CYBERCOMPLIANCE & ITS IMPACT ON LITIGATION (Discovery)

Primerus Webinar Series
June 2, 2020

Presenters:

Aaron Mutnick
Senior Litigation Attorney
Shelter Insurance
St. Louis, Missouri

Kenneth N. Rashbaum
Partner
Barton, LLC
New York City, New York

J. Paul Zimmerman
Partner
Christian & Small
Birmingham, Alabama

Moderator:

Dale O. Thornsjo
Shareholder
O'Meara, Leer, Wagner & Kohl, P.A.
Minneapolis, Minnesota

CYBERCOMPLIANCE & ITS IMPACT ON LITIGATION (Discovery)

I. INTRODUCTION.

A. You are retained to defend a company that is being sued for a serious injury arising from one of its products. The company has operations and customers across the country, including California, and in Europe. Opposing counsel is seeking discovery on: employees who made decisions about the product design and warnings, information showing alternative designs, prior customer injuries with this product, and customer complaints about the product.

B. Your client wants you to do everything possible to resist production or reduce the scope of production. They are concerned about the exposure in this case, but a bigger concern is that the plaintiff will use discovery in this case to evaluate the potential for a class action. The client has advised that:

1. most of the product design information is stored on servers in Ireland;

2. several official working groups have created project pages on Slack to discuss design decisions;

3. the company knows that most employees are part of a private Facebook group but does not monitor the topics or encourage employees to use that forum for work.

II. WHAT STANDARDS COULD APPLY TO THE DATA THAT IS BEING SOUGHT THAT COULD AID IN CRAFTING AN OBJECTION AND ULTIMATELY RESISTING DISCOVERY?

A. General Data Protection Regulation ("EU GDPR")

1. Three entities are present in all scenarios where personal data is present.

a. Data Subjects: people whose personal data is collected. These are the EU citizens that the law is designed to protect.

b. Data Controllers: those that are doing the actual data collection.

c. Data Processors: organizations that are tasked with processing[1] the information collected.

[1] "Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; available at https://gdpr-info.eu/art-4-gdpr/.

2. The client in this hypothetical can be a controller, and the firm could be both a controller and processor once the firm receives data and passes it along via discovery. However, the jurisdictional scope of the EU GDPR may not apply to the firm. But if the processor becomes a controller they are answerable to the citizens whose private information originated with the lawyer's client.

    a. Article 3 limits the extraterritorial scope of the EU GDPR. Specifically, the EU GDPR will not apply unless (i) the controller or processor is "established" in the EU or (ii) a non-EU controller or processor "targeted" an EU data subject, either with goods and services or through "monitoring" that data subject's activity in the EU. *See* § 27:37 Collecting documents located in foreign countries: Privacy laws, 3 N.Y. Prac., Com. Litig. in New York State Courts § 27:37 (4th ed.)

3. Personal data: "any information relating to an identified or identifiable natural person ('data subject')." Personal data can include names, e-mails, social media posts, IP addresses or other metadata. The GDP also protects information that can be used to infer personal data attributes. *See Id*.

4. The EU GDPR gives EU data subjects legal control and individual redress rights related to access and use of their data anywhere in the world. *See Id*.

5. Key Issues:

    a. Consent. Article 7.

        i. "Explicit custodian/data subject consent continues to be a valid basis for both processing and transferring personal data to the U.S. (The data subject must be informed of the possible risks of such transfers.) In the typical commercial cross-border litigation, the custodian/data subject is an employee of one of the parties. However, changes under the EU GDPR have made it more difficult to rely on consent as a means of obtaining discovery. It is more difficult because consent must be freely given,[2] and, due to the nature of the employer/employee relationship, an employee's consent is deemed inherently coerced. Consent must be clear and distinguishable from other matters and

[2] EU GDPR, Article 7 provides that "when assessing whether consent is freely given, utmost account shall be taken of whether, inter alia, the performance of a contract, including the provision of a service, is conditional on consent to the processing of personal data that is not necessary for the performance of that contract"; available at https://gdpr-info.eu/art-7-gdpr/.

provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.[3] The fact that the data subject can revoke her consent at any point could present challenges in U.S. litigation where documents containing the personal data may already have been produced to the other side, and potentially disseminated to others, at the time consent is revoked. Id.

b. Right to erasure (right to be forgotten). Article 17.

i. if the data subject invoked her right to have her data deleted at a time when her employer reasonably anticipated litigation and she was identified as someone who had relevant documents that should be preserved, questions of spoliation would no doubt abound. The reply, however, may be very simple. Clearly the employer has no control over the data and, given the employee's undeniable (and inalienable) right to have that data deleted upon her request, possession and control would be lacking. *Id*.

3. Exception. Article 49.

i. "The transfer is necessary for the establishment, exercise, or defence of legal claims;" Article 49 1(e).

ii. Compelling Legitimate interest.

- The transfer of personal data to the United States for discovery purposes is permitted where there is a compelling legitimate interest.[4] The following criteria must be met to satisfy this provision:

(i) the one-time transfer of data affects only a limited number of data subjects;

[3] The data subject has the right to: (i) provide approval for the use of their data; (ii) be informed about how their data will be used and for what purpose; (iii) access any of their data that is being used upon request; (iv) revoke consent at any time; (v) have their data returned to them; and (vi) have their data deleted upon request. See EU GDPR, Arts. 12-23, Rights of the data subject, available at https://gdpr-info.eu/rights/.

[4] EU GDPR, Art. 49, Derogations for specific situations, available at https://gdpr-info.eu/art-49-gdpr/.

(ii) the transfer is necessary for compelling legitimate interests to the data transferring entity;

(iii) these interests are not outweighed by the interests or rights and freedoms of data subjects; and

(iv) the transferring entity has assessed all circumstances surrounding the data transfer and has provided suitable safeguards. The open issue here is whether the defense or prosecution of litigation will be deemed a compelling legitimate interest.

Id.

B. State Privacy Laws

1. Every state has a different statutory definition for Personal Information. For example, in Colorado's Co Rev. Stat. 6-1-716

a. Breach: An unauthorized acquisition and access to unencrypted or unredacted computerized data that materially compromises the security, confidentiality or integrity of PI maintained by an entity.

2. Personal Information:

a. An individual Colorado resident's first name or initial and last name in combination with any one or more of the following data elements that relate to the resident, when the data elements are not encrypted, redacted, or secured by any other method rendering the name or the element unreadable or unusable:

i. Social security number;

ii. student, military, or passport identification number;

iii. driver's license number or identification card number;

iv. medical information;

v. health insurance identification number; or

vi. biometric data.

b. A Colorado resident's username or e-mail address, in combination with a password or security questions and answers, that would permit access to an online account.

c. Account number or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

3. Notice: All entities must provide notices to affected individuals in the most expeditious time possible and without unreasonable delay.

4. Exemptions: 1) encrypted or redacted PI; 2) misuse of PI not reasonably likely to occur; (3) entities compliant with Gramm-Leach Bliley Act; (4) any entity regulated notification law of a primary or functional state or federal regulator; (5) any entity that maintains its own notification policy that is consistent with the statute.

5. Penalties/Enforcement: The statute "provides that the 'attorney general may bring an action ... to address violations of this section,' but also provides that the 'provisions of this section are not exclusive.' Col.Rev.Stat. § 6–1–716(4). This permissive language is, as Plaintiffs' argue, at least ambiguous as to whether there is a private right of action under Colorado law. Given the procedural posture of this Motion, which requires the Court to view the law in the light most favorable to Plaintiffs, and absent any authority construing this ambiguity to exclude private rights of action, Plaintiffs' Colorado claim will not be dismissed." *In re Target Corp. Data Sec. Breach Litig.*, 66 F.Supp.3d 1154, 1169 (D. Minn. 2014).

C. Rules of Civil Procedure when analyzed in light of the state or foreign law:

1. Fed. R. Civ. P. 34 and 45:

From The Sedona Conference's Commentary on Federal Rules of Civil Procedure 34 and 45:

a. **"Principle 4:** *Rule 34 and Rule 45 notions of 'possession, custody, or control' should never be construed to override conflicting state or federal privacy or other statutory obligations, including foreign data protection laws.*" (emphasis original). The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control", 17 Sedona Conf. J. 467, 566 (2016).

b. "The mere fact that a party may be deemed to have possession, custody, or control over certain Documents or ESI is not necessarily dispositive of whether the Documents and ESI ultimately can or should be produced. State and federal statutory limitations, privacy laws, or international laws may preclude or

limit disclosure of the kind of Documents or ESI sought. Thus, the possession, custody, or control analysis should also factor in federal and state statutory non-disclosure obligations, along with foreign data protection laws, to ensure that discovery obligations are not inconsistent and do not force non-compliance. This is particularly true when the scope of discovery implicates disclosure of information involving consumers' rights and privacy considerations." *Id*.

2. Fed. R. Civ. P. Rule 26(b)(1):

> (1) *Scope in General*. 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.

3. Fed. R. Civ. P. Rule 26(b)(2)(B):

> (B) *Specific Limitations on Electronically Stored Information*. A party need not provide discovery of electronically stored information from sources that the party identifies as not reasonably accessible because of undue burden or cost. On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.

III. CAN THESE STANDARDS BE USED AS A SHIELD TO AVOID PRODUCTION ALTOGETHER?

A. *Brooks Sports, Inc. v. Anta (China) Co.*, No. 1:17-CV-1458 (LO/TCB), 2018 WL 7488924 (E.D. Va. Nov. 30, 2018):

1. Trademark infringement case brought by Brooks against Anta (a Chinese corporation).

2. "Anta stated that it could not produce the WeChat communications of fourteen of Brooks' requested custodians as they had invoked their privacy

rights under Chinese law. The undersigned will not delve into an analysis of the applicable Chinese law and will assume the custodians lawfully invoked their rights. However, the Court remains very troubled that high-level executives, including Anta's co-founder and Dacheng Peng—the person who was initially identified in Anta's Rule 26(a) disclosures as the only person having information related to this litigation—refused to allow the company to search their WeChats. Their refusal is even more concerning given the evidence before the Court that WeChat is used extensively by Anta employees to conduct business." *Brooks* at *13.

3. "Finally, regarding the WeChat communications, Anta claims that it should not be penalized for the argued legitimate refusal under Chinese law by its employees to allow searches of their WeChat accounts. The Court disagrees. Anta may not avoid penalties for their claimed inability to produce those communications. Anta clearly knowingly allowed its employees to use WeChat for substantive business communications through only their personal accounts and devices. In fact, the sole person identified in Anta's initial disclosures as having knowledge of the facts of the case, Dacheng Peng, refused to allow his WeChat to be search, which the Court finds particularly troubling. Anta should not be able to conveniently use Chinese law to shield production of communications responsive to discovery requests when it could have set up Anta-controlled WeChat accounts for its employees' use which would not have the same issues regarding Chinese privacy laws." *Brooks* at *13.

IV. CAN THESE STANDARDS BE USED TO LIMIT PRODUCTION OR SHIFT COSTS?

A. *Finjan, Inc. v. Zscaler, Inc.*, No. 17-CV-06946-JST (KAW), 2019 WL 618554, (N.D. Cal. Feb. 14, 2019).

1. Plaintiff sought emails of a United Kingdom citizen that contained certain search terms. *Finjan* at *1.

2. Defendant argued that plaintiff's overbroad search terms required the production of unnecessary personal data, and thus was in conflict with the EU GDPR which "limits discovery of personal data to that which is objectively relevant to the issues being litigated." The defendant also argued that anonymizing or redacting the personal data would be very costly. *Id*.

3. The plaintiff maintained that anonymization would impede its review of the emails, and that the defendant could produce the emails for "Attorney's Eyes Only" to satisfy the EU GDPR. *Id*

4. The court resolved the issue by turning to the decades-old Supreme Court decision in *Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court*

for S. Dist. of Iowa, 482 U.S. 522, 107 S.Ct. 2542, 96 L.Ed.2d 461 (1987), where the Court held, as a general rule, that a foreign country's statute precluding disclosure of evidence "do[es] not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute." *Id*

5. The court then applied the five-factor test articulated in *Richmark Corporation v. Timber Falling Consultants*, 959 F.2d 1468, 1475 (9th Cir. 1992), to determine whether the foreign statute excuses noncompliance with the discovery order.[5]

6. Finally, the court added another test: the extent to which the foreign government enforces its laws. The last test was particularly critical, and it weighed heavily in favor of disclosure given that defendant failed to provide any information on the likelihood of enforcement by the United Kingdom. The court ordered the defendant to produce the requested emails in an unredacted form, subject to the existing protective order. *See also* § 27:37 Collecting documents located in foreign countries: Privacy laws, 3 N.Y.Prac., Com. Litig. In New York State Courts § 27:37 (4th ed.).

B. *Corel Software, LLC v. Microsoft Corp.*, No. 2:15-CV-00528-JNP-PMW, 2018 WL 4855268 (D. Utah Oct. 5, 2018):

1. Corel was suing Microsoft for patent infringement for copying WordPerfect's "RealTime Preview" feature. Corel RealTime Preview lets you see how a formatting change will look before applying it to your document, reducing the need to undo and redo unsatisfactory changes. For example, when you use the property bar to change the font and scroll through the list of available fonts, WordPerfect shows you how each font will look. Corel wanted Microsoft's data showing how non-Microsoft entities used Microsoft's allegedly infringing version (this is called telemetry data).

2. Microsoft's Argument against production:

a. "Microsoft admits that it has already produced some Telemetry Data to Corel, but contends that producing all Telemetry Data is infeasible because of its size. Microsoft asserts that locating the

[5] "In determining whether the foreign statute excuses noncompliance with the discovery order, courts consider: (1) the importance of the documents or other information requested to the litigation; (2) the degree of specificity of the request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; and (5) the extent to which noncompliance would undermine important interests of the United States." *Finjan* at *1.

portion of Telemetry Data that relates to the Live Preview feature, which is the feature accused of infringement in this case, is highly burdensome. Microsoft further maintains that retaining Telemetry Data 'raises tension with Microsoft's obligations under the European General Data Protection Regulation 2016/679 ["GDPR"], which regulates (among other things) telemetry data and would require additional burdensome steps to anonymize the data.' For those reasons, Microsoft argues that continued retention and production of Telemetry Data is 'technically challenging and cost prohibitive,' cumulative in nature, unlikely to add any probative value, and disproportional to the needs of this case." *Corel* at *1.

3. Court's Rationale for producing:

   a. First, Telemetry Data … and information regarding its deletion are directly relevant to the claims and defenses in this case …. Specifically, … infringement, damages, and validity. Importantly, Microsoft has not disputed the relevance of either Telemetry Data or information concerning its deletion and, based upon Microsoft's prior production of some Telemetry Data, Microsoft essentially concedes its relevance. *Corel* at *2.

   b. Second, the court concludes that production of Telemetry Data and information about its deletion is proportional to the needs of this case. In reaching that conclusion, the court has weighed the relevant factors set forth in *Rule 26(b)(1)*. The court has determined that the information sought by Corel is important to and will help resolve the issues at stake in this case, as that information is directly relevant to the parties' claims and defenses. The court has also considered Microsoft's resources and has determined that those resources weigh against a finding that production of the information sought by Corel is unduly expensive. Additionally, the court is not persuaded by Microsoft's arguments concerning undue burden. Contrary to those arguments, the court concludes that, for many of the reasons already stated, the benefit of producing the information sought by Corel outweighs the burden and expense imposed upon Microsoft.

   c. The court did not rely on *Société Nationale* or the factors set forth in *Richmark* in its analysis. Rather, the court relied on the proportionality test set forth in Fed. R. Civ. P. 26(b)(1) and ordered retention and production, on the grounds that the benefit of the data, which was relevant and proportional, outweighed the burden or expense of compliance. The court did not specifically address Microsoft's EU GDPR argument, perhaps because Microsoft provided no specifics whatsoever to support its boilerplate claim—

critical information for any court. *See* § 27:37 Collecting documents located in foreign countries: Privacy laws, 3 N.Y. Prac., Com. Litig. In New York State Courts § 27:37 (4th ed.).

C. *In re Hansainvest Hanseatische Inv.-GmbH*, 364 F.Supp.3d 243, 252 (S.D.N.Y. 2018):

1. Hansainvest sought discovery for use in a foreign proceeding pursuant to 28 U.S.C. § 1782.[6] Applicants seek the production of documents via subpoena from Cerberus Capital Management, L.P., J.C. Flowers & Co. LLC, and GoldenTree Asset Management LLP ("Respondents") to use in a contemplated, but as-yet-uninitiated action in Germany against a third party, HSH, regarding alleged violation of German law in connection with the sale of HSH to private investors. *Id.* at 247.

2. Therefore, while the application is granted in its entirety with respect to documents held by U.S. custodians, the Court grants the application with respect to documents held by *foreign* custodians only to the extent that the Hansainvest (1) assume the costs of the document production, including the costs of compliance with the EU GDPR or other applicable European data privacy laws and (2) indemnify Respondents against any potential breaches of European data privacy laws. *Id.* at 252.

V. CASE STUDY: *In re Mercedes-Benz Emissions Litig.*, No. 16-cv-881 (KM) (ESK), 2020 WL 487288 (D.N.J. Jan. 30, 2020):

A. Issue:

Was it error for the Special Masters to order Mercedes to turn over unredacted organizational charts with identities of current and former EU citizens, pursuant to a Discovery Confidentiality Order, in light of Mercedes' EU GDPR obligations and the international comity analysis required by *Société Nationale*. 2020 WL 487288, at *3.

B. Background/Ground Rules:

1. The Special Masters ruling is reviewed on an abuse of discretion standard. *Id.* at *4.

2. The party relying on foreign law has the burden to show the law bars production. *Id.* at *6.

[6] 28 U.S.C. § 1782, Assistance to Foreign and International Tribunals and to Litigants before such Tribunals, provides that "[t]he district court of the district in which a person resides or is found may order him to give his testimony or statement or to produce a document or other thing for use in a proceeding in a foreign or international tribunal."

3. Even where a disclosure would violate a foreign law an American court has the power to order the production. *Id.* at *6.

4. The Court should follow the five factor international comity analysis set forth in *Société Nationale*? *Id.* at *6:

   a. the importance to the litigation of the documents or other information requested;

   b. the degree of specificity of the request;

   c. whether the information originated in the United States;

   d. the availability of alternative means of securing the information; and

   e. the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interest of the state where the information is located.

C. Application:

1. Under the five factor analysis the Court found weighed in favor:

   a. The information was important because it was "directly relevant to Plaintiffs' claims." *Id.* at *6.

   b. The Court used the second factor to claim that it looked at the extent to which the discovery will burden Mercedes because the disclosure is prohibited under foreign law, but the Court never analyzed the requirements of the EU GDPR and the penalties. Instead the Court said that because "business records" would be produced "'in their ordinary form'- in other words, the production of unredacted documents commonly produced in U.S. litigation," that the second factor weighs in favor of production. *Id.* at *7.

   c. The court determined the data did originate in the EU. So the third factor weighed against production. *Id.* at *7.

   d. The Court determined that there is not an alternative means for obtaining current and former employees' names, positions, titles, or professional contact information, and specifically rejected Mercedes' "layered" approach finding that Mercedes "reiterate[ed] the same arguments" and "present[ed] no evidence…that the Special Master abused his discretion in entering the operative Discovery Privacy Order." *Id.* at *7.

e. The Court found that the Special Master properly weighed the interest of the class of US consumers who were claiming they were unlawfully mislead into purchasing certain vehicles against the privacy of EU citizens' private data (that the Court previously stated constituted a "business record") and which would be classified as "Highly Confidential" information pursuant to a Discovery Confidentiality Order. *Id.* at *8.

i. The Court was unmoved by Mercedes' arguments that a violation of the EU GDPR would place Mercedes in legal jeopardy, threaten severe reputation harm, and damage the morale of the workforce. *Id.* at *8

D. Conclusion and Takeaways:

1. The Special Master's international comity analysis was not an abuse of discretion by prohibiting redaction of relevant, responsive documents because it can be designated and protected as "Highly Confidential" pursuant to the Discovery Confidentiality Order and thus ensures that "Plaintiffs obtain the discovery they are entitled to pursuant to the Federal rules of Civil Procedure while protecting EU citizens' private data." *Id.* at *8.

2. The Court pointed out that "not every piece of foreign private data within a document may be relevant, but Plaintiffs are entitled to the basic identifies of individuals so that Plaintiffs can determine relevance." *Id.* at *7.

3. The Court did not address how the EU GDPR penalties were factored into the international comity analysis.

4. "An additional strategy for a European litigant in the United States confronted with discovery requests seeking information and documents that may be protected by European data laws and other protections, such as bank secrecy laws, is to issue a request, such as a letter of request pursuant to The Hague Evidence Convention, to the respective European authorities seeking authorization to produce the information and documents in the litigation in the United States. The European company litigant should insist that the letter of request be submitted to the European authorities by the United States court, and not the party itself, as this will lend greater weight to such a request with the European data protection authorities."

a. § 23:29. Privileges and protections—Data protection and privacy laws, 1 Successful Partnering Between Inside and Outside Counsel § 23:29

5. Courts in the Second Circuit also consider two additional factors:

a. the hardship of compliance on the party or witness from whom discovery is sought; and

b. the good faith of the party resisting discovery. *See Laydon v. Mizuho Bank, Ltd.*, 183 F.Supp.3d 409, 420 (S.D.N.Y. 2016).

VI. THE SEDONA CONFERENCE WORKING GROUP 6 ("WG6") CONSIDERATIONS:

A. The Sedona Conference, Practical In-House Approaches for Cross-Border Discovery & Data Protection, 17 Sedona Conf. J. 397 (2016) (https://thesedonaconference.org/sites/default/files/publications/Practical%20In-House%20Approaches%20for%20Cross-Border%20Discovery%20%26%20Data%20Protection.17TSCJ397.pdf).

Provides "a 'tool kit' for implementing an effective in-house data protection and cross-border discovery process that includes a detailed model corporate policy, a model cross-border discovery management checklist, model Frequently Asked Questions language and a useful infographic for employee and client education, and an exemplar 'heat map' for identifying cross-border data protection issues most relevant to a particular enterprise or project.

Provides eight essential Practice Points:

1. Balance the need for urgency in preserving information with the need to proceed deliberately in countries with comprehensive Data Protection Laws.

2. As early as possible, meet and reach agreements with key stakeholders on a plan that sets expectations regarding legal obligations, roles and responsibilities, and a reasonable timeline.

3. Identify and define privacy issues with opposing parties or regulators through Outside counsel where possible.

4. Set up transparency "checkpoints," beginning with preservation and continuing through the life of the matter, to avoid revocation of consent.

5. Plan a successful in-country collection with detailed surveys of appropriate systems well in advance, and by soliciting support from key stakeholders, both in corporate departments and local business units.

6. Use the processing stage of discovery as an opportunity to balance compliance with both discovery and Data Protection Laws, thereby demonstrating due respect for Data Subjects' privacy rights.

7. During review of data for production and disclosure, parties may consider ways to limit the production of Protected Data; when production of Protected Data is necessary, safeguards can be established to demonstrate due respect for both discovery and Data Protection Laws.

8. To avoid keeping data longer than necessary, counsel should prepare to release legal holds and return or dispose of data promptly upon termination of a matter.

B. The Sedona Conference, Commentary on Rule 34 and Rule 45 "Possession, Custody, or Control", 17 Sedona Conf. J. 467 (2016) (https://thesedonaconference.org/sites/default/files/publications/Commentary%20on%20Rule%2034%20and%20Rule%2045.17TSCJ467.pdf).

"This Commentary is intended to provide practical, uniform, and defensible guidelines regarding when a responding party should be deemed to have "possession, custody, or control" of documents and all forms of electronically stored information (hereafter, collectively referred to as "Documents and ESI") subject to Rule 34 and Rule 45 requests for production."

"A secondary, corollary purpose of this Commentary is to advocate abolishing use of the common-law 'Practical Ability Test' for purposes of determining Rule 34 and Rule 45 'control' of Documents and ESI. Simply stated, this common-law test has led to inequitable situations in which courts have held that a party has Rule 34 'control' of Documents and ESI even though the party did not have the actual ability to obtain the Documents and ESI."[7]

Lists six Principles:

Principle 1: A responding party will be deemed to be in Rule 34 or Rule 45 "possession, custody, or control" of Documents and ESI

[7] This point is discussed in the New York City Bar E-Discovery Working Group February 2020 reissuance of its publication "CROSS-BORDER E-DISCOVERY: NAVIGATING FOREIGN DATA PRIVACY LAWS AND BLOCKING STATUTES IN U.S. LITIGATION" which addresses:

(a) the conflict that New York practitioners face when documents within the scope of a client's discovery obligations reside in a foreign jurisdiction that prohibits transferring those same documents to the United States and
(b) strategies and workflows that will minimize, if not completely overcome, that conflict.

(https://s3.amazonaws.com/documents.nycbar.org/files/2017324-EDiscovery_Working_Group_Memo.pdf).

when that party has actual possession or the legal right to obtain and produce the Documents and ESI on demand.

Principle 2: The party opposing the preservation or production of specifically requested Documents and ESI claimed to be outside its control, generally bears the burden of proving that it does not have actual possession or the legal right to obtain the requested Documents and ESI.

Principle 3(a): When a challenge is raised about whether a responding party has Rule 34 or Rule 45 "possession, custody, or control" over Documents and ESI, the Court should apply modified "business judgment rule" factors that, if met, would allow certain, rebuttable presumptions in favor of the responding party.

Principle 3(b): In order to overcome the presumptions of the modified business judgment rule, the requesting party bears the burden to show that the responding party's decisions concerning the location, format, media, hosting, and access to Documents and ESI lacked a good faith basis and were not reasonably related to the responding party's legitimate business interests.

Principle 4: Rule 34 and Rule 45 notions of "possession, custody, or control" should never be construed to override conflicting state or federal privacy or other statutory obligations, including foreign data protection laws.

Principle 5: If a party responding to a specifically tailored request for Documents or ESI (either prior to or during litigation) does not have actual possession or the legal right to obtain the Documents or ESI that are specifically requested by their adversary because they are in the "possession, custody, or control" of a third party, it should, in a reasonably timely manner, so notify the requesting party to enable the requesting party to obtain the Documents or ESI from the third party. If the responding party so notifies the requesting party, absent extraordinary circumstances, the responding party should not be sanctioned or otherwise held liable for the third party's failure to preserve the Documents or ESI.

C. The Sedona Conference International Principles on Discovery, Disclosure & Data Protection in Civil Litigation (*Transitional Edition*) (January 2017) (https://thesedonaconference.org/publication/International_Litigation_Principles).

Succeeds The Sedona Conference International Principles on Discovery, Disclosure & Data Protection (the "International Litigation Principles") (2011):

> "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."

Takes into consideration:

> the E.U.-U.S. Safe Harbor data transfer framework was invalid in the wake of the Snowden revelations, and a finding that access to and processing of data transferred from EU States to the U.S. was incompatible with the purposes for which the data was transferred (Case C-362/14, Schrems v. Data Protection Comm'r (Ireland), 2015 E.C.R. (October 6, 2015))
>
> New Privacy Shield frameworks;
>
> Countries outside of the E.U. enacting their own Data Protection Laws;
>
> 2015 "Proportionality" Amendments to the Federal Rules of Civil Procedure.

The Six Principles:

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.

Includes:

A Model U.S. Federal Court Protective Order which "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 which "outlines a practical, standardized approach to protecting data at the preservation and collection levels, designed to maximize compliance with applicable laws.

United States District Judge Michael Baylson's (E. D. Pa.) Model U.S. Federal Court Order Addressing Cross-Border ESI Discovery.

Application: *Behrens v. Arconic, Inc.*, 2020 WL 1250956 (E.D. Pa.) (Baylson, J.)

D. The Sedona Conference, International Principles for Addressing Data Protection in Cross-Border Government & Internal Investigations: Principles, Commentary & Best Practices, 19 Sedona Conf. J. 557 (2018) (https://thesedonaconference.org/sites/default/files/publications/International%20Investigations%20Principles%20%282018%29.pdf).

"[P]rovides eight Principles to guide Organizations in planning for and responding to investigations while ensuring that Protected Data is safeguarded at all times against avoidable risks of disclosure":

1. Organizations doing business across international borders, in furtherance of corporate compliance policies, should develop a framework and protocols to identify, locate, process, transfer, or disclose Protected Data across borders in a lawful, efficient, and timely manner in response to Government and Internal Investigations.

2. Data Protection Authorities and other stakeholders should give due regard to an Organization's need to conduct Internal Investigations

for the purposes of regulatory compliance and other legitimate interests affecting corporate governance, and to respond adequately to Government Investigations.

3. Courts and Investigating Authorities should give due regard both to the competing legal obligations, and the costs, risks, and burdens confronting an Organization that must retain and produce information relevant to a legitimate Government Investigation, and the privacy and data protection interests of Data Subjects whose personal data may be implicated in a cross-border investigation.

4. Where the laws and practices of the country conducting an investigation allow it, the Organization should at an early stage of a Government Investigation engage in dialogue with the Investigating Authority concerning the nature and scope of the investigation and any concerns about the need to produce information that is protected by the laws of another nation.

5. Organizations should consider whether and when to consent to exchanges of information among Investigating Authorities of different jurisdictions in parallel investigations to help minimize conflicts among Data Protection Laws.

6. Investigating Authorities should consider whether they can share information about, and coordinate, parallel investigations to expedite their inquiries and avoid, where possible, inconsistent or conflicting results and minimize conflicts with Data Protection Laws.

7. Courts and Data Protection Authorities should give due regard to the interests of a foreign sovereign seeking to investigate potential violations of its domestic laws.

8. A party's conduct in undertaking Internal Investigations and complying with Investigating Authorities' requests or demands should be judged by a court, Investigating Authority, or Data Protection Authority under a standard of good faith and reasonableness.

E. The Sedona Conference, Commentary and Principles on Jurisdictional Conflicts over Transfers of Personal Data Across Borders, 21 Sedona Conf. J. 393 (April 2020) (https://thesedonaconference.org/publication/Commentary_and_Principles_on_Jurisdictional_Conflicts_over_Transfers_of_Personal_Data_Across_Borders).

Commentary goals:

(1) a practical guide to corporations and others who must make day-to-day operational decisions regarding the transfer of data across borders; and

(2) to provide a framework for the analysis of questions regarding the laws applicable to cross-border transfers of personal data.

"[S]ix Principles to guide readers in determining which nation's laws should apply in a given context.

Principle 1: A nation has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, natural persons and organizations in or doing business in its territory, regardless of whether the processing of the relevant personal data takes place within its territory.

Principle 2: A nation usually has nonexclusive jurisdiction over, and may apply its privacy and data protection laws to, the processing of personal data inextricably linked to its territory.

Principle 3: In commercial transactions in which the contracting parties have comparable bargaining power, the informed choice of the parties to a contract should determine the jurisdiction or applicable law with respect to the processing of personal data in connection with the respective commercial transaction, and such choice should be respected so long as it bears a reasonable nexus to the parties and the transaction.

Principle 4: Outside of commercial transactions, where the natural person freely makes a choice, that person's choice of jurisdiction or law should not deprive him or her of protections that would otherwise be applicable to his or her data.

Principle 5: Data in transit ("Data in Transit") from one sovereign nation to another should be subject to the jurisdiction and the laws of the sovereign nation from which the data originated, such that, absent extraordinary circumstances, the data should be treated as if it were still located in its place of origin.

Principle 6: Where personal data located within, or otherwise subject to, the jurisdiction or the laws of a sovereign nation is material to a litigation, investigation, or other legal proceeding within another sovereign nation, such data shall be provided when it is subject to appropriate safeguards that regulate the use, dissemination, and disposition of the data.

VII. SO YOU ARE NOW FAMILIAR WITH THE APPLICABLE LAWS AND LIMITED CASE LAW. WHAT DO YOU DO?

A. Educate your adversary about the laws and constraints.

B. Have your client educate you on the following (possibly with the assistance of a technical expert):

1. Where is the electronic information located?

2. Who are the potential custodians?

3. What are the technical systems that store the data?

4. What data is readily accessible?

5. How much will it cost to search, collect, and review the documents?

6. What is the nature of the data that is due to be protected, and what is involved in redacting or withholding it?

7. What data source or witness might serve as a substitute, based on the circumstances?

VIII. THE COURT HAS ORDERED LIMITED PRODUCTION, SHIFTED THE COST TO YOUR OPPONENT AND GIVEN YOU EVERYTHING YOU'VE WANTED. ARE YOU DONE? WHAT ELSE, AND WHO ELSE DO YOU NEED?

A. From § 27:37 Collecting documents located in foreign countries: Privacy laws, 3 N.Y. Prac., Com. Litig. in New York State Courts § 27:37 (4th ed.)

1. redact personal data where feasible;

2. enter into a protective order with robust provisions that specifically addresses documents subject to privacy laws;

3. process and host the data in the source country if possible; if that is not possible, heavily filter the data in the source country before it is transferred; and

4. document all the steps that were taken to protect the data subject's privacy.

2. Example Solution and Protective Order from *Uniloc 2017 LLC v. Microsoft Corp.*, No. 8:18-CV-02053-AG (JDEx), 2019 WL 451345, at *4–5 (C.D. Cal. Feb. 5, 2019).

a. "Pursuant to the terms of a stipulated protective order, that included data protected by, among other things, the **GDPR**, the parties agreed that

"[u]nless otherwise ordered by the court or permitted in writing by the designating party, a receiving party may disclose any information or item designated 'Protected Data' (only to certain groups of individuals that can receive Highly Confidential—Attorney Eyes Only materials ….)."

b. Excerpt of Protective Order from *Uniloc:*

6. HANDLING OF PROTECTED DATA

6.1 Protected Data. "Protected Data": refers to any information that a party or non-party reasonably believes 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 ("HIPAA") and the regulations thereunder, 45 CFR Part 160 and Subparts A and E of Part 164 (medical information); 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, also known as the General Data Protection Regulation ("GDPR").

6.2 Disclosure of Protected Data. Unless otherwise ordered by the court or permitted in writing by the designating party, a receiving party may disclose any information or item designated "PROTECTED DATA" only to certain groups of individuals that can receive HIGHLY CONFIDENTIAL – ATTORNEY EYES ONLY materials, as indicated in Section 4.3 herein.

6.3 The parties agree that productions of Protected Data Information may require additional safeguards pursuant to Federal, State or foreign statutes, regulations or privacy obligations and will meet and confer to implement these safeguards if and when needed.

IX. AS THE CASE PROGRESSES YOUR CLIENT BECOMES FRUSTRATED BY THE TIME IT HAS TAKEN THEM TO TRACK DOWN RESPONSIVE DATA AND THEIR LACK OF POLICIES AND PROCEDURES FOR RETAINING AND COLLECTING DATA. AT THE CONCLUSION OF THE CASE, YOUR CLIENT ASKS FOR YOUR RECOMMENDATION ABOUT HOW TO BECOME MORE "CYBER" COMPLIANT AND HOW THEY CAN MAKE THE DISCOVERY PROCESS EASIER IN THE FUTURE. WHAT DO YOU SUGGEST?

A. Create a data map.

B. Draft information retention policies.

C. Advise client on the types of insurance products available in the event of a breach.