the disclosure of Protected Data if the substitution can be done in a way that does not inappropriately compromise the usability of the produced data. Thus, the impact on Data Subjects may be minimized when the Data Controller relies on alternative sources of information that may be less inclusive of Protected Data but ultimately convey an equally adequate level of otherwise relevant and responsive information.

F. Limitations on the format of production

The choice of one production format over another may be appropriate in a particular production to minimize the disclosure of Protected Data if it can be done in a way that does not inappropriately compromise the usability of the produced data. For example, producing data in an image format with a text-searchable load file may be preferable to production in its native format to shield disclosure of Protected Data through the production of metadata or because of redaction difficulties with native format.

[43] In WP158 the Article 29 Working Party references "filtering" two times. First, under "necessary for the purposes of a legitimate interest" the Working Party recommends that non-relevant data be filtered "possibly by a trusted third party in the European Union." Second, under "Proportionality" it is recommended that any filtering should be carried out locally in the country in which the Personal Data is found before the Personal Data that is deemed to be relevant to the litigation is transferred to another jurisdiction outside the EU ("[I]t may be that this would require the services of a trusted third party in a Member State.")

Principle 4

Where a conflict exists between Data Protection Laws and preservation, disclosure, or discovery obligations, a stipulation or court order should be employed to protect Protected Data and minimize the conflict.

Comment

When a conflict exists between a requesting party's U.S. litigation rights regarding relevant data and a responding party's Protected Data obligations, the parties may act creatively and work cooperatively to enter into stipulations or agreements that create private legal obligations. Parties with data disclosure and data privacy conflicts are encouraged to draft stipulations (in the form of a stipulated court order, when possible) that acknowledge a responding party's conflicting burdens and assign duties to the requesting party to protect and dispose of Protected Data in a manner consistent with the applicable Data Protection Laws. If the parties cannot cooperatively reach stipulations regarding data protection, then the responding party should seek a protective order. A protective order is commonly used to protect privacy in discovery.[44]

The three-stage approach advanced by the *International Principles* suggests conflict resolution through stipulations and protective orders. The approach envisions efforts by parties to avoid and minimize potential conflicts of law, including seeking an order from the U.S. court that extends special protections to data covered by Data Protection Laws; a separate order that schedules or phases discovery, and a protocol or legitimization plan that maximizes simultaneous compliance with the Data Protection Law and the preservation, disclosure, and discovery obligations. Depending on the circumstances of the case, some or all of these steps should be applied, recognizing that a stipulation between the parties may be appropriate in circumstances where a court order is not necessary or the matter is not yet before a court.

Protective Order or Stipulation

The protective order or stipulation should, where possible, be negotiated between the parties and agreed upon, but it may be submitted to the court unilaterally if cooperation is not forthcoming. A protective order signifies to data protection authorities that the Data Protection Laws are respected and that Protected Data will be treated appropriately by the parties and, in the case of a protective order, under the auspices and protections of the U.S. court.[45] *The Sedona Conference® Model Protected*

[44] *Seattle Times Co. v. Rhinehart,* 467 U.S. 20, 35-36 (1984)("The prevention of the abuse that can attend the coerced production of information under a State's discovery rule is sufficient justification for the authorization of protective orders").

[45] While protective orders entered by a state or federal court will be accorded due respect by other U.S. courts in civil litigation, documents transmitted to the U.S. under a protective order may still be subject to disclosure under a grand jury subpoena in a criminal matter. Federal Circuit Courts of Appeals are split in their treatment of grand jury subpoenas for documents subject to a protective order. Three circuits, the 4th, 9th, and 11th, apply a *per se* rule, holding that once documents are within the jurisdiction of the grand jury, they are subject to subpoena, regardless of the existence of a protective order. *See, e.g.*, *In re Grand Jury Subpoena*, 646 F. 3d 159 (4th Cir. 2011). Two circuits, the 1st and 3d, apply a balancing test in which there is a strong presumption in favor of enforcing the grand jury subpoena, which may yield to a civil protective order under exceptional circumstances. *See, e.g.*, *In re Grand Jury*, 286 F. 3d 153, 162 (3d Cir. 2002). The 2d Circuit gives due deference to the civil protective order and will only allow the grand jury subpoena to proceed upon

Data Protective Order, set forth in Appendix B, contains several provisions that extend protections to Protected Data in a format that can be easily tailored to a specific matter as negotiated between the parties or unilaterally ordered by the court.

Scheduling Stipulation or Order

Through the use of a scheduling stipulation or order the parties may agree on, or the court may order deadlines and sequencing for completion of discovery. The primary purpose of the scheduling order is to ensure sufficient time to "legitimize" the processing and transfer of Protected Data. Scheduling contemplates that information that is not subject to data protection laws would be identified, collected, processed, and produced first, thereby minimizing the likelihood that the same or similar information will be required from sources subject to Data Protection Laws.

Legitimization Plan

In this third prong, the party responding to discovery would develop a plan setting forth the methodology by which it contemplates preserving, processing, transferring, and producing Protected Data. The legitimization plan should be tailored to each applicable Data Protection Law and should seek to comply with those requirements, as well as with U.S. preservation and discovery obligations. The legitimization plan may be prepared unilaterally or in conjunction with the requesting party and/or data protection authorities. The plan can help to demonstrate compliance with applicable laws and to identify and thereafter resolve processing and transfer concerns before they materialize. The Legitimization Plan is also useful to prepare *The Sedona Conference® Cross-Border Data Safeguarding Process + Transfer Protocol* set forth in Appendix C and described in the Comment to Principle 5.

a showing that the civil protective order was improvidently granted. *Palmieri v. State of New York*, 779 F. 2d 861, 866 (2d Cir. 1985).

Principle 5

A Data Controller subject to preservation, disclosure, or discovery obligations should be prepared to demonstrate that data protection obligations have been addressed and that appropriate data protection safeguards have been instituted.

Comment

Data Controllers often find themselves subject to Data Protection Laws in one country that may conflict with broad preservation, discovery, or disclosure obligations in U.S. Litigation. Under such circumstances, the Data Controller may find it beneficial to prepare the documentation following *The Sedona Conference® Cross-Border Data Safeguarding Process + Transfer Protocol* set forth in Appendix C. The *Protocol* recommends the steps that a Data Controller should undertake to comply with the relevant Data Protection Law as well as U.S. preservation, discovery, and disclosure obligations. TSC believes that including the appropriate persons in the execution and documentation of the *Protocol* will help demonstrate good faith, reasonableness, and proportionality. For example, involving a company's Data Privacy Officer, from the start, in developing protocols for processing and transfers of Protected Data, and then validating them with local Data Protection Authorities, reflects well on the company's commitment to protect the rights of the Data Subject.

Documentation of steps taken under the *Protocol* may accompany the Protected Data (like a modern day bill of lading that accompanies physical cargo) from one jurisdiction to another. The documentation may provide some or all of the following information:

1. The purpose for which the Protected Data is being collected and transferred (this would include a brief description of the litigation, investigation, or matter in the United States as well as the identification of the intended recipients of the Protected Data);

2. Data Protection Laws at issue should be identified, as well as their significance. The specific sources of Protected Data and their location should be identified, including the locations from which and to where the Protected Data will be transferred;

3. An identification of reasonable measures taken to narrow and cull the processing and transfer of Protected Data to only that which is relevant and necessary for U.S. preservation and discovery purposes. This may include, for example, the use of preliminary questionnaires and interviews, the use of tools and processes to conduct iterative search and retrieval, and de-duplication;

4. The identification of categories of Protected Data collected (e.g., information that is likely to identify the Data Subject, sensitive Personal Data, trade secret data, restricted data);

5. Confirmation that the Protected Data is subject to a protective order or stipulation that, for example, restricts its use and dissemination of data, imposes confidentiality, compels security measures, provides for Data Subject access, and restricts onward transfer (attaching a copy of the protective order or stipulation);

6. Description of the processes and transfers concerning Protected Data to demonstrate transparency. This may include the steps taken (if and as appropriate or feasible) to make information available or to notify Data Subjects of processing, transfer, and onward transfer of Protected Data (e.g., posting notice, internal circular requesting consent);

7. Description of the steps taken to make the remaining Protected Data secure prior to onward transfer (e.g., third-party agreements, nature and type of encryption, access limitation, password protection);

8. Compliance with obligations (if any) to notify others with oversight of data protection (e.g., company's Data Protection Officer, government's Data Protection Authority, works council);

9. Basis upon which Protected Data is transferred, using for example one of the three classical methods for legitimizing the transfer of Protected Data (Safe Harbor, model contractual clauses, and binding corporate rules), coupled with a protective order for the onward transfer imposing like obligations on the requesting party or otherwise as required by the jurisdiction;

10. Disposition of processed and transferred Protected Data when no longer needed to fulfill U.S. obligations of the given matter at hand (e.g., destruction or return of Protected Data); and;

11. Identification and signature of the person or persons ultimately responsible for processing and transferring Protected Data and affixing signatures signifying the steps recorded have been taken.

Use of the *Protocol* addresses data protection concerns by providing proof that reasonable efforts have been undertaken to provide adequate safeguards to Protected Data processed or transferred for purposes of U.S. Litigation, while also recognizing the broad discovery and disclosure obligations many global companies face when subject to government investigations or litigation in the United States.

Principle 6

Data Controllers should retain Protected Data only as long as necessary to satisfy legal or business needs. While a legal action is pending or remains reasonably anticipated, Data Controllers should preserve relevant information, including relevant Protected Data, with appropriate data safeguards.

Comment

The purpose of Principle 6 is to provide guidance to Data Controllers regarding records retention generally, as well as the specific scope and duration of their obligation to preserve Protected Data that is relevant to U.S. Litigation.

The goal of this Principle is to reinforce the records management axiom that records and information do not need to be preserved when they are no longer needed for business or legal reasons. This principle also recognizes that the potential conflict between discovery obligations and Data Protection Laws is lessened by reducing the amount of data that organizations create and retain before preservation and discovery obligations attach.

Many organizations worldwide have become electronic data hoarders. While the retention of paper-based information had tangible physical consequences and costs, it has become relatively inexpensive and more expedient to expand storage capacity rather than to apply records management lifecycle discipline to ESI. There are numerous direct and indirect costs and risks associated with unbridled accumulation and retention of data. Legal risks may also arise, especially in the context of data protected by Data Protection Laws, in the over-retention of information.

Organizations should take good faith, reasonable efforts to retain, manage, and dispose of inactive data both on a prospective and retrospective basis. Consistent with the opinion of the U.S. Supreme Court in *Arthur Andersen LLP v. United States*,[46] persons and organizations need not keep all information forever. Rather, reasonable and systematic records management rules can be applied, so long as they are applied uniformly, and not in a fashion to avoid a litigant's common law duty to preserve relevant information, once the litigant is on notice of actual or reasonably anticipated litigation. Organizations are encouraged to implement data privacy and data protection technologies to further this goal and to design information systems and processes with data protection in mind, e.g. privacy by design.[47]

[46] 544 U.S. 696, 724 (2005) "'Document retention policies,' which are created in part to keep certain information from getting into the hands of others, including the Government, are common in business. It is, of course, not wrongful for a manager to instruct his employees to comply with a valid document retention policy under ordinary circumstances.") [citation omitted] *See also, The Sedona Conference® Commentary on Inactive Information Sources* (forthcoming in 2012).

[47] "Privacy by design" means that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use, and ultimate disposal. *See* European Commission, *A Digital Agenda for Europe*, EUC, 26/8/2010, COM(2010) 245 final/2.

Similarly, European data protection authorities stress that "data minimization" is an essential strategy for data protection. The less Personal Data that is collected or retained by an organization, the lower the costs and risks to data protection.[48]

This Principle reinforces the notion that the obligation to preserve Protected Data for the purposes of litigation is accompanied by a corresponding obligation to take reasonable steps to protect the reliability, integrity, access, and confidentiality of the data while it is being preserved. This includes meaningful efforts to implement "privacy by design" protections into new ESI systems, consistent with the call of the Article 29 Working Party's "The Future of Privacy" document.[49] Data Controllers should continue to observe substantive data protection and confidentiality requirements under Data Protection Laws, such as those implemented by member states under the EU Data Protection Directive, even if they are merely distributing notice of and requiring compliance with a legal hold notice relating to relevant Protected Data.

This Principle also makes clear that the preservation obligation is limited in duration to the time that a legal action is pending or remains reasonably anticipated. A prior Commentary from TSC Working Group 1 explains that "reasonable anticipation of litigation arises when an organization is on notice of a credible probability that it will become involved in litigation, seriously contemplates initiating litigation, or when it takes specific actions to commence litigation."[50] This limitation should provide assurance to non-U.S. data protection and privacy officials that the duty to preserve is not based upon mere conjecture, supposition, or possibility that legal action may occur at some time in the future.[51]

[48] Article 6(1)(c) of the Data Protection Directive; *Guide to Data Protection* published by the UK Information Commissioner, p. 59.

[49] Article 29 Data Protection Working Party, Working Party on Police and Justice, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168 (adopted Dec.1 2009) *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf.

[50] The Sedona Conference®, *The Sedona Conference® Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265, 269 (2010).

[51] Unfortunately, there is no black-and-white definition of when litigation is deemed to be "reasonably anticipated." Like many legal standards throughout the world, it depends upon the facts and circumstances of the particular situation. More frequently than not, preservation conduct is judged long after the fact. As a result, additional guidance on this issue will be welcomed by both U.S. and non-U.S.-based litigants.

Appendix A: Bibliography

COURT OPINIONS CITED

Am. Home Assur. Co. v. Société Commerciale Toutelectric, 128 Cal.Rptr. 2d 430 (Cal. Ct. App. 2002)

Arthur Andersen LLP v. United States, 544 U.S. 696 (2005)

Bodner v. Paribas, 202 F.R.D. 370 (E.D.N.Y. 2000)

Consul. Aluminum Corp. v. Alcoa, Inc., 244 F.R.D. 335 (M.D.La. 2006)

Danis v. USN Communications, Inc., 2000 WL 1694325 (N.D.Ill. Oct. 23, 2000)

Devon Robotics v. De Viedma, 2010 WL 3985877 (E.D.Pa. Oct. 8, 2010)

Dexia Credit Local v. Rogan, 231 F.R.D. 538 (N.D.Ill. 2004)

Flowers v. Torrance Memorial Hosp. Med. Ctr. 8 Cal. 4th 992 (Sup.Ct.Cal. 1994)

Hilton v. Guyot, 159 U.S. 113, 16 S.Ct. 139, 40 L.Ed. 95 (1895)

In re Auto. Refinishing Paint Antitrust Litig., 358 F.3d 288 (2d. Cir. 2004)

In re Grand Jury, 286 F. 3d 153 (3d Cir. 2002)

In re Grand Jury Subpoena, 646 F. 3d 159 (4th Cir. 2011)

In re KMART Corp., 371 B.R. 823 (Bankr. N.D.Ill. 2007)

In re Nat'l Century Fin. Enters., 2009 WL 2169174 (S.D.Ohio July 16, 2009)

In Re Uranium Antitrust Litig., 480 F. Supp. 1138 (N.D.Ill. 1979)

In re Vitamins Antitrust Litig., 2001 WL 1049433 (D.D.C. June 20, 2001)

Knight v. Ford Motor Co., 615 A.2d 297 (N.J.Super. 1992)

Laker Airways Ltd. v. Sabena, Belgian World Airlines, 731 F.2d 909 (D.C. Cir. 1984)

Mancia v. Mayflower Textile Servs. Co., 253 F.R.D. 354 (D.Md. 2008)

Marshall v. Brunner, 668 F.2d 748 (3d Cir.1982)

Palmieri v. State of New York, 779 F.2d 861 (2d Cir. 1985)

Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468 (9th Cir. 1992)

Rimkus Consulting Grp., Inc. v. Cammarata, 688 F.Supp.2d 598 (S.D.Tex. 2010)

Rossi v. Motion Picture Ass'n of America, 391 F.3d 1000 (9th Cir. 2004)

Salerno v. Lecia, 1999 WL 299306 (W.D.N.Y. Mar. 23, 1999)

Seattle Times Co. v. Rhinehart, 467 U.S. 20 (1984)

Société Internationale Pour Participations v. Rogers, 357 U.S. 197 (1958)

Société Nationale Industrielle Aérospatiale v. United States District Court for the Southern District of Iowa, 482 U.S. 522 (1987)

Strauss v. Credit Lyonnais, S.A., 249 F.R.D. 429 (E.D.N.Y. 2008)

Victor Stanley, Inc. v. Creative Pipe, Inc., 269 F.R.D. 497 (D.Md. 2010)

Volkswagen AG, Relator v. Valdez, 909 S.W.2d 900 (Tex. 1995)

Zubulake v. UBS Warburg LLC (Zubulake IV), 220 F.R.D. 212 (S.D.N.Y. 2003)

U.S. RULES CITED

Fed. R. Civ. P. 1
Fed. R. Civ. P. 11
Fed. R. Civ. P. 11(b)
Fed. R. Civ. P. 26
Fed. R. Civ. P. 26(a)(1)
Fed. R. Civ. P. 26(a)(1)(B)
Fed. R. Civ. P. 26(b)(1)
Fed. R. Civ. P. 26(b)(2)(i), (ii), and (iii)
Fed. R. Civ. P. 34
Fed. R. Civ. P. 34(1)(A)
Fed. R. Civ. P. 37(f)

U.S STATUTES CITED

Digital Millennium Copyright Act of 1998, 17 U.S.C. §512(c)(3)(A)(v)

Uniform Commercial Code

NON-U.S. AUTHORITIES CITED

Article 29 Data Protection Working Party, *Working Document 1/2009 on pre-trial discovery for cross-border civil litigation*, 00339/09/EN, WP 158 (adopted Feb. 11, 2009)
Article 29 Data Protection Working Party, Working Party on Police and Justice, *The Future of Privacy: Joint contribution to the Consultation of the European Commission on the legal framework for the fundamental right to protection of personal data*, WP 168 (adopted Dec. 1, 2009), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp168_en.pdf

Article 6(1)(c) of the Data Protection Directive; Guide to Data Protection published by the UK Information Commissioner

Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

European Commission, *A Digital Agenda for Europe*, EUC, 26/8/2010, COM(2010) 245 final/2

OTHER AUTHORITIES CITED

Allman, Thomas Y., *Rule 37(f) Meets Its Critics: The Justification for a Limited Preservation Safe Harbor for ESI*, 5 NW. J. TECH. & INTELL. PROP. 1 (2006)

Daley, M. James, *Information Age Catch 22: The Challenge of Technology to Cross-Border Disclosure and Data Privacy*, 12 SEDONA CONF. J. 121 (2011)

Judicial Conference of the United States, Committee on Rules of Practice and Procedure, *Report of the Civil Rules Advisory Committee* (Aug. 2004), *available at* http://www.uscourts.gov/RulesAndPolicies/rules/comment2005/CVAug04.pdf

Judicial Conference of the United States, *Report of the Judicial Conference Committee on Rules and Practice and Procedure* (Sept. 2005), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/Reports/ST09-2005.pdf at 34

Patzak, Andrea, Mark C. Hilgard and Tim Wybitul, *Cross Border Data Transfer in E-Discoveries in the U.S. and the European and German Privacy Laws*, COMPUTER L. REV. INT'L 13 (Jan. 2011)

Summers, Robert, *'Good Faith' in General Contract Law and the Sales Provisions of the Uniform Commercial Code*, 54 VA. L. REV. 195 (1968)

Summers, Robert, *The General Duty of Good Faith – Its Recognition and Conceptualization*, 67 CORNELL L. REV. 810 (1982)

The American Law Institute, *Restatement of the Law, Third, Foreign Relations Law of the United States* §101 cmt. e (1987); §442 cmt. h (1987); §442(1)(a)

The American Law Institute, *Restatement of the Law, Third, Foreign Relations Law of the United States (Revised)* § 437(1)(c) (Tent. Draft No. 7, 1986) (approved May 14, 1986)

The Sedona Conference®, *The Case for Cooperation*, 10 SEDONA CONF. J. 339 (2010 Supp)

The Sedona Conference®, *The Sedona Canada Commentary on Proportionality in Electronic Disclosure and Discovery* (October 2010)(available at http://www.thesedonaconference.org/dltForm?did=Canadian__Proportianality.pdf)

The Sedona Conference®, *The Sedona Conference® Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265 (2010)

U.S. Department of Health and Human, *Summary of HIPAA Privacy Rule*, *available at* http://www.hhs.gov/ocr/privacy/hipaa/understanding/summary/index.html

Appendix B:

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

_____,	)	
	)	
Plaintiff.	)	Case No.: _____
	)	
v.	)	**Stipulated Protective Order Re: Protected Data**
	)	
_____,	)	
	)	
Defendant.	)	
	)	

WHEREAS, to facilitate the production and receipt of information during discovery in the above-captioned litigation (the "Litigation"), the parties agree and stipulate, through their respective counsel, to the entry of the following Protective Order for the protection of Confidential and Highly Confidential Materials (as defined herein) that may be produced or otherwise disclosed during the course of this Litigation by or on behalf of any party or non-party. The Court has been fully advised in the premises and has found good cause for its entry.

Accordingly, IT IS HEREBY ORDERED that the terms and conditions of this Protective Order shall govern the handling of discovery materials in the Litigation:

1. **Applicability of Order:** This Order does not and will not govern any trial proceedings in this Litigation, but will otherwise be applicable to and govern the handling of documents, depositions, deposition exhibits, interrogatory responses, responses to requests for admissions, responses to requests for production of documents, and all other discovery obtained

pursuant to the Federal Rules of Civil Procedure by or from, or produced on behalf of, a party in connection with the Litigation (this information hereinafter referred to as "Discovery Material"). As used herein, "Producing Party" or "Disclosing Party" shall refer to the parties to this action that give testimony or produce documents or other information and to non-parties for purposes of Section 10, "Receiving Party" shall refer to the parties to this action that receive such information, and "Authorized Recipient" shall refer to any person or entity authorized by Sections 11 and 12 of this Order to obtain access to Confidential Material, Highly Confidential Material, or the contents of such Material.

2. **Designation of Material**: Any Producing Party may designate Discovery Material that is in its possession, custody or control to be produced to a Receiving Party as "Confidential" or "Highly Confidential" under the terms of this Order if the Producing Party in good faith reasonably believes that such Discovery Material contains non-public, confidential material as defined in Sections 4 and 5 below (hereinafter "Confidential Material" or "Highly Confidential Material").

3. **Exercise of Restraint and Care in Designating Material for Protection**. Each Producing Party that designates information or items for protection under this Order must take care to limit any such designation to specific material that qualifies under the appropriate standards. Mass, indiscriminate, or routinized designations are prohibited.

4. **Confidential Material**: For purposes of this Order, Confidential Material is any information that a party believes in good faith to be confidential or sensitive information, including, but not limited to, trade secrets, research, design, development, financial, technical, marketing, planning, personal, or commercial information, as such terms are used in Rule 26(c)(1)(G) of the Federal Rules of Civil Procedure and any applicable case law interpreting Rule 26(c)(1)(G) or the former Rule 26(c)(7).

5. **Highly Confidential Material**: For purposes of this Order, Highly Confidential Material is any Protected Data (defined below) and/or Confidential Material as defined in Section 4 which also includes non-public product design and testing information or extremely sensitive, highly confidential, non-public information, consisting either of trade secrets or proprietary or other highly confidential business, financial, regulatory, or strategic information (including information regarding business plans, technical data, and non-public designs), the disclosure of which would create a substantial risk of competitive or business injury to the Producing Party. Certain Protected Data may compel alternative or additional protections beyond those afforded Highly Confidential Material, in which event the parties shall meet and confer in good faith, and, if unsuccessful, shall move the Court for appropriate relief.

a. **Protected Data**: Protected Data shall refer to any information that a party believes in good faith to be subject to federal, state or foreign data protection laws or other privacy obligations. Protected Data constitutes highly sensitive materials requiring special protection. Examples of such data protection laws include but are not limited to The Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 et seq. (financial information); The Health Insurance Portability and Accountability Act and the regulations thereunder, 45 CFR Part 160 and Subparts A and E of Part 164 (medical information); 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, 1995 O.J. (L281/31) (European Union personal information); Data Protection Act 1998 (c. 29) (United Kingdom personal information); the German Federal Data Protection Act (Germany personal information); the Belgian Law of December 8, 1992 on Privacy Protection in relation to the Processing of Personal Data (Belgium personal information); Personal Information Protection and Electronic Documents Act (PIPEDA),

S.C. 2000, c. 5 (Canada personal information); The Federal Law on Protection of Personal Data held by Private Parties (published July 5, 2010) (Mexico personal information); and The Personal Information Protection Act (Law No. 57 of 2003) (Japan personal information).

6. **Designating Confidential Material or Highly Confidential Material**: The designation of Discovery Material as Confidential Material or Highly Confidential Material for purposes of this Order shall be made in the following manner:

a. **Documents**: [INSERT]

b. **Deposition and Other Proceedings**: [INSERT]

c. **Non-Written Materials**: [INSERT]

7. **Inadvertent Disclosure**: The inadvertent failure to designate Discovery Material as Confidential or Highly Confidential does not constitute a waiver of such claim and may be remedied by prompt supplemental written notice upon discovery of the inadvertent disclosure, with the effect that such Discovery Material will be subject to the protections of this Order.

8. **Copies**: The Receiving Party may make copies of Discovery Material, but such copies shall become Confidential Material or Highly Confidential Material to the same extent, and subject to the same protections, as the Discovery Material from which those copies were made. The Receiving Party shall exercise good faith efforts to ensure that copies it makes of Discovery Material produced to it, and copies made by others who obtained such Discovery Material directly or indirectly from the Receiving Party, include the appropriate confidentiality legend, to the same extent that the Discovery Material has been marked with the appropriate confidentiality legend by the Producing Party. In the event that the Receiving Party receives notice in accordance with Section 7 of this Order that Discovery Material was inadvertently disclosed without being designated as Confidential or Highly Confidential Material, the Receiving Party shall exercise good faith efforts to ensure that copies it makes of Discovery Material produced to it, and copies made by others who

obtained such Discovery Material directly or indirectly from the Receiving Party, are marked with the appropriate confidentiality legend, are made available in whole or in part only to persons authorized to receive Confidential or Highly Confidential Material (as the case may be), and are at all times handled and used only in the manner that this Order permits or requires Confidential or Highly Confidential Material (as the case may be) to be handled and used.

9. **Notes of Confidential Material or Highly Confidential Material**: Any notes, lists, memoranda, indices, compilations prepared or based on an examination of Confidential Material or Highly Confidential Material, or any other form of information (including electronic form), that quote from, paraphrase, copy or disclose Confidential Material or Highly Confidential Material with such specificity that the Confidential Material or Highly Confidential Material can be identified, or by reasonable logical extension can be identified, shall be accorded the same status of confidentiality as the underlying Confidential Material or Highly Confidential Material from which they are made and shall be subject to all of the terms of this Protective Order.

10. **Notice to Non-Parties**: Any party issuing a subpoena to a non-party shall enclose a copy of this Protective Order with a request that, within ten (10) calendar days, the non-party either request the protection of this Protective Order or notify the issuing party that the non-party does not need the protection of this Protective Order or wishes to seek different protection.

11. **Persons Authorized to Receive Confidential Material**: Discovery Material designated "Confidential" or its contents may be disclosed, summarized, described, characterized or otherwise communicated or made available in whole or in part only to the following persons:

a. [INSERT]

12. **Persons Authorized to Receive Highly Confidential Material**: Except as specifically provided for in this or subsequent Court orders, Highly Confidential Material or its contents shall not be disclosed, summarized, described, characterized or otherwise communicated or

made available in whole or in part to any person or entity, directly or indirectly, other than the following:

a. [INSERT]

13. **Qualification of Outside Experts and Consultants**: Neither Confidential nor Highly Confidential Material shall be disclosed to any outside experts or consultants who are current employees of a direct competitor of any party named in the Litigation. [INSERT ANY EXCEPTIONS].

14. **Use of Discovery Material**: Discovery Material containing Confidential and/or Highly Confidential Material shall be used solely for purposes of the Litigation, including any appeal and retrial. Any person or entity in possession of Discovery Material designated Confidential or Highly Confidential shall maintain those materials in accordance with Section 18 below.

15. **Agreement Must be Signed Prior to Disclosure**: Each person to whom Confidential or Highly Confidential Material may be disclosed that is also required to sign the "Agreement Concerning Information Covered by Protective Order" (attached hereto as Exhibit A) pursuant to Sections 11(c)-11(h), 11(j), 12(b)-12(f), and 12(h) shall deliver to the Disclosing Party a completed and originally executed copy of Exhibit A hereto prior to the time such Material is disclosed to such proposed Receiving Party.

16. **Exclusion of Individuals From Depositions**: Counsel for any Producing Party shall have the right to exclude from depositions any person who is not authorized by this Order to receive documents or information designated Confidential or Highly Confidential, but only during periods of examination or testimony directed to or comprising information that is Confidential or Highly Confidential.

17. **Storage Of Confidential Material or Highly Confidential Material**: The recipient of any Confidential Material or Highly Confidential Material that is provided under this

Protective Order shall maintain such information in a reasonably secure and safe manner that ensures that access is limited to the persons authorized under this Order, and shall further exercise the same standard of due and proper care with respect to the storage, custody, use and/or dissemination of such information as is exercised by the recipient with respect to its own proprietary information.

18. **Filing of Confidential Material or Highly Confidential Material**: The following procedures apply provided they do not conflict with applicable rules and orders of the court. [INSERT]

19. **No Prejudice**: Agreeing to be bound by this Protective Order, agreeing to and/or producing or receiving Confidential Material or Highly Confidential Material or otherwise complying with the terms of this Order shall not: [INSERT RIGHTS OF PARTIES PROTECTED]

20. **Challenging Designation of Materials**: A party shall not be obligated to challenge the propriety of a Confidential Material or Highly Confidential Material designation at the time made, and failure to do so shall not preclude a subsequent challenge thereto during the pendency of this Litigation.

a. **Challenge**: [INSERT STEPS]

b. **Meet and Confer and Motion**: [INSERT STEPS]

c. **Status of Challenged Designation Pending Judicial Determination**: [INSERT STEPS]

21. **No Application to Public or Otherwise Available Information**: This Order shall not limit or restrict a Receiving Party's use of information that the Receiving Party can demonstrate: (i) was lawfully in the Receiving Party's possession prior to such information being designated as Confidential or Highly Confidential Material in the Litigation and that the Receiving Party is not otherwise obligated to treat as confidential; (ii) was obtained without any benefit or use of

Confidential or Highly Confidential Material from a third party having the right to disclose such information to the Receiving Party without restriction or obligation of confidentiality; (iii) was independently developed by it after the time of disclosure by personnel who did not have access to the Producing Party's Confidential or Highly Confidential Material; or (iv) has been published to the general public. If the Receiving Party believes that the Disclosing Party has designated information that is covered by any of the preceding categories as Confidential Material or Highly Confidential Material, the Receiving Party may challenge the propriety of such designation using the procedure outlined in Section 21 above. Any challenged designation remains in force until the propriety of such designation has been decided as outlined above.

22. **No Waiver of Privilege**: Pursuant to Federal Rule of Evidence 502(d), disclosure (including production) of information that a party or non-party later claims should not have been disclosed because of a privilege, including, but not limited to, the attorney-client privilege or work product doctrine ("Privileged Information"), shall not constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, attorney work product, or other ground for withholding production as to which the Disclosing or Producing Party would be entitled in the Litigation or any other federal or state proceeding.

23. **Effect of disclosure of Privileged Information:** Pursuant to Federal Rule Civil Procedure 26(b)(5)(B) and Federal Rule of Evidence 502(e), the Receiving Party hereby agrees to return, sequester, or destroy any Privileged Information disclosed or produced by Disclosing or Producing Party upon request. If the Receiving Party reasonably believes that Privileged Information has been inadvertently disclosed or produced to it, it shall promptly notify the Disclosing or Producing Party and sequester such information until instructions as to disposition are received. The failure of any party to provide notice or instructions under this Paragraph shall not constitute a waiver of, or estoppel as to, any claim of attorney-client privilege, attorney work product, or other

ground for withholding production as to which the Disclosing or Producing Party would be entitled in the Litigation or any other federal or state proceeding.

a. [INSERT ADDITIONAL STEPS]

24. **Additional Parties or Attorneys**: In the event additional parties join or intervene in this Litigation, the newly joined party(ies) shall not have access to Confidential Material or Highly Confidential Material until its/their counsel has executed and, at the request of any party, filed with the Court the agreement of such party(ies) and such counsel to be fully bound by this Order. If any additional attorneys make appearances in this Litigation, those attorneys shall not have access to Confidential Material or Highly Confidential Material until they execute the "Agreement Concerning Information Covered by Protective Order" attached hereto as Exhibit A.

25. **Protective Order Remains in Force**: This Protective Order shall remain in force and effect until modified, superseded, or terminated by consent of the parties or by order of the Court made upon reasonable written notice. Unless otherwise ordered, or agreed upon by the parties, this Protective Order shall survive the termination of this Litigation. The Court retains jurisdiction even after termination of this Litigation to enforce this Protective Order and to make such amendments, modifications, deletions and additions to this Protective Order as the Court may from time to time deem appropriate.

26. **No Prejudice for Further Relief**: This Protective Order is without prejudice to the right of any party to seek other or further relief from the Court.

27. **No Waiver of Grounds for Producing Material**: This Protective Order shall not be construed as waiving any right to assert a claim of privilege, relevance, overbreadth, burdensomeness or other grounds for not producing material called for, and access to such material shall be only as otherwise provided by the discovery rules and other applicable laws.

28. **Termination of Access to Confidential Material and Highly Confidential Material**:

a. **Change in Status**: [INSERT]

b. **Conclusion of Litigation**: [INSERT]

29. **No Loss of Confidential or Highly Confidential Status By Use In Litigation or Appeal**: In the event that any Confidential or Highly Confidential Material is used in any court proceeding in this Litigation or any appeal therefrom, such Confidential or Highly Confidential Material shall not lose its status as Confidential or Highly Confidential through such use. Counsel shall comply with all applicable local rules and shall confer on such procedures that are necessary to protect the confidentiality of any documents, information and transcripts used in the course of any court proceedings, including petitioning the Court to close the court room.

30. **Confidential or Highly Confidential Material Subpoenaed or Ordered Produced in Other Actions**: If any person receiving documents covered by this Order (the "Receiver") is served with a subpoena, order, interrogatory, or document or civil investigative demand (collectively, a "Demand") issued in any other action, investigation, or proceeding, and such Demand seeks Discovery Material that was produced or designated as Confidential Material or Highly Confidential Material by someone other than the Receiver, the Receiver shall give prompt written notice by hand or facsimile transmission within ten (10) business days of receipt of such Demand to the party or non-party who produced or designated the material as Confidential Material or Highly Confidential Material, and shall object to the production of such materials on the grounds of the existence of this Order. The burden of opposing the enforcement of the Demand shall fall upon the party or non-party who produced or designated the material as Confidential Material or Highly Confidential Material. Unless the party or non-party who produced or designated the Confidential Material or Highly Confidential Material obtains an order directing that the Demand

not be complied with, and serves such order upon the Receiver prior to production pursuant to the Demand, the Receiver shall be permitted to produce documents responsive to the Demand on the Demand response date. Compliance by the Receiver with any order directing production pursuant to the Demand of any Confidential Material or Highly Confidential Material shall not constitute a violation of this Order. Nothing in this Order shall be construed as authorizing a party to disobey a lawful subpoena issued in another action.

31. **Advice Based on Discovery Material Allowed**: Nothing in this Protective Order shall bar or otherwise restrict any attorney from rendering advice to his or her client with respect to this Litigation and, in the course of rendering advice, referring to or relying generally on the examination of Confidential Material or Highly Confidential Material; provided, however, that in rendering such advice and in otherwise communicating with his or her client, the attorney shall not disclose the contents of any Confidential Material or Highly Confidential Material produced by another party or a non-party if that disclosure would be contrary to the terms of this Protective Order.

32. **Redaction Allowed**: Any Producing Party may redact from the documents and things it produces matter that the Producing Party claims is subject to attorney-client privilege, work product immunity, a legal prohibition against disclosure, or any other privilege or immunity. The Producing Party shall mark each thing where matter has been redacted with a legend stating "REDACTED," and specify the basis for the redaction (e.g., privilege, confidential, highly confidential, etc.), as appropriate, or a comparable notice. Where a document consists of more than one page, at least each page on which information has been redacted shall be so marked. The Producing Party shall preserve an unredacted version of each such document. [INSERT specific provisions for the redaction of privileged matter from electronic files produced in native format, if applicable.] In addition to the foregoing, the following shall apply to redactions of Protected Data:

a. Any party may redact Protected Data that it claims, in good faith, requires protections under the terms of this Order. Protected Data, however, shall not be redacted from Discovery Material to the extent it directly relates to or identifies an individual named as a party.

b. Protected Data shall be redacted from any public filing not filed under seal.

c. The right to challenge and process for challenging the designation of redactions shall be the same as the right to challenge and process for challenging the designation of Confidential Material and Highly Confidential Material as set forth in Section 21.

33. **Personally Identifiable Information**: Personally identifiable information that a party has designated as Protected Data based on its good faith belief that the information is subject to federal, state or foreign data protection laws, data privacy laws, or other privacy obligations, or any of the information contained therein, shall be handled by Counsel for the Receiving Party with the highest care, including but not limited to the procedures that they would employ to protect their own personally identifiable information; and the documents produced shall be stored and secured in a manner designed to prevent access to persons other than the above-listed permitted individuals, and that all such information stored in electronic form shall be password protected.

34. **Violations of Protective Order**: In the event that any person or party should violate the terms of this Protective Order, the aggrieved Disclosing Party may apply to the Court to obtain relief against any such person or party violating or threatening to violate any of the terms of this Protective Order. In the event that the aggrieved Disclosing Party seeks injunctive relief, it must petition the District Judge for such relief, which may be granted at the sole discretion of the District Judge. The parties and any other person subject to the terms of this Protective Order agree that this Court shall retain jurisdiction over it and them for the purpose of enforcing this Protective Order.

35. **Headings**: The headings herein are provided only for the convenience of the parties, and are not intended to define or limit the scope of the express terms of this Protective Order.

IT IS SO ORDERED.

Dated: _____, 20__

_____
United States District Judge

Dated: _____, 20__

Respectfully stipulated to and submitted by,

By: _____

[Name, firm, address, phone, bar number]

Counsel for Plaintiff

By: _____

[Name, firm, address, phone, bar number]

Counsel for Defendant

EXHIBIT A

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

_____,	)	
	)	Case No.: _____
Plaintiff.	)	
	)	
v.	)	Agreement Concerning Information Covered
	)	By Stipulated Protective Order
_____,	)	
	)	
Defendant.	)	
	)	

I, _____, hereby acknowledge that I have received a copy of the Stipulated Protective Order entered in the above-captioned action by the United States District Court for the _____ District of _____ (hereinafter, the "Protective Order").

I have either read the Protective Order or have had the terms of the Protective Order explained to me by my attorney.

I understand the terms of the Protective Order and agree to comply with and to be bound by such terms.

If I receive documents or information designated as Confidential Material or Highly Confidential Material (as those terms are defined in the Protective Order), I understand that such information is provided to me pursuant to the terms and restrictions of the Protective Order.

I agree to hold in confidence and not further disclose or use for any purpose (other than is permitted by the Protective Order) any information disclosed to me pursuant to the terms of the Protective Order.

I hereby submit myself to the jurisdiction of the United States District Court for the _____ District of _____ for resolution of any matters pertaining to the Protective Order.

My address is _____

My present employer is _____

Dated: _____

Signed: _____

Appendix C: The Sedona Conference® Cross-Border Data Safeguarding Process + Transfer Protocol

INSTRUCTIONS

The Sedona Conference® Cross-Border Data Safeguarding Process + Transfer Protocol has two interrelated purposes. First, it is an ease-of-reference guide that identifies common techniques used to achieve best possible legal compliance with conflicting U.S. eDiscovery rules and Data Protection laws when foreign data needs to be processed and transferred for the purposes of U.S. litigation. Second, the Protocol is designed as a record which can be presented to those with regulatory responsibilities for Data Protection, evidencing the steps taken to best comply with Data Protection Laws. The Protocol requires customization in order to record fully the various activities undertaken to achieve best possible legal compliance, including a detailed explanation of the circumstances and factors taken into account. The following instructions should be used with the chart below.

12. Explain the reasons for collecting the data. Identify clearly the U.S. proceedings for which the Protected Data is processed and transferred. If the Protected Data is collected for reasons other than for litigation, identify the investigation or regulatory proceeding, or other proceeding requiring the processing and transfer.

13. Determine whether relevant data that is required to be preserved, processed or produced in the U.S. is subject to Data Protection Laws and, if so, which laws apply. Assess whether alternative, preferably domestic, sources of that relevant data exist. To the extent possible, produce U.S. sources of data, making production of relevant Protected Data unlikely or unnecessary. Identify and segregate relevant sensitive personal data that is preliminarily presumed to be subject to stricter applicable data protection measures. Likewise, determine the sources of relevant Protected Data, if it has been or will be processed, its transfer points and to where it will be transferred.

14. Describe measures taken to minimize the processing and transfer of Protected Data, explaining the methodology used to filter out non-relevant Protected Data. These culling activities often begin with a questionnaire or an in-person interview and iteratively progress, through use of software tools and other processes, towards a production consisting of only that Protected Data that is relevant and necessary. Consider compiling Protected Data in one central location in one European country to be able to minimize the burden of filtering efforts. Identify categories of Protected Data processed and transferred best suited to satisfy notions of transparency and to develop an understanding of the type of data that is affected or is expected to be affected by the applicable Data Protection Laws.

15. Describe the various categories of Protected Data that will be processed or transferred by type, including sensitive personal data, trade secret data, restricted data, data identifying a person, etc.

16. If appropriate, consider use of The Sedona Conference® Model Protective Order Re: Protected Data or similar protective orders, or stipulations with data protection language providing agreed-upon or court-ordered restrictions on the use, disclosure and dissemination

of Protected Data. Consider including options to redact and designate Protected Data as "Confidential" or "Highly Confidential." Further, consider restrictions related to the onward transfer of data once it reaches the U.S.

17. Strive to provide a transparent processing and transfer protocol to the Data Subjects, identifying impacted Data Subjects and the means to communicate to them the purpose for the processing and transfer of Protected Data, the categories of Protected Data at issue, the duties and obligations attendant to that Protected Data, data protection measures that will or have been put in place and such other factors as may be required or appropriate under the circumstances. Such communications to Data Subjects may include postings, one-on-one meetings, group presentations, requesting consent and providing question and answer information, in writing or orally.

18. Identify steps taken to make Protected Data secure by describing the protective measures undertaken by the Data Controller, including, for example, agreements with third parties, the existence of a protective order, the nature and type of encryption, the limitations on access to the Protected Data and other means of securing the Protected Data.

19. Describe the efforts to be undertaken or those that have been undertaken if notice to others involved in data protection is contemplated or required. Others that may be consulted may include data protection personnel associated with the Data Controller, such as Data Protection Officers, and, in some countries, Data Protection Authority having jurisdiction over the Protected Data or company works councils.

20. Identify the mechanism that will be used or has been used to legitimize the transfer of Protected Data. These mechanisms typically involve the use of Binding Corporate Rules, Safe Harbor certification, Model Contracts or some other means of satisfying transfer safeguards.

21. Document the procedures that will be or have been used to destroy or return Protected Data to the Data Controller when it is no longer necessary.

22. Consider identifying the person or persons responsible for overseeing preservation, processing, and transfer of the Protected Data and obtaining that person's or persons' signatures signifying that the steps recorded have been taken.

ACTION ITEM	INFORMATION
1. Purpose for processing and transfer of Protected Data	Identify the type of action for which Protected Data is processed or transferred (e.g., reasonably anticipated or active civil litigation, government investigation; subpoena) with specific identification information (e.g., case name, docket number, filing location, date of filing, description of litigation)
2. Data Protection Laws at issue and specific sources of Protected Data	Identify the country whose Data Protection Laws are at issue, the specific Data Protection Laws implicated, and the significance of each; identify the location of the Protected Data, where it is processed and the location from where and to where it will be transferred
3. Measures taken to minimize the processing and transfer of Protected Data	Explain methodology used to narrow and cull the processing and transfer of Protected Data to only that which is relevant and necessary (e.g., use of preliminary questionnaires and interviews, use of tools and processes for iterative search and keyword refinement, de-duplication)
4. Categories of Protected Data processed and transferred	Identify categories of Protected Data processed and transferred (e.g., information that is likely to identify the Data Subject, sensitive personal data, trade secret data, restricted data)
5. Limitation on Use and dissemination of Protected Data	Identify stipulations or protective orders and their material terms or a attach copies of them (e.g., use of The Sedona Conference® Model Protective Order Re: Protected Data, general protective order, confidentiality agreement, Data Protection stipulation)
6. Transparency of processes and transfers concerning Protected Data	Identify steps taken (if and as appropriate or feasible) to make information available or to notify Data Subjects of processing, transfer and onward transfer of Protected Data (e.g., posting notice, internal circular requesting consent)
7. Steps taken to make remaining Protected Data secure prior onward transfer	Identify steps taken to secure Protected Data (e.g., third-party agreements, nature and type of encryption, access limitation, password protection)
8. Compliance with notification obligations (if any) to others with oversight of data protection.	Identify others involved or that may need to be consulted (e.g., the company's Data Protection Officer, government's Data Protection Authority, works council) that have responsibility for implementation of Data Protection and explain their involvement and means of notification

9. Bases upon which Protected Data is transferred	Identify acceptable modes of the transfer of Protected Data (e.g., Safe Harbor Certification, Model Contract Clauses, Binding Corporate Rules or some other means of satisfying transfer safeguards)
10. Disposition of transferred Protected Data when no longer needed	Describe disposition of processed and transferred Protected Data (e.g., destruction of or return of Protected Data) when no longer needed to fulfill U.S. obligations of the given matter at hand.
11. Person responsible for transfer and processing of Protected Data	Consider identifying the person or persons ultimately responsible for processing and transferring Protected Data and affixing signatures signifying that the steps recorded have been taken.

Appendix D: 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; (7) e-discovery in Canadian civil litigation; (8) mass torts and punitive damages; and (9) patent damages and remedies. See the "Working Group Series" area of our website www.thesedonaconference.org for further details on our Working Group Series and the Membership Program.

wgs

Visit www.thesedonaconference.org