The Sedona Conference Working Group Series

wgs

The Sedona Conference

International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)

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

January 2017

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)

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

JANUARY 2017

Author:	The Sedona Conference
Editor in Chief:	Denise E. Backhouse
Editors:	Cecilia Álvarez, M. James Daley, Amor Esteban, Natascha Gerlach, Peggy Kubicz Hall, Taylor Hoffman, Jerami Kemnitz, Michael Pomarico, David C. Shonka, Kenneth J. Withers
Managing Editor:	Susan McClain, with the assistance of Shruti Chopra

The editors would like to thank Hon. Michael M. Baylson, United States District Judge, Eastern District of Pennsylvania, for his review and contributions.

Editors of the 2011 European Union Edition:	Moze Cowper, M. James Daley, Amor A. Esteban (editor-in-chief), John K. Rabiej, Daniel L. Regard, Kenneth J. Withers, and Christian Zeunert. Special thanks to Dr. Alexander Dix, LL.M. (ret.), former Berlin Commissioner for Data Protection and Freedom of Information, and Hon. Shira A. Scheindlin (ret.), former United States District Judge for the Southern District of New York.

Preface

Welcome to *The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)*, a project of The Sedona Conference Working Group Six on International Electronic Information Management, Discovery and Disclosure (WG6). This is one of a series of Working Group commentaries published by The Sedona Conference, a 501(c)(3) research and educational institute dedicated to the advanced study of law and policy in the areas of antitrust law, complex litigation, and intellectual property rights. The mission of The Sedona Conference is to move the law forward in a reasoned and just way.

WG6 was launched in 2005 after The Sedona Conference's first International Programme, held at Claire College in Cambridge, England. 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 engage in dialogue about the management, discovery, and disclosure of electronically stored information that is subject to the potentially conflicting rules of multiple jurisdictions. An important goal of WG6 has been to develop a set of principles to guide parties as they attempt to navigate the challenges of cross-border conflicts, complicated by the tension between the concept of pretrial discovery or disclosure in common law jurisdictions, and the evolving Data Protection Laws of the European Union (EU) and other regions of the world.

Between 2005 and 2011, WG6 met in Barcelona, Spain; Washington, D.C.; and Lisbon, Portugal in order to develop and test 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 WG6 to invited members of the judiciary as well as data protection and data privacy thought leaders from around the world. Since 2009, WG6 also engaged in an active dialogue with the EU's Article 29 Working Party in order to share ideas and develop solutions to the EU/U.S. cross-border data transfer conundrum. In 2011, WG6 released the public comment version of *The Sedona Conference International Principles on Discovery, Disclosure & Data Protection* (the "*International Litigation Principles"*). This document set forth a three-stage approach addressing cross-border conflicts while also providing useful commentary. It demonstrated that data protection and discovery need not be at intellectual or practical odds. The *International Litigation Principles* was well-received by practitioners, and individual members of the Article 29 Working Party considered it to be both a positive contribution and an opening for further dialogue.

Following the publication of the *International Litigation Principles*, WG6 broadened the dialogue to include members of the judiciary, data protection authorities, and government officials from beyond the U.S. and EU, including from Asia, Canada, Australasia, and Africa. Between 2012 and 2016, WG6 met in Toronto, Canada; Zurich, Switzerland; London, England; Hong Kong, PRC; and Berlin, Germany. This turned out to be a watershed period in the evolution of data protection law

worldwide, as described in detail in the Foreword and Introduction, culminating in the adoption of the General Data Protection Regulation (GDPR), which will replace the 1995 EU Data Protection Directive in May 2018.

Throughout this period, it became apparent that the *International Litigation Principles*, originally subtitled "European Union Edition," transcended both the specific context of EU/U.S. cross-border litigation and significant changes in data protection law globally. The original authors anticipated this, stating that, "[a]lthough focused principally on the relationship between U.S. preservation and discovery obligations and the EU Data Protection Directive, the [document] 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."

In 2016, WG6 determined that the commentary and supporting practice materials in the *International Litigation Principles* needed immediate revision to reflect the significant intervening changes to the legal and regulatory landscape, including the 2015 amendments to the U.S. Federal Rules of Civil Procedure and the transition from the EU Data Protection Directive to the GDPR. However, the drafters have added an important phrase to the title of the resulting document, "Transitional Edition," to emphasize that we anticipate further revision after May of 2018, when the GDPR takes effect. We hope that this Transitional Edition provides immediate guidance, while stimulating ideas, comments, and suggestions, which may be submitted to comments@sedonaconference.org.

In addition, we encourage your active engagement in the dialogue. Membership in The Sedona Conference Working Group Series is open to all. The Series includes WG6 and several other Working Groups in the areas of electronic document management and discovery, patent litigation best practices, data privacy and security, and other "tipping point" issues in the law. Information on membership and a description of current Working Group activities is available at https://thesedonaconference.org/wgs.

As with this Transitional Edition of the *International Litigation Principles*, the 2011 edition was prepared by attorneys from around the globe whose practices focus on cross-border discovery and data protection. We would like to acknowledge the WG6 Steering Committee of that time, all of whom were deeply involved in drafting and editing the first edition. The Co-Chairs of the Steering Committee in 2011 were Quentin Archer (UK) and M. James Daley (US). Steering Committee members in 2011 were Steven C. Bennett (US), Amor A. Esteban (US), Richard J. Hood (US), Sandra Potter (AU), Cecilia Álvarez Rigaudias (ES), and Christian Zeunert (CH). In formulating the *International Litigation Principles*, WG6 gained the perspective of—and would like to thank—the many recognized authorities on the subject who joined the dialogue, 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 1995 EU Data Protection Directive and will continue to do so regarding the GDPR. We expect to continue being engaged in dialogue with the

Article 29 Working Party (in its current form and as the European Data Protection Board under the GDPR in the near future) during the transition to the GDPR. It is through these various sources and many years of study that The Sedona Conference provides this work to advance the law in an area often thought of as so complex and confounding that it has been largely ignored.

Kenneth J. Withers
Deputy Executive Director
The Sedona Conference
January 2017

Foreword

The Sedona Conference Working Group 6 (WG6) recognizes that the rapid proliferation of electronic information and the increasing interdependence of individuals, multinational companies, and governments arising from a global marketplace present novel and unique legal challenges that previously did not exist. These challenges have made the legal community rethink deeply held notions of privacy, personal freedom, and how legal conflicts are resolved. WG6, more specifically, recognizes 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 jurisdiction, but that information is located in another jurisdiction where it is protected by a data protection law, commercial secrecy law, or a "blocking statute" which prohibits its disclosure.

For example, all European Union (EU) Member States implemented the 1995 EU Data Protection Directive[1] which imposed restrictions on the use and dissemination of personal information. It is challenging to navigate the restrictions relating to the processing and transfer of personal information to the U.S., which is deemed by the EU as a country with inadequate personal data protection and, thus, a potential danger to the fundamental right the European privacy legislation aims to protect. The purpose of the *International Litigation Principles* is to provide guidance to public and private parties, counsel, data protection authorities, and the judiciary regarding the management of such conflicts.

However, the legal landscape in which the *International Litigation Principles* was placed in 2011 is rapidly changing on many fronts.

Currently, the 1995 EU Data Protection Directive is being replaced by the General Data Protection Regulation (GDPR),[2] which comes into effect on May 25, 2018. The GDPR is the result of extensive negotiations between the European Commission, the European Parliament, and the Council of the European Union. Different from a directive, a regulation under EU law has direct, binding effect on the EU Member States. Across Member States, initiatives to adapt secondary law in relation to the GDPR have begun. Even though the United Kingdom voted in 2016 to withdraw from the EU, "it would be expected and quite normal for [the UK government] to opt into the GDPR and then look later at how best . . . to help British business with data protection while maintaining high levels

---

1 The Data Protection Directive is more formally known as 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. *See* 1995 O.J. (L 281), Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. *See* 1995 O.J. (L 281), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT [hereinafter EU Data Protection Directive].

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1) [hereinafter GDPR], came into force on May 25, 2016. *See* http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf.

of protection for members of the public."[3] But until May of 2018, the laws of Member States (including the UK) that implemented the EU Data Protection Directive will continue to govern data processing and transfers out of the EU.

In October 2015, the Court of Justice of the European Union declared that the European Commission's determination in 2000 that the widely relied-upon EU-U.S. Safe Harbor data transfer framework provided an adequate level of data protection for EU citizens was invalid[4] in the wake of the Snowden revelations and a subsequent Commission finding in 2013 that

> the United States authorities were able to access the personal data transferred from the Member States to the United States and process it in a way incompatible, in particular, with the purposes for which it was transferred, beyond what was strictly necessary and proportionate to the protection of national security. Also, the Commission noted that the data subjects had no administrative or judicial means of redress enabling, in particular, the data relating to them to be accessed and, as the case may be, rectified or erased.[5]

Safe Harbor has since been replaced by a new framework, called the EU-U.S. Privacy Shield, which is supported by a new adequacy determination.[6] However, the adequacy of the Privacy Shield framework is being challenged.[7]

Also in the intervening years since the *International Litigation Principles* was published, a growing number of countries outside of the EU have adopted Data Protection Laws, often modeled on those in the EU.[8] The Asia-Pacific Economic Cooperation "Privacy Framework" was adopted in 2014. In

---

3 Testimony of The Rt. Hon. Karen Bradley MP, Secretary of State for Culture, Media and Sport, given at the Parliamentary Committee Meeting on Responsibilities of the Secretary of State for Culture, Media and Sport, HC 764, October 24, 2016, *available at* http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/responsibilities-of-the-secretary-of-state-for-culture-media-and-sport/oral/42119.html.

4 Case C-362/14, Schrems v. Data Protection Comm'r (Ireland), 2015 E.C.R. (October 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=135693.

5 *Id.* at ¶ 90.

6 *See generally* PRIVACY SHIELD FRAMEWORK, https://www.privacyshield.gov/welcome. A Swiss-U.S. Privacy Shield Framework will be available in April 2017. *Id.*

7 Press Release, Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield (July 26, 2016), *available at* http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf. In late 2016, advocacy groups Digital Rights Ireland and French-based La Quadrature du Net both filed actions against the European Commission with the Court of Justice of the European Union to have the EU-U.S. Privacy Shield adequacy decision annulled (Case T-670/16 and Case T-738/16).

8 *See, e.g.*, Philippines, Data Privacy Act, Republic Act 10173 (August 2012); Columbia, General Provisions for the Protection of Personal Data, Law 1581 (October 2012); South Africa, Protection of Personal Information (POPI) Act, No. 4 of 2013 (November 2013).

the U.S., the Federal Rules of Civil Procedure were amended, effective December 2015, to more narrowly focus the scope of pretrial discovery and to encourage more active judicial supervision of discovery proceedings.

Thus, we have chosen to call this edition of the *International Litigation Principles* "Transitional," in recognition of this multi-faceted, fluid situation.

Given the frequency of disputes in the U.S. involving data located in EU Member States, the *International Litigation Principles* is naturally influenced by conflicts of law that arise because of processing and transfer restrictions currently imposed by the 1995 EU Data Protection Directive and the implementing Member State laws, as well as in the future by the GDPR. Nonetheless, the *International Litigation Principles* is intended to transcend parochial treatment and apply broadly to any data protection law in conflict with U.S. preservation, disclosure, or discovery obligations, regardless of the law at issue or the State that enacted it. Thus, this Transitional Edition of the *International Litigation Principles* has omitted the subtitle "European Union Edition" that appeared on the 2011 public comment edition. WG6 has established committees that are exploring the cross-border data transfer issues arising in other parts of the world, such as the Asia-Pacific, Latin America, and Middle East regions. These explorations may result in future supplementary commentaries on the *International Litigation Principles*, but the essential Principles themselves are providing useful guidance to practitioners in these regions already.

Similarly, while thematically centered on data in electronic form, the *International Litigation Principles* is intentionally written to apply equally to Protected Data in any form, whether recorded electronically, on paper, or on some other media.

As part of the *International Litigation Principles*, WG6 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 *Model U.S. Federal Court Protective Order* (the "*Protective Order," infra* Appendix C) 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* (the "*Protocol," infra* Appendix D) outlines a practical, standardized approach to protecting data at the preservation and collection levels, designed to maximize compliance with applicable laws. These models have been examined in light of increased concern for data security since they were first published in 2011. In addition, we are grateful to United States District Judge Michael Baylson of the Eastern District of Pennsylvania for permission to reprint his *Model U.S. Federal Court Order Addressing Cross-Border ESI Discovery* (the "*Pretrial Order," infra* Appendix B).

The *International Litigation Principles*, together with the *Protective Order,* the *Protocol*, and the *Pretrial Order*, 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.

Table of Contents

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition) 1

I. Introduction 2

II. Definitions 8

III. The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation 9

Principle 1 9

Principle 2 11

Principle 3 14

A. Limit the Scope of the Request 16

B. Discovery with Specificity 16

C. Phased Discovery 17

D. Minimize the Production of Protected Data 18

E. Substitution of Data 18

F. Limitations on the Format of Production 19

Principle 4 20

A. Protective Order or Stipulation 20

B. Scheduling Stipulation or Order 21

C. Legitimization Plan 21

Principle 5 22

Principle 6 24

Appendix A: Bibliography 26

Appendix B: Model U.S. Federal Court Order Addressing Cross-Border ESI Discovery 33

Appendix C: Model U.S. Federal Court Protective Order 39

Appendix D: The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol 59

The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (Transitional Edition)

1. With regard to data that is subject to preservation, disclosure, or discovery in a U.S. legal proceeding, 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, 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.

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.

I. INTRODUCTION

"Discovery" is a central—and somewhat unique—feature of civil litigation in the American legal system. 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. U.S. state courts generally employ similar rules, often patterned after the federal rules. Fed. R. Civ. P. 34 applies where one party seeks documents and electronically store information (ESI) from another party to the litigation.[9] Fed. R. Civ. P. 45 applies where any party seeks documents and ESI from a non-party.[10] Several factors determine the appropriateness of a request for documents under Fed. R. Civ. P. 34. As a threshold matter, the material sought must be relevant to a party's claim or defense in the action and proportional to the needs of the case.[11] Likewise, the material sought should not be cumulative or duplicative, and it should be sought from the source that is most convenient, least burdensome, and least expensive.[12]

The legal tradition in the United States is that discovery is conducted by the litigants themselves (or, in most cases, by counsel for the litigants) under the supervision of the court. Discovery is also not limited to securing the documents and testimony that will be used at trial. Traditionally, litigants have been allowed access to any sources of information relevant to the issues in dispute in the litigation, limited by court-enforced rules of privilege and an unevenly-applied concept of proportionality,

---

[9] The definitions of "document" and "electronically stored information" (ESI) are broad. Fed. R. Civ. P. 34(a)(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."

[10] While the discovery procedures under Fed. R. Civ. P. 45 differ from Fed. R. Civ. P. 34, the scope of discovery is essentially the same.

[11] Fed. R. Civ. P. 26(b)(1) states:

> 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 and proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit. Information within this scope of discovery need not be admissible in evidence to be discoverable.

[12] Fed. R. Civ. P. 26(b)(2)(C) states:

> 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 proposed discovery is outside the scope permitted by Rule 26(b)(1).

usually articulated as a prohibition on "undue burden." Unlike courts in civil law countries, American courts are not equipped to independently inquire into the facts of a civil dispute. There are no court officers available to request and review documents or conduct interviews with witnesses.

While this concept of discovery had some precedents in common law and equity, it was enshrined into the Federal Rules in 1938 and rapidly incorporated into the court rules of each of the individual states. The goal of this system is to encourage the parties to discover, for themselves, before trial, what factual assertions essential to their case are supported by the evidence and what are not. This is designed to pave the way for the parties to settle their dispute without trial, stipulate to the facts and present the case to the court for a ruling without trial ("summary judgment"), or significantly narrow the issues for trial. Although many cases in American courts involve only minimal discovery, the availability of discovery is essential to the fair adjudication of nearly all disputes.

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, technological, 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 U.S., which often conflicts with the significantly narrower scope permitted in other countries, particularly concerning information deemed confidential or subject to Data Protection Laws.

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 U.S. 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 ESI—which now accounts for virtually all business information. Indeed, the volume of ESI and number of ESI transmissions grows dramatically each year.[13]

This unprecedented explosion in information is due in large part to the ubiquitous, mobile, and easily-replicated nature of ESI. Today, an employee from a Toronto company can conduct business

---

[13] Focusing on just email as one form of ESI communication, a well-respected technology market research firm reported:

> In 2015, the number of worldwide email users will be nearly 2.6 billion. By the end of 2019, the number of worldwide email users will increase to over 2.9 billion. . . . In 2015, the number of emails sent and received per day total over 205 billion. This figure is expected to grow at an average annual rate of 3% over the next four years, reaching over 246 billion by the end of 2019. . . . In 2015, the number of business emails sent and received per user per day totals 122 emails per day. This figure continues to

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, transmitted, 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, has blurred traditional U.S. legal notions of "possession, custody, or control"—the touchstone for traditional analysis of preservation and production obligations under U.S. law.[14]

A necessary precondition for effective discovery is that the information has been preserved, giving rise to a duty of preservation.[15] 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 should 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 may be remediated or punished by the court. Remedial measures and punishment a court can impose include

---

show growth and is expected to average 126 messages sent and received per business user by the end of 2019.

The Radicati Group, *Email Statistics Report, 2015-2019*, *available at* http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf.

[14] The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control*," 17 SEDONA CONF. J. 467 (2016), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Rule%2034%20and%20Rule%2045%20%E2%80%9CPossession%2C%20Custody%2C%20or%20Control%E2%80%9D.

[15] 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) ("The duty to preserve evidence 'includes an obligation to identify, locate, and maintain, information that is relevant to specific, predictable, and identifiable litigation'") (quoting The Sedona Conference, *Commentary On Legal Holds: The Trigger & The Process*, THE SEDONA CONFERENCE (August 2007 Public Comment Version) at 3, https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Legal%20Holds); Apple Inc. v. Samsung Elecs. Co., 881 F. Supp. 2d 1132, 1137 (N.D. Cal. 2012) (same and noting that "[i]t is well-established that the duty pertains only to relevant documents.") (citing Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec. LLC, 685 F. Supp. 2d 456, 466 (S.D.N.Y. 2010)).

granting additional discovery, or imposing monetary or other 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.[16]

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 accessible to a responding party but subject to the Data Protection Laws of another country. Frequently, however, information that is subject to discovery may be held by 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 U.S.[17]

Importantly, U.S. courts have the authority to order the production of the information sought even if it is located outside the U.S. 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 pursuant to guidance provided by the U.S. Supreme Court.[18] 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, administrative, 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

---

[16] *See, e.g.*, Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (A party, upon recognizing the threat of litigation, need not preserve "every shred of paper, every email or electronic document, and every backup tape[.]"); Marten Transp., Ltd. v. PlattForm Advert., Inc., No. 14-cv-02464-JWL-TJJ, 2016 WL 492743, at *4 (D. Kan. Feb. 8, 2016) (the intent of Fed. R. Civ. P. 37(e), as amended in December 2015, is to curtail excessive preservation efforts: "[t]his rule recognizes that 'reasonable steps' to preserve suffice; it does not call for perfection") (quoting JUDICIAL CONF. COMM. ON RULES OF PRACTICE & PROCEDURE, REPORT OF THE JUDICIAL CONF. COMM. ON RULES OF PRACTICE AND PROCEDURE 15 (Sept. 2014)).

[17] U.S. federal courts apply divergent tests for determining whether a party has "possession, custody or control" of documents sought in discovery; moreover, the analysis is intensely fact-based. *Compare* Genentech, Inc. v. Trs. of the Univ. of Pa., No.10-2037, 2011 U.S. Dist. LEXIS 128526 (N.D. Cal. Nov. 7, 2011) (applying 9th Circuit's "legal right" test and declining to compel wholly-owned U.S. subsidiary of German parent company to produce documents outside of narrow contractual agreement), *with In re* Ski Train Fire of November 11, 2000 Kaprun Aus., MDL 1428, 2006 U.S. Dist. LEXIS 29987 (S.D.N.Y. May 16, 2006) (compelling German parent company party to produce discovery from its non-party, wholly-owned Austrian subsidiary where parent had the practical ability to obtain it), *and* S2 Automation LLC v. Micron Tech., Inc., No. 11-0884, 2012 U.S. Dist. LEXIS 120097, at *54 and *passim* (D.N.M. Aug. 9, 2012) ("the party to whom the discovery is directed need not have legal ownership or actual physical possession, but rather a practical ability to obtain the documents. . . . '[I]f a party has access and the practical ability to possess documents not available to the party seeking them, production may be required.'" (citing Shcherbakovskiy v. Da Capo Al Fine, Ltd., 490 F.3d 130, 138 (2d Cir. 2007)). *See generally*, The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,*" *supra* note 14.

[18] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522, 544 n.28 (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)).

compelled to preserve and produce information 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 Litigation 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 The Sedona Conference (TSC), as reflected in its widely accepted *Cooperation Proclamation* published in July 2008.[19] 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, restricted, or postponed consideration of discovery in circumstances where privacy rights are deemed more important than the discovery sought by litigants.[20]

To this end, the *International Litigation 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 obliga-

---

[19] The Sedona Conference, *The Case for Cooperation*, 10 SEDONA CONF. J. 339 (2009 Supp.), *available at* https://thesedonaconference.org/publication/Supplement%20to%20Volume%2010%20of%20The%20Sedona%20Conference%20Journal%C2%AE%20-%20Cooperation. The *Sedona Conference Cooperation Proclamation* (2008) 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 THE SEDONA CONFERENCE, http://www.thesedonaconference.org/content/tsc_cooperation_proclamation.

[20] *See, e.g.*, Salerno v. Lecia, Inc., 97-CV-9735(H), 1999 U.S. Dist. LEXIS 7169, at *10 (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, A.G. v. Valdez, 909 S.W.2d 900, 902–03 (Tex. 1995) (denying request to produce company telephone book protected by German Federal Data Protection Act (BUNDESDATENSCHUTZGESETZ [BDSG], Dec. 20, 1990, BGBL. I at 2954, as amended) 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); Da Silva Moore v. Publicis Groupe S.A., 287 F.R.D. 182, 188–89 (S.D.N.Y. 2012) (emails of defendant's French CEO excluded from first phase of discovery) (citing *Aérospatiale,* 482 U.S. at 522, and The Sedona Conference, *International Principles on Discovery, Disclosure and Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation, European Union Ed.*, THE SEDONA CONFERENCE (Dec. 2011 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20InternInterna%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection).

tion. The *International Litigation Principles* includes six definitions, six Principles, and a comment section under each Principle to elucidate the purpose of each Principle and provide references to supporting treaties, case law, and other authorities. The roadmap provided by the *International Litigation Principles* is designed to help chart the course for compliant, defensible discovery. It has been applied in scores of litigations since 2011 and has advanced the interests of both fair adjudication and data protection.

II. DEFINITIONS

The following definitions apply to the Principles, commentary, and associated guidance:[21]

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.[22]

2. "Data Protection Laws" include any law or regulation, including U.S. laws and regulations, that restricts the usage or disclosure of data, requires safeguarding data, or imposes obligations in the event of compromises to the security or confidentiality of data. The *International Litigation Principles* is intended to apply broadly wherever Data Protection Laws, regardless of national origin, conflict with U.S. common law preservation and discovery obligations, whether those laws take the form of privacy regulations, blocking statutes, trade secret, or other protections.

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.[23]

6. "U.S. Litigation" includes civil proceedings requiring the discovery of relevant information whether in federal, state, or other U.S. fora. "U.S. Litigation" does not include—and these International Litigation Principles are not intended to apply in—criminal proceedings or any other government investigations.[24]

---

[21] Many of the definitions used in the *International Litigation Principles* parallel the terms used in the EU Data Protection Directive and are also found in the GDPR. We use these definitions intentionally in order to achieve and maintain a common platform of understanding. It should be noted, however, that the *International Litigation 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.

[22] Under the GDPR, a Data Processor who is not also a Data Controller may nevertheless also become subject to a similar level of accountability as a Data Controller or subject to potential joint liability for processing performed on behalf of a Data Controller. GDPR, *supra* note 2, at arts. 28(10) and 82–83.

[23] The use of the word "data" in the *International Litigation 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.

[24] For specific guidance concerning internal and civil investigations implicating cross-border data transfers, *see* The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices* ("*International Investigations Principles*"), THE SEDONA CONFERENCE (forthcoming 2017 at https://thesedonaconference.org/node/107952).

III. THE SEDONA CONFERENCE INTERNATIONAL PRINCIPLES ON DISCOVERY, DISCLOSURE & DATA PROTECTION IN CIVIL LITIGATION

Principle 1

With regard to data that is subject to preservation, disclosure, or discovery in a U.S. legal proceeding, 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 limiting preservation or discovery. The first, recognized by the U.S. Supreme Court in *Aérospatiale*,[25] is that international comity[26] 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.[27] The notion of comity is traditionally supported by the U.S.

---

[25] Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522 (1987).

[26] 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 OF THE UNITED STATES § 101 cmt. e (1987) (quoting Hilton v. Guyot, 159 U.S. 113, 163–64 (1895)).

[27] *See Aérospatiale,* 482 U.S. at 546:

> [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 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, 304 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. Sociétée Commerciale Toutelectric, 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. Ct. 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); *In re* Xarelto (Rivaroxaban) Prods. Liab. Litig., MDL 2592, 2016 WL 3923873, at *17 (E.D. La., Jul. 21, 2016) (noting that "the balancing of national interests carries the most weight" among the factors considered by courts engaging in a comity analysis).

judiciary as presumptively applicable and necessary for the functioning of the international legal system.[28] It has been described as the "the mortar which cements together a brick house."[29] The "due respect" standard advanced by Principle 1 applies this presumption while recognizing that comity is not without limits.[30] The second tenet, consistent with Fed. R. Civ. P. 26(g), 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.[31]

---

[28] *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 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.'").

[29] *Id.*

[30] *Id.* at 937–38. ("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.")

[31] *See* FED. R. CIV. P. 26(g):

> (g) Signing Disclosures and Discovery Requests, Responses, and Objections.
>
> (1) Signature Required; Effect of Signature. Every disclosure under Rule 26(a)(1) or (a)(3) and every discovery request, response, or objection must be signed by at least one attorney of record . . . By signing, an attorney or party certifies that to the best of the person's knowledge, information, and belief formed after a reasonable inquiry: (A) with respect to a disclosure, it is complete and correct as of the time it is made; and (B) with respect to a discovery request, response, or objection, it is: (i) consistent with these rules and warranted by existing law or by a nonfrivolous argument for extending, modifying, or reversing existing law, or for establishing new law; (ii) not interposed for any improper purpose, such as to harass, cause unnecessary delay, or needlessly increase the cost of litigation; and (iii) neither unreasonable nor unduly burdensome or expensive, considering the needs of the case, prior discovery in the case, the amount in controversy, and the importance of the issues at stake in the action.

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); Strauss v. Credit Lyonnais, S.A., 249 F.R.D. 429, 439 (E.D.N.Y. 2008) (noting that courts within the Second Circuit consider "'the good faith of the party resisting discovery'") (quoting Minpeco, S.A. v. Conticommodity Servs., Inc., 116 F.R.D. 517, 523 (S.D.N.Y. 1987)); NML Capital v. Republic of Argentina, No. 03 Civ. 8845, 2013 U.S. Dist. LEXIS 17572, at *45 (S.D.N.Y. Feb. 8, 2013) (same); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 cmt. h (1987) ("Parties to litigation . . . may be required to show that they have made serious efforts before appropriate authorities

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, 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 U.S. 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 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.[32] 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. For example, parties to a litigation are required to meet and confer in order to attempt "in

---

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).

[32] Under U.S. law, the duty to preserve relevant information arises when litigation is "reasonably anticipated." The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265, 268, 69 (2010), *available at* https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Legal%20Holds. ("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.").

good faith to agree on the proposed discovery plan[.]"[33] However, efforts to define good faith usually involve trying to identify what it is not.[34] That is, if an action is not in "bad faith," then it must be in "good faith."[35] Courts often assess good faith to determine exemptions from liability or to assess rights and obligations. Courts interpreting federal statutes, for example, traditionally have interpreted "good faith" to encompass a subjective standard and "reasonableness" to encompass an objective standard.[36] 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.[37]

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 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."[38]

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.[39] Courts and parties are required to apply the rules to achieve the "just, speedy, and inexpensive determination of every action and proceeding."[40] For example, courts are obliged to restrict discovery where it is outside the scope permitted

---

33 FED. R. CIV. P. 26(f)(2).

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

35 The definition of "bad faith," itself, is subject to dispute. The architects of Fed. R. Civ. P. 37(e) removed the term from early drafts of the proposed rule, noting that clarity required a court to make a specific finding of "intent to deprive an-other party of the information's use" before imposing a sanction for the loss or destruction of ESI subject to discovery.

36 *See, e.g.,* Rossi v. Motion Picture Ass'n of Am., 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. § 512(c)(3)(A)(v), analyzing similar interpretations under various federal statutes and noting that "the objective reasonableness standard is distinct from the subjective good faith standard, and that Congress understands this distinction").

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

38 Flowers v. Torrance Mem'l Hosp. Med. Ctr., 884 P.2d 142, 144 (Cal. 1994).

39 *See* FED. R. CIV. P. 26(b)(1).

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

by Fed. R. Civ. P. 26(b)(1)—i.e., not relevant to any party's claim or defense or not proportional to the needs of the case, considering the importance of the issues at stake in the action, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit.[41] 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.[42] Commentaries published by other TSC Working Groups in the U.S. and Canada have expounded on the application of proportionality to common law discovery.[43]

In the *Aérospatiale* decision, the U.S. Supreme Court 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.[44] 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.

---

41 FED. R. CIV. P. 26(b)(2)(C)(iii); FED. R. CIV. P. 26(b)(1).

42 FED. R. CIV. P. 26(g)(1)(B)(iii); s*ee 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.").

43 The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, THE SEDONA CONFERENCE (November 2016 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Proportionality; *The Sedona Canada Commentary on Proportionality in Electronic Disclosure and Discovery*, THE SEDONA CONFERENCE (October 2010 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Canada%20Commentary%20on%20Proportionality%20in%20Electronic%20Disclosure%20and%20Discovery.

44 Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522, 544 n.28 (1987) (quoting RESTATEMENT OF FOREIGN RELATIONS LAW OF THE UNITED STATES (REVISED) § 437(1)(c) (Tent. Draft No. 7, 1986) (approved May 14, 1986), subsequently adopted as RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 442(1)(c)); *see also* British Int'l Ins. Co. v. Seguros La Republica, S.A., 90 Civ. 2370, 2000 U.S. Dist. LEXIS 7509, at *26–27 (S.D.N.Y. June 1, 2000) (noting that *Aérospatiale* quoted the "tentative draft of Restatement of Foreign Relations Law of the United States (Revised) § 437(1)(c), subsequently adopted as Restatement (Third) of Foreign Relations Law of the United States § 442(1)(c)").

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 Litigation 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[45] *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 protect the information, 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, likely including measures to restrict distribution and maintain confidentiality, which often can be achieved through the use of stipulations and court orders, as described in Principle 4, *infra*.

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 that is both *relevant* to the claims and defenses raised by the pleadings and *in proportion* to the needs of the case.[46] Courts especially emphasize

---

[45] The Sedona Conference, *Commentary on Rule 34 and Rule 35 "Possession, Custody, or Control," supra* note 14.

[46] Discovery in U.S. Litigation is not unlimited. The Federal Rules of Civil Procedure have been amended several times in order to correct perceived abuses of discovery. In 2015, Fed. R. Civ. P. 26(b)(1) was amended to remove references to discovery of information related to the general "subject matter" of the dispute, and to clarify that all discovery must be relevant to the stated claims and defenses in the litigation. Most importantly, Fed. R. Civ. P. 26(b)(1)

this point when it comes to Protected Data, considering whether the information sought is *necessary, vital, or crucial* to a claim or defense before compelling production, in light of comity concerns.[47] Narrowing the focus of preservation and discovery through stipulations and court orders can provide the same benefit.

This heightened level of scrutiny aligns with the approach taken by 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

---

now states that all discovery is subject to six proportionality factors: "the importance of the issues at stake in the litigation, the amount in controversy, the parties' relative access to relevant information, the parties' resources, the importance of the discovery in resolving the issues, and whether the burden or expense of the proposed discovery outweighs its likely benefit." Most state courts, however, retain broader definitions of the scope of discovery to include information relevant to the "subject matter of the dispute," with only oblique references to limitations based on proportionality factors. It is anticipated that this will change over the next few years, as more states conform to the narrower scope of Fed. R. Civ. P. 26(b)(1), and state court judges become open to applying proportionality factors to limit the scope of discovery when properly raised by the parties.

47 *See, e.g., In re* Vitamins Antitrust Litig., No. 99-197, 2001 U.S. Dist. LEXIS 8904, at *56 n.20 (D.D.C. June 20, 2001); Strauss v. Credit Lyonnais, S.A., 249 F.R.D. 429, 440 (E.D.N.Y. 2008) (noting that "some courts have applied a more stringent test of relevancy when applying the Federal Rules to foreign discovery" focusing on whether the information sought is vital, such as the courts in *Aérospatiale* and *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468, 1475 (9th Cir. 1992)); *see also In re* Bard IVC Filters Prods. Liab. Litig., MDL 15-02641, 2016 WL 4943393, at *5 (D. Ariz. Sept. 16, 2016) ("[t]he Court concludes that the burden and expense of searching ESI from 18 foreign entities over a 13-year period outweighs the benefit of the proposed discovery—a mere possibility of finding a foreign communication inconsistent with United States communication"). Courts operating under the broader scope of discovery permissible under Fed. R. Civ. P. 26(b)(1) before the 2015 Amendments often ordered the production of documents when the information sought was only relevant, even if not vital to the litigation, such as the court in *Compagnie Française D'Assurance Pour Le Commerce Extérieur v. Phillips Petroleum Co.*, 105 F.R.D. 16, 32 n.8 (S.D.N.Y. 1984) ("In ordering production of these documents, this Court does not need to find, nor can it find at this point, that the requested documents are 'vital' . . . ."). *See also* Milliken & Co. v. Bank of China, 758 F. Supp. 2d 238, 245–46 (S.D.N.Y. 2010) (noting that "Courts have diverged in their treatment of the importance of the information requested as a factor in determining whether to require a party to utilize Convention procedures. Some suggest that in order for this factor to be considered favorable to the requesting party, the information sought must be 'vital' to the litigation [citing *Richmark*, 959 F.2d at 1475, and *Strauss*, 249 F.R.D. at 440]. Others hold that it is sufficient for the requested evidence simply to be relevant" (citing Reino de Espana v. Am. Bureau of Shipping, 03 Civ. 3373, 2005 U.S. Dist. LEXIS 15685, at *7 (S.D.N.Y. Aug. 1, 2005) and *Compagnie Française D'Assurance Pour Le Commerce Extérieur*, 105 F.R.D. at 32 n.8)). The *Milliken* court further held that with respect to the categorization of evidence as 'vital' or not 'vital,':

> it is necessary only to judge the degree of importance of the information—where it falls on the spectrum between merely relevant at one end and crucial at the other—and then weigh this along with all the other factors. . . . In any event, the analysis in this case does not turn on the standard for evaluating the relevance factor, since the information sought by Milliken is clearly crucial to the litigation . . . [and] strongly favors Milliken.

> 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.[48]

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 discovery 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 as specified by Fed. R. Civ. P. 34(b)(1); and (2) restricting the breadth of requests to fewer, more relevant custodians, allowing an iterative process to extend the request, if needed.

B. Discovery with Specificity

In the U.S., a requesting party often makes broad requests for disclosure and production of relevant information. Although Fed. R. Civ. P. 34(b)(1) makes such generalized requests inappropriate, phrases such as "any and all" still appear in many requests, especially in state court litigation, where the state has not yet conformed its rules to the Federal Rules. However, many courts that have considered the matter have required that production of materials implicating foreign Data Protection Laws must be relevant and also necessary or vital to the litigation.[49]

A 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.

---

[48] Article 29 Data Protection Working Party, *Working Document 1/2009 on Pre-trial Discovery for Cross-border Civil Litigation*, 00339/09/EN, WP 158, 10–11 (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 Data Protection Directive), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf.

[49] *See* Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522, 544 n.28 (1987) (noting that "the importance to the . . . litigation of the documents or other information requested" is one of the factors relevant to any comity analysis) (citing RESTATEMENT OF FOREIGN RELATIONS LAW OF THE UNITED STATES (REVISED) § 437(1)(c) (Tent. Draft No. 7, 1986) (approved May 14, 1986)); Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1475 (9th Cir. 1992) (noting unwillingness to override foreign laws unless outcome

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 law by endorsing a narrowing of broad discovery requests.[50]

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 around 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.

Phased Discovery is contemplated by the second stage of the three-stage approach advanced by the *International Litigation 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.[51]

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 local Data Protection Laws (for example, federal laws such as the Gramm–Leach–Bliley Act (GLBA)[52] and Health

---

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"); Gucci Am., Inc. v. Curveal Fashion, 09 Civ. 8458, 2010 U.S. Dist. LEXIS 20834, at *5–6, *21–22 (S.D.N.Y. Mar. 8, 2010) (requiring production pursuant to the Restatement and *Aérospatiale*, and noting that the information sought was "both relevant and vital to the litigation"); *In re* Activision Blizzard, Inc. Stockholder Litig., 86 A.3d 531, 545 (Del. Ch. 2014) (same).

[50] *See Aérospatiale*, 482 U.S. at 545 ("When it is necessary to seek evidence abroad . . . the district court must supervise pretrial proceedings particularly closely to prevent discovery abuses."); Devon Robotics v. DeViedma, No. 09-cv-3552, 2010 U.S. Dist. LEXIS 108573, at *10–*17 (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").

[51] It should be noted, however, that consistent with the second tenet of Principle No. 1, phasing of discovery should be proposed in good faith and not for an improper purpose or to delay preservation or discovery.

[52] Pub. L. No. 106–102, 113 Stat. 1338 (enacted Nov. 12, 1999 and codified in various sections of Chapters 12 and 15 of the U.S.C.).

Insurance Portability and Accountability Act (HIPAA),[53] and state laws such as Massachusetts Standards for The Protection of Personal Information of Residents of the Commonwealth[54]);

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.[55]

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, limiting by date range or data source, or the application of computer algorithms designed to search and retrieve data relevant to specific criteria. Filtering, 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" and similar treatment to Protected Data take place in the EU to minimize the exposure of non-relevant and unnecessary Protected Data to disclosure risks.[56] Depending on the context, anonymization or pseudonymization techniques may also be considered.[57]

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

---

53 Pub. L. No. 104–191, 110 Stat. 1936 (enacted Aug. 21, 1996 and codified in various sections of Chapters 29 and 42 of the U.S.C.).

54 201 MASS. CODE REGS. 17.00 (2010), *available at* http://www.mass.gov/ocabr/docs/idtheft/201cmr1700reg.pdf.

55 *See Model U.S. Federal Court Order Addressing Cross-Border ESI Discovery*, *infra* Appendix B.

56 In WP 158 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 ("It may be that this would require the services of a trusted third party in a Member State.").

57 "Pseudonymisation" is defined in the GDPR as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person." GDPR, *supra* note 2, at art. 4(5).

done in a way that does not inappropriately compromise the produced data's functionality and evidentiary value. 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 irrelevant metadata or because of redaction problems with native format.[58]

[58] *See, e.g.*, Hon. Michael M. Baylson, *Cross-Border Discovery at a Crossroads*, 100 JUDICATURE 56, 59 (Winter 2016), *available at* https://law.duke.edu/judicature/volume100-number4/ (proposing the possible use of redactions and production in hard-copy format to eliminate protected personal information from ESI obtained from cross-border sources).

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.[59]

The three-stage approach advanced by the *International Litigation 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 protects and limits the use of sensitive information such as trade secrets and 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.

A. 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 agreement is not reached. 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 under the auspices and protections of

[59] 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."); *see also* King v. Olympic Pipeline Co., 16 P.3d 45, 62 (Wash. Ct. App. 2000) (noting the "need for protective orders to preserve privacy interests" and a court's "substantial latitude to decide when a protective order is appropriate and what degree of protection is required given the unique character of the discovery process.").

the U.S. court.[60] The *Model U.S. Federal Court Protective Order*, set forth in Appendix C, 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.

B. 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.

C. 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 D and described in the Comment to Principle 5.

---

[60] 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 to a grand jury in a criminal matter. However, grand jury proceedings are sealed to prevent public disclosure. FED. R. CRIM. P. 6(e)(6). 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 a showing that the civil protective order was improvidently granted or upon demonstration of "compelling need" or "extraordinary circumstances." 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 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* (the "*Protocol*") set forth in Appendix D. 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.[61] 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. The identification and significance of the Data Protection Laws at issue (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 (e.g., 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 identifies or is likely to identify the Data Subject, sensitive personal data, trade secret data, any other restricted data)

5. Confirmation that the Protected Data is subject to a protective order or stipulation that may, for example, restrict its use and dissemination, impose confidentiality, compel security measures, provide for Data Subject access, and restrict onward transfer; attaching a copy of the protective order or stipulation

---

[61] Art. 24(1) of the forthcoming GDPR (*supra* note 2) specifically requires that the controller should be able to "demonstrate that processing is performed in accordance with this Regulation."

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 to 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, data protection authority, works council)

9. Basis upon which Protected Data is transferred to the U.S. in accordance with applicable Data Protection Laws (such as the legal claims derogation under the 1995 EU Data Protection Directive[62]), 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)

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 processes have been adopted and followed by the parties 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.

---

[62] EU Data Protection Directive, *supra* note 1, at § IV, art. 26(d) ("the transfer is necessary or legally required . . . for the establishment, exercise or defence of legal claims").

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, including security 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*,[63] persons and organizations need not keep all information forever. Rather, reasonable and systematic records management rules can be applied, provided 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.[64]

Privacy by design is part of the "data minimization" principle (GDPR art. 5(1)(c)), a core principle of the EU Data Protection Laws, whereby data processing should be "adequate, relevant and limited

---

[63] 544 U.S. 696, 704 (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).

[64] "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 Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on*

to what is necessary in relation to the purposes for which they are processed." The less personal data collected or retained by an organization, the lower the costs and risks to data protection.[65]

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, confidentiality, and security of the data while it is being preserved. This includes meaningful efforts to implement privacy-by-design protections in new ESI systems, consistent with the GDPR's requirements. 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 1995 EU Data Protection Directive and the GDPR, 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."[66] 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.[67]

A Digital Agenda for Europe, at 17 n.21, COM (2010) 245 final/2 (Aug. 26, 2010), *available at* http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245R(01). The privacy-by-design principle is now codified in Article 25(1) of the GDPR:

> Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

65 EU Data Protection Directive, *supra* note 1, at art. 6(1)(c); UK Information Commissioner's Office, *The Guide to Data Protection*, at 37–38, ICO (Oct. 25, 2016), *available at* https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-6.pdf.

66 The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, *supra* note 32.

67 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

In re Activision Blizzard, Inc. Stockholder Litig., 86 A.3d 531 (Del. Ch. 2014)

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

Apple Inc. v. Samsung Elecs. Co., 881 F. Supp. 2d 1132 (N.D. Cal. 2012)

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

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

In re Bard IVC Filters Products Liab. Litig., MDL 15-02641, 2016 WL 4943393 (D. Ariz. Sept. 16, 2016)

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

British Int'l Ins. Co. v. Seguros La Republica, S.A., 90 Civ. 2370, 2000 U.S. Dist. LEXIS 7509 (S.D.N.Y. June 1, 2000)

Compagnie Française D'Assurance Pour Le Commerce Extérieur v. Phillips Petroleum Co., 105 F.R.D. 16 (S.D.N.Y. 1984)

Da Silva Moore v. Publicis Groupe S.A., 287 F.R.D. 182 (S.D.N.Y. 2012)

Devon Robotics v. DeViedma, No. 09-cv-3552, 2010 U.S. Dist. LEXIS 108573 (E.D. Pa. Oct. 8, 2010)

Flowers v. Torrance Mem'l Hosp. Med. Ctr., 884 P.2d 142 (Cal. 1994)

Genentech, Inc. v. Trs. of the Univ. of Pa., No.10-2037, 2011 U.S. Dist. LEXIS 128526 (N.D. Cal. Nov. 7, 2011)

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

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

Gucci Am., Inc. v. Curveal Fashion, 09 Civ. 8458, 2010 U.S. Dist. LEXIS 20834 (S.D.N.Y. Mar. 8, 2010)

Hilton v. Guyot, 159 U.S. 113 (1895)

King v. Olympic Pipeline Co., 16 P.3d 45 (Wash. Ct. App. 2000)

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

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

Lord Abbett Mun. Income Fund, Inc. v. Asami, No. C-12-03694, 2014 WL 5477639 (N.D. Cal. Oct. 29, 2014)

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

Marshall v. Brunner, 668 F.2d 748, 753 (3d Cir. 1982)

Marten Transp., Ltd. v. PlattForm Advert., Inc., No. 14-cv-02464-JWL-TJJ, 2016 WL 492743 (D. Kan. Feb. 8, 2016)

Milliken & Co. v. Bank of China, 758 F. Supp. 2d 238 (S.D.N.Y. 2010)

Minpeco, S.A. v. Conticommodity Servs., Inc., 116 F.R.D. 517 (S.D.N.Y. 1987)

NML Capital v. Republic of Argentina, No. 03 Civ. 8845, 2013 U.S. Dist. LEXIS 17572 (S.D.N.Y. Feb. 8, 2013)

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

Pension Comm. of Univ. of Montreal Pension Plan v. Banc of Am. Sec. LLC, 685 F. Supp. 2d 456 (S.D.N.Y. 2010)

Reino de Espana v. Am. Bureau of Shipping, 03 Civ. 3373, 2005 U.S. Dist. LEXIS 15685, (S.D.N.Y. Aug. 1, 2005)

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 Am., 391 F.3d 1000 (9th Cir. 2004)

S2 Automation LLC v. Micron Tech., Inc., No. 11-0884, 2012 U.S. Dist. LEXIS 120097 (D.N.M. Aug. 9, 2012)

Salerno v. Lecia, Inc., 97-CV-9735(H), 1999 U.S. Dist. LEXIS 7169 (W.D.N.Y. Mar. 23, 1999)

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

Shcherbakovskiy v. Da Capo Al Fine, Ltd., 490 F.3d 130 (2d Cir. 2007)

In re Ski Train Fire of November 11, 2000 Kaprun, Aus., MDL 1428, 2006 U.S. Dist. LEXIS 29987 (S.D.N.Y. May 16, 2006)

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

Société Nationale Industrielle Aérospatiale v. U.S. Dist. Ct. for the S. Dist. 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)

In re Vitamins Antitrust Litig., No. 99-197, 2001 U.S. Dist. LEXIS 8904 (D.D.C. June 20, 2001)

Volkswagen, A.G. v. Valdez, 909 S.W.2d 900 (Tex. 1995)

In re Xarelto (Rivaroxaban) Prods. Liab. Litig., MDL 2592, 2016 WL 3923873 (E.D. La., Jul. 21, 2016)

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

U.S. RULES

FED. R. CIV. P. 1

FED. R. CIV. P. 26(a)(1)

FED. R. CIV. P. 26(a)(1)(A)

FED. R. CIV. P. 26(a)(1)(A)(ii)

FED. R. CIV. P. 26(b)(1)

FED. R. CIV. P. 26(b)(2)

FED. R. CIV. P. 26(b)(2)(C)

FED. R. CIV. P. 26(b)(2)(C)(iii)

FED. R. CIV. P. 26(f)(2)

FED. R. CIV. P. 26(g)

FED. R. CIV. P. 26(g)(1)(B)(iii)

FED. R. CIV. P. 34

FED. R. CIV. P. 34(a)(1)(A)

FED. R. CIV. P. 34(b)(1)

FED. R. CIV. P. 37(e)

FED. R. CIV. P. 45

FED. R. CRIM. P. 6(e)(6)

U.S. RESTATEMENTS

RESTATEMENT OF FOREIGN RELATIONS LAW OF THE UNITED STATES (REVISED) § 437(1)(c) (Tent. Draft No. 7, 1986) (approved May 14, 1986)

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES (1987)

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 101 cmt. e (1987)

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 442 cmt. h (1987)

RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 442(1)(c) (1987)

U.S. STATUTES

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

Gramm–Leach–Bliley Act, Pub. L. No. 106–102, 113 Stat. 1338 (1999)

Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996)

Standards for the Protection of Personal Information of Residents of the Commonwealth of Massachusetts, 201 MASS. CODE REGS. 17.00 (2010)

INTERNATIONAL AUTHORITIES

Columbia

General Provisions for the Protection of Personal Data, Law 1581 (October 2012)

European Union

Article 29 Data Protection Working Party, *Working Document 1/2009 on Pre-trial Discovery for Cross-border Civil Litigation*, 00339/09/EN, WP 158 (Feb. 11, 2009), http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp158_en.pdf

Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield, COM (2016) 4176 final (Dec. 12, 2016), http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf

Press Release, Article 29 Working Party Statement on the decision of the European Commission on the EU-U.S. Privacy Shield (July 26, 2016), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/20160726_wp29_wp_statement_eu_us_privacy_shield_en.pdf

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on A Digital Agenda for Europe, 26/8/2010, COM (2010) 245 final/2 (Aug. 26, 2010), http://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52010DC0245R(01)

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. (L 281), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:EN:NOT

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119/1), http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf

Schrems v. Data Protection Comm'r (Ireland), Case C-362/14, 2015 E.C.R. (October 6, 2015), http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=en

Germany

BUNDESDATENSCHUTZGESETZ [BDSG] [FEDERAL DATA PROTECTION ACT], Dec. 20, 1990, BGBL. at 2954, as amended

Philippines

Data Privacy Act of 2012, Republic Act No. 10173 (August 2012)

South Africa

The Protection of Personal Information (POPI) Act, No. 4 of 2013 (November 2013)

United Kingdom

UK Information Commissioner's Office, *The Guide to Data Protection*, https://ico.org.uk/media/for-organisations/guide-to-data-protection-2-6.pdf

Testimony of the Rt. Hon Karen Bradley MP, Secretary of State for Culture, Media and Sport, given at the Parliamentary Committee Meeting on Responsibilities of the Secretary of State for Culture, Media and Sport, HC 764, October 24, 2016, http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/culture-media-and-sport-committee/responsibilities-of-the-secretary-of-state-for-culture-media-and-sport/oral/42119.html

OTHER AUTHORITIES

JUDICIAL CONF. COMM. ON RULES OF PRACTICE & PROCEDURE, REPORT OF THE JUDICIAL CONF. COMM. ON RULES OF PRACTICE AND PROCEDURE (Sept. 2014), http://www.uscourts.gov/sites/default/files/fr_import/ST09-2014.pdf

Hon. Michael M. Baylson, *Cross-Border Discovery at a Crossroads*, 100 JUDICATURE 56 (Winter 2016), https://law.duke.edu/judicature/volume100-number4/

Hon. Michael Baylson, *Model Pretrial Order Re International Discovery*, The 8th Annual Sedona Conference International Programme, Berlin, June 2016

The Radicati Group, *Email Statistics Report, 2015-2019*, http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf

The Sedona Conference, *The Case for Cooperation*, 10 SEDONA CONF. J. 339 (2009 Supp.), https://thesedonaconference.org/publication/Supplement%20to%20Volume%2010%20of%20The%20Sedona%20Conference%20Journal%C2%AE%20-%20Cooperation

The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, 11 SEDONA CONF. J. 265 (2010), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Legal%20Holds

The Sedona Conference, *Commentary on Legal Holds: The Trigger & The Process*, THE SEDONA CONFERENCE (August 2007 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Legal%20Holds

The Sedona Conference, *Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control,"* 17 SEDONA CONF. J. 467 (2016), https://thesedonaconference.org/publication/The%20Sedona%20Conference%20Commentary%20on%20Rule%2034%20and%20Rule%2045%20%E2%80%9CPossession%2C%20Custody%2C%20or%20Control%E2%80%9D

The Sedona Conference, *Commentary on Proportionality in Electronic Discovery*, THE SEDONA CONFERENCE (November 2016 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Canada%20Commentary%20on%20Proportionality%20in%20Electronic%20Disclosure%20and%20Discovery

The Sedona Conference, *International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices ("International Investigations Principles")*, THE SEDONA CONFERENCE (forthcoming 2017 at https://thesedonaconference.org/node/107952)

The Sedona Conference, *International Principles on Discovery, Disclosure and Data Protection: Best Practices, Recommendations & Principles for Addressing the Preservation Discovery of Protected Data in U.S. Litigation, European Union Ed.*, THE SEDONA CONFERENCE (Dec. 2011 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Conference%C2%AE%20Intern Interna%20Principles%20on%20Discovery%2C%20Disclosure%20%2526%20Data%20Protection

The Sedona Conference, *The Sedona Canada Commentary on Proportionality in Electronic Disclosure and Discovery*, THE SEDONA CONFERENCE (October 2010 Public Comment Version), https://thesedonaconference.org/publication/The%20Sedona%20Canada%20Commentary%20on %20Proportionality%20in%20Electronic%20Disclosure%20and%20Discoveryhttps://thesedonaco nference.org/download-pub/468

The Sedona Conference, *The Sedona Conference Cooperation Proclamation*, THE SEDONA CONFERENCE (2008), http://www.thesedonaconference.org/content/tsc_cooperation_proclamation

The Sedona Conference, *The Sedona Guidelines: Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases*, THE SEDONA CONFERENCE (March 2007), https://thesedonaconference.org/publication/Working%20Group%202%20Guidelines

Robert S. Summers, *The General Duty of Good Faith—Its Recognition and Conceptualization*, 67 CORNELL L. REV. 810 (1982), http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article= 2399&context=facpub

Robert S. Summers, *"Good Faith" in General Contract Law and the Sales Provisions of the Uniform Commercial Code*, 54 VA. L. REV. 195 (1968), http://scholarship.law.cornell.edu/cgi/viewcontent.cgi?article=2408&context=facpub

U.S. Department of Commerce, *Privacy Shield Framework*, https://www.privacyshield.gov/Program-Overview

Paul D. Weiner & Denise E. Backhouse, *Securing Protected Data in U.S. Legal Proceedings: Protective Orders*, The 8th Annual Sedona Conference International Programme, Berlin, June 2016, https://thesedonaconference.org/system/files/Securing%20Protected%20Data%20in%20U.S.%20 Legal%20Proceedings_Protective%20Orders.pdf.

Appendix B: Model U.S. Federal Court Order Addressing Cross-Border ESI Discovery[68]

UNITED STATES DISTRICT COURT

_____ DISTRICT OF _____

_____,	)	
	)	
Plaintiff.	)	Case No.: _____
	)	
v.	)	**Pretrial Order Regarding**
	)	**International Discovery**
_____,	)	
	)	
Defendant.	)	
	)	

PRETRIAL ORDER RE: INTERNATIONAL DISCOVERY

AND NOW, this day of _____, 20__:

Pursuant to the Court's authority under Rule 16, Fed. R. Civ. P., the parties having advised the Court [the Court determining from review of the pleadings and any other initial papers in the case] that international discovery may be involved, which may result in substantial delays in concluding discovery, the Court sets special procedures for expediting international discovery.

[68] Appendix B is a model Pretrial Order addressing cross-border discovery pursuant to a U.S. Court's authority under Fed. R. Civ. P. 16. The Hon. Michael M. Baylson (E.D. Pa.), an active member of The Sedona Conference Working Group 6, granted permission to include this *Model U.S. Federal Court Order Addressing Cross-Border ESI Discovery* as an appendix to the *International Litigation Principles*. He developed this model in order to facilitate party discovery outside the U.S. and/or pursuant to the laws of other countries, and to enable courts to promptly rule on any dispute that arises concerning international discovery. This model can be tailored to the specific issues in individual matters. The Sedona Conference WG6 thanks Judge Baylson for his permission to include this model as an appendix. *See* U.S. District Judge Michael Baylson (EDPA), *Model Pretrial Order Re International Discovery*, The 8th Annual Sedona Conference International Programme, Berlin, June 2016.

The provisions of this Order are intended to facilitate the parties taking of discovery outside the United States and/or pursuant to the laws of other countries, and will enable the Court to promptly rule on any disputes that arise concerning international discovery.

It is therefore **ORDERED**:

1. Within _____ days, any party which intends to initiate discovery outside of the United States shall file and serve a statement making disclosure of its intention as of this time, including, but not limited to, the following:

(a) Whether applications will be made under the Hague Convention or any other treaty.

(b) Whether Letters Rogatory will be used.

(c) Whether parties abroad are likely to be deponents in this case.

(d) Whether documents located outside the United States will be sought for production, including but not limited to, electronically stored information (ESI).

(e) Whether a party is aware of any blocking statutes or Data Protection Laws that may apply to a request for discovery in a particular country and, if so, identify the country and if possible cite the laws which may be applicable.

2. Within _____ days other parties shall respond to this initial disclosure of foreign discovery, by commenting:

(a) To what extent it will or will not oppose such discovery.

(b) If there will be opposition, state concisely the nature of the opposition and the reasons.

3. Within _____ days after the response, the parties shall meet and confer to discuss reaching agreement, or narrowing disputes concerning:

(a) Conducting discovery outside of the United States, pursuant to the Federal Rules of Civil Procedure or otherwise.

(b) What date shall be set to complete international discovery.

(c) Whether any objections will be presented to this Court and, if so, when?

(d) Whether any protective order will be sought and the extent to which disputes remain as to the contents of a protective order.

4. The Court set a deadline for the initiation of any discovery to take place outside the United States as _____ [date].

5. Motions that may be necessary or appropriate on international discovery issues will be filed no later than _____[date]. Responses will be due within fourteen (14) days, and a reply brief should be filed within fourteen (14) days thereafter.

6. In most countries with blocking statutes and/or data protection rules, an authorized official or judge within that country, may be permitted to negotiate, hear, and/or authorize disclosure of information for use in litigation, even though it is arguable that a blocking statute or data protection law may be construed otherwise. In each party's pretrial disclosures on international discovery, the Court requires each party relying on any such statute or rule to state:

(a) Its knowledge of this practice as applied to this case;

(b) Its position on this issue;

(c) The contact information for the official or judge in each country who is likely to be knowledgeable or authorized to act within that country.

7. The Court anticipates having pretrial conferences with counsel to discuss the course, progress, and any problems in international discovery. The first conference will take place on _____ [date]. Subsequent conferences will be scheduled on a need basis. If problems and issues arise frequently, the Court may schedule conferences on a regular basis.

8. Counsel who do not practice regularly in this District may appear by telephone by notifying Chambers at least 48 hours prior to any pretrial conference.

9. Counsel appearing at these conferences, whether in person or by telephone, shall be authorized to speak on behalf of their client, and shall discuss with their client issues as they are arising so that they can accurately inform the Court of their position.

10. If it appears that certain discovery is relevant in this case, but cannot be secured by normal means of discovery through the Federal Rules of Civil Procedure, or any convention or other recognized international procedure, the Court may itself undertake initiation of communications with any data protection officer of a foreign country or court of a foreign country to determine if such discovery can be authorized, facilitated, and completed on a prompt basis.

11. The obligations stated above apply throughout this litigation, and apply to any initiation of international discovery.

12. The Court encourages the parties to adopt, in this case, the Sedona Conference Principles of International Discovery, Disclosure & Data Protection as follows:

(a) 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.

(b) 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.

(c) 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.

(d) 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.

(e) 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.

(f) 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.

BY THE COURT:

_____

[INSERT JUDGE'S NAME], U.S.D.J.

IN THE UNITED STATES DISTRICT COURT

FOR THE _____ DISTRICT OF _____

_____,	)	
	)	
Plaintiff.	)	Case No.: _____
	)	
v.	)	**Pretrial Order Regarding**
	)	**International Discovery**
_____,	)	
	)	
Defendant.	)	
	)	

AND NOW, this day of _____, 20__, upon consideration of defendant's Motion for Issuance of Letters of Request Pursuant to the Hague Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, it is hereby **ORDERED** that said Motion is **GRANTED**.

It is further **ORDERED** that the original executed copies of the Letters of Request attached to defendant's Motion as Exhibits A and B shall be provided to counsel for defendant to serve and execute in conformity with the Hague Convention.

BY THE COURT:

_____

[INSERT JUDGE'S NAME], U.S.D.J.

Appendix C:
Model U.S. Federal Court Protective Order

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**: Except as provided in Paragraphs 18(b) and 32(b), *infra,* this Order does not and will not govern any court 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.

5.1 **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, without limitation, 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) / Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and repealing Directive 95/46/EC (General Data Protection Regulation) (L119/1)(EU personal information); Data Protection Act 1998 (c. 29) (United Kingdom personal information); the German Federal Data Protection Act (Germany personal information); the Spanish Data Protection Act 15/1999; 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 Act on the Protection of Personal Information (Law No. 57 of 2003) (APPI) (Japan personal information). ***[N.B.: This list must be updated and tailored to the relevant jurisdictions in a particular matter]***

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:

6.1 **Documents**: [INSERT]

6.2 **Deposition and Other Proceedings**: [INSERT]

6.3 **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 notify the Producing Party, 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 forms), 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:

11.1 [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:

12.1 [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**: Except as provided in Paragraph 30, *infra,* 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.[69] [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

---

[69] The presumption in U.S. courts is that all filings are public, unless the court makes a specific finding of good cause for sealing the filing. In the absence of a local rule or standing order addressing the process of filing of confidential material and requesting that it be sealed, a common provision of a negotiated protective order is for confidential material to be filed with the court clerk under temporary seal with notice to the parties and a 10-day period for any party to file a motion to prevent the material from automatically becoming part of the public record. *See generally,* The Sedona Conference, *The Sedona Guidelines: Best Practices Addressing Protective Orders, Confidentiality & Public Access in Civil Cases*, THE SEDONA CONFERENCE (March 2007), *available at* https://thesedonaconference.org/publication/Working%20Group%202%20Guidelines.

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.

20.1 **Challenge**: [INSERT STEPS]

20.2 **Meet and Confer and Motion**: [INSERT STEPS]

20.3 **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 independently published to the general public, and relevant Data Protection Laws do not apply. 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 20 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.

23.1 [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.[70]

---

[70] The parties may want to insert a mutually agreed upon mediation clause to resolve any issues arising after termination of the litigation, should the Court decline to retain jurisdiction.

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**:

    28.1 **Change in Status**: [INSERT]

    28.2 **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, unless it has been lawfully placed on the public record. 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, document

request, 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 email 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. The Receiver will ensure that Confidential Material or Highly Confidential Material is adequately secured during transfer. 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:

32.1 Any party may redact Protected Data that it claims, in good faith, requires protection 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.

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

32.3 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 20.

33. **Personally Identifiable Information**: Personally identifiable information that a party has designated as Protected Data as defined in Section 5.a, *supra*, 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.

34. **Data Security**: Any person in possession of Confidential Material or Highly Confidential Material shall maintain a written information security program that includes reasonable administrative, technical, and physical safeguards designed to protect the security and confidentiality of such Confidential Material or Highly Confidential Material, protect against any reasonably anticipated threats or hazards to the security of such Confidential Material or Highly Confidential Material, and protect against unauthorized access to Confidential Material or Highly Confidential Material.[71] To the extent a party or person does not have an

[71] The language sets forth minimum standards that should be included. Depending on the circumstances, other provisions that may be specified include utilization of Secure File Transfer Protocol (SFTP), Secure Sockets Layer (SSL), or Virtual Private Network (VPN) technologies when transferring files; encryption of the data, when data is being transferred to and stored by the Receiver; controlled access to the files themselves (e.g., background checks for personnel handling the data stored in servers, rooms, etc.; agreement between parties as to specified vendor and data

information security program, they may comply with this provision by having the Confidential Material or Highly Confidential Material managed by and/or stored with eDiscovery vendors or claims administrators that maintain such an information security program. If a Receiving Party or Authorized Recipient discovers any loss of Confidential Material or Highly Confidential Material or a breach of security, including any actual or suspected unauthorized access, relating to another party's Confidential Material or Highly Confidential Material, the Receiving Party or Authorized Recipient shall: (1) promptly provide written notice to Disclosing Party of such breach; (2) investigate and make reasonable efforts to remediate the effects of the breach, and provide Disclosing Party with assurances reasonably satisfactory to Disclosing Party that such breach shall not recur; and (3) provide sufficient information about the breach that the Disclosing Party can reasonably ascertain the size and scope of the breach. The Receiving Party or Authorized Recipient agrees to cooperate with the Producing Party or law enforcement in investigating any such security incident. In any event, the Receiving Party or Authorized Recipient shall promptly take all necessary and appropriate corrective action to terminate the unauthorized access.

35. **End-of-Matter Data Disposition**: Upon final resolution of this Litigation the Parties will certify that all Confidential Material and/or Highly Confidential Material

security technologies); liquidated damages provision for breach, secured by a bond or other security; access rights management; physical space and device access and usage controls; or where applicable, incorporation of statutory or sectoral standards and specifications. *See* Paul D. Weiner & Denise E. Backhouse, *Securing Protected Data in U.S. Legal Proceedings: Protective Orders*, The 8th Annual Sedona Conference International Programme, Berlin, June 2016, *available at* https://thesedonaconference.org/system/files/Securing%20Protected%20Data%20in%20U.S.%20Legal%20Proceedings_Protective%20Orders.pdf.

has been returned to the Producing Party and/or been destroyed in a secure manner [INSERT DETAILS].[72]

36. **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.

37. **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.

---

[72] The decision to destroy material that has been subject to a legal hold has inherent risks that are best mitigated by an express agreement of the parties or an order by the Court. *See, e.g.,* Lord Abbett Mun. Income Fund, Inc. v. Asami, No. C-12-03694, 2014 WL 5477639 (N.D. Cal. Oct. 29, 2014) (disposal of computer hard drives permitted while appeal pending, upon finding that burden and expense of continued preservation outweighed any further value to the litigation).

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**
_____,	)	**Re: Protected Data**
	)	
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 agree to maintain and abide by the Data Security provisions and End-of-Matter Data Disposition provisions set forth in 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 D: The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol

INSTRUCTIONS

The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol (the "*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 extra-U.S. Data Protection Laws when foreign data needs to be processed and transferred for the purposes of U.S. Litigation. Second, the *Protocol* creates a record that can be presented to those with regulatory responsibilities for Data Protection, evidencing the steps taken to best comply with Data Protection Laws. The *Protocol* must be customized to record fully the actions undertaken to maximize legal compliance and should include a detailed explanation of the circumstances and factors taken into account. The following instructions should be used with the chart below:

1. Explain the reasons for preserving or collecting the data. Identify clearly the U.S. proceedings for which the Protected Data is processed and transferred. If the Protected Data is to be preserved or collected for reasons other than litigation, identify the legal proceeding requiring the processing and transfer.

2. Determine whether data required to be preserved, processed, or disclosed in the U.S. is subject to Data Protection Laws and, if so, which laws apply. Assess whether alternative, non-protected, sources of that relevant data exist. To the extent possible, produce non-protected sources of data, making production of relevant Protected Data less necessary. Determine the sources of relevant Protected Data, the methods of preservation, if it has been or will be further processed, and where it will ultimately be transferred.

3. Describe measures taken to minimize the processing and transfer of Protected Data, explaining the methodology used to filter and eliminate irrelevant Protected Data. These culling activities may begin with a questionnaire or an in-person interview, followed by iterative use of software tools and other processes, creating a subset of relevant and necessary Protected Data for disclosure. Consider compiling Protected Data locally or in a country that is not subject to the transfer restrictions under the applicable Data Protection law. Identify categories of Protected Data potentially affected by the applicable Data Protection Laws.

4. Describe the various categories of Protected Data that will be processed or transferred by type, including personal and sensitive personal data, trade secrets data, restricted data, consumer data, state secrets, etc.

5. If appropriate, consider using the *Model U.S. Federal Court Protective Order* (set forth in Appendix C) or similar protective orders, or stipulations with data protection language providing agreed-upon or court-ordered restrictions on the use, disclosure, and dissemination of Pro-

tected 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.

6. 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, or notice and acknowledgement documentation requesting consent and providing question and answer information, in writing or orally, in both English and the local language.

7. Identify steps taken to secure Protected Data by describing the protective measures undertaken by the Data Controller, including, for example, agreements with third parties, use of a protective order, the nature and type of encryption at rest and in transit, limitations on access to the Protected Data, and any other means of securing the Protected Data. Also describe procedures for responding in the event of a data breach.

8. Describe the efforts undertaken if notice is contemplated or required. Others to be consulted may include the Data Controller's data protection personnel such as data protection officers, data protection authorities with jurisdiction over the Protected Data, or local company organizations such as works councils.

9. Identify mechanism(s) used to legitimize the transfer of Protected Data. For the EU, depending on the U.S. recipient and transfer purpose, these mechanisms typically include the use of Binding Corporate Rules (intra-group transfers only), the new Privacy Shield certification,[73] Model Contracts, or some other means of satisfying transfer safeguard requirements.

10. Document procedures used to destroy or return Protected Data to the Data Controller when it is no longer necessary.

11. Consider identifying those responsible for overseeing preservation, processing, and transfer of the Protected Data and obtaining their signatures to signify that the steps recorded were in fact taken.

---

[73] The new EU/U.S. Privacy Shield came into effect on June 12, 2016, with certification available since August 1, 2016 (*Commission Implementing Decision of 12.7.2016 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield*, COM (2016) 4176 final (Dec. 12, 2016), *available at* http://ec.europa.eu/justice/data-protection/files/privacy-shield-adequacy-decision_en.pdf), replacing the old EU-U.S. Safe Harbor certification after the Commission decision on which it was based was declared invalid by the Court of Justice of the European Union on October 6, 2015.

The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol	
ACTION ITEM	**INFORMATION**
1. Purpose for processing and transfer of Protected Data	Identify the type of legal proceeding for which Protected Data is being 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, filing date, description of legal proceeding)
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 to which it will be transferred
3. Measures taken to minimize the processing and transfer of Protected Data	Explain methodology used to narrow and cull Protected Data for processing and transfer purposes to include only relevant and necessary material (e.g., use of preliminary questionnaires and interviews; use of technology and processes to de-duplicate and apply iterative searches; filter and compile information in a country not subject to transfer restrictions under the applicable Data Protection Laws)
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 attach a copy (e.g., *Model U.S. Federal Court Protective Order* (set forth in Appendix C); 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., internal communications; posted notice)
7. Steps taken to secure transferred Protected Data	Identify steps taken to secure Protected Data (e.g., third-party agreements, nature and type of encryption, password protection, access limitation and control)

The Sedona Conference Cross-Border Data Safeguarding Process + Transfer Protocol	
ACTION ITEM	**INFORMATION**
8. Compliance with notification obligations (if any) to others with oversight of data protection	Identify others involved or who may need to be consulted with responsibility for Data Protection implementation (e.g., the company's data protection officer or works council; government data protection authority); explain their involvement and means of notification
9. Bases upon which Protected Data is transferred	Identify Protected Data transfer mechanisms relied on for each U.S. recipient (e.g., EU/U.S. Privacy Shield Certification, EU Model Contract Clauses, Binding Corporate Rules, or other means of satisfying transfer safeguard requirements)
10. Disposition of transferred Protected Data when no longer needed	Describe disposition of processed and transferred Protected Data (e.g., destruction or return of Protected Data) when no longer needed to fulfill obligations of the specific matter
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 requiring their signed acknowledgement that the steps recorded have been taken