PRETRIAL PRACTICE & DISCOVERY

Section of Litigation

Summer 2019, Vol. 27 No. 4

August 20, 2019

The Future of U.S. Pretrial Discovery Involving European Union Data after *Salt River*

The Arizona District Court may have provided a blueprint.

By Craig D. Cannon, James J. Hefferan Jr., Katie King, and Virginia D. Ring

The underlying issues addressed in *Salt River Project Agricultural Improvement and Power District v. Trench-France SAS, et al.* are hardly novel, but the Arizona District Court's decision represents a potential watershed moment in U.S. pretrial discovery practice and procedure. 303 F. Supp. 3d 1004 (D. Ariz. 2018). The long-standing tension between the common-law regime of the United States (with broad discovery requirements and little regard for data privacy) and the civil-law traditions of most European countries (with limited or no pretrial discovery and immense deference to individual rights and data privacy) has previously resulted in a long list of court orders that outright reject European Union (EU) data-privacy laws in favor of U.S. discovery laws. As discussed in more detail below, the *Salt River* court, however, may have provided the blueprint for the future of U.S. pretrial discovery that involves the handling of protected EU data. Indeed, *Salt River* promotes the application of a foreign mechanism to US discovery overseen by a foreign discovery master. The implications of potential discovery delays, increased costs, the need to hire local counsel, and more, are far-reaching.

Blocking Statutes Have a History of Blocking Nothing

By the mid-twentieth century, momentum gathered for an international treaty to bridge the pretrial discovery disconnect between the U.S. and EU legal systems. The Hague Convention on Taking of Evidence Abroad followed in 1970, creating formal procedures by which litigants in common-law countries, such as the United States, could obtain evidence located in foreign nations. 20: Convention of 18 March 1970 on the Taking of Evidence Abroad in Civil or Commercial Matters, Hague Conference on Privacy International Law; *see also* Geoffrey Sant, "Court-Ordered Law Breaking," 81 *Brook. L. Rev.* 181, 185 (2015). To ensure that the United States followed the Hague Convention, many nations passed what are commonly referred to as "blocking statutes." Blocking statutes are intended "to prevent

Summer 2019, Vol. 27 No. 4

domestic individuals or corporations from having to comply with US discovery production requests" and generally prohibit "the disclosure, copying, inspection, or removal of documents located in the territory of the enacting state in compliance with orders of foreign authorities." Kristen A. Knapp, "Enforcement of US Electronic Discovery Law Against Foreign Companies: Should US Courts Give Effect to the EU Data Protection Directive?," 10 *Rich. J. Global L. & Bus.* 111, 122 (2010) (quoting *Restatement (Third) of Foreign Relations Law of the US* § 442 n.4 (1987)). Violations of blocking statutes can lead to the imposition of civil and criminal penalties, including fines and imprisonment.

The fears motivating the enactment of blocking statutes appear to be well founded as, notwithstanding the Hague Convention, U.S. courts have routinely asserted the power to demand evidence held by foreign entities through the Federal Rules of Civil Procedure. In *Société Nationale Industrielle Aérospatiale v. US District Court for the Southern District of Iowa*, the U.S. Supreme Court considered whether the Hague Convention constituted the exclusive procedure for obtaining evidence held abroad. 482 US 522, 524 (1987). A bare majority answered this question in the negative, holding that the Hague Convention is not the exclusive procedure or even necessarily the procedure of first resort. Rather, district courts must undertake a particularized international comity analysis to determine whether to resort to the Hague Convention, considering the following factors:

> (1) the importance to the litigation of the documents or other information requested;
>
> (2) the degree of specificity of the request;
>
> (3) whether the information originated in the United States;
>
> (4) the availability of alternative means of securing the information; and
>
> (5) the extent to which noncompliance with the request would undermine important interests of the United States, or compliance with the request would undermine important interests of the state where the information is located.

Id. at 544 n.28. Interestingly, and perhaps foreshadowing the rulings to come, the four dissenting justices described the majority's decision as an affront to foreign nations and worried that the comity analysis envisioned by the majority would be inundated with pro-forum biases. *Id.* at 547–48, 553 (Blackmun, J., dissenting).

PRETRIAL PRACTICE & DISCOVERY

Section of Litigation

Summer 2019, Vol. 27 No. 4

District courts' application of the comity analysis in the years since *Aérospatiale* appears to substantiate the dissent's concerns. Indeed, a 2015 empirical study determined that courts applying the *Aérospatiale* test have found that each of the four subjective factors of the test weigh in favor of U.S. discovery by at least a four-to-one ratio, with two of those factors favoring U.S. discovery by a ten-to-one ratio. *See* Sant, 81 *Brook. L. Rev.* at 191–92. Since 1997, this pro-forum bias has led to a 2,500 percent increase in cases where litigants have asked courts to reject foreign privacy laws as compared to the period from 1987 to 1997. *See*, *e.g.*, *Knight Capital Partners Corp. v. Henkel AG & Co., KGAA*, 290 F. Supp. 3d 681 (E.D. Mich. 2017) (addressing German data-protection statute); *Republic Tech. LLC v. BBK Tobacco & Foods, LLP*, No. 16-3401, 2017 WL 4287205 (N.D. Ill. Sept. 27, 2017) (addressing French blocking statute); *In re Xarelto (Rivaroxaban) Prods. Liab. Litig.,* MDL No. 2592, 2016 WL 3923873 (E.D. La. July 21, 2016) (addressing German data-protection statute); *Laydon v. Mizuho Bank, Ltd.*, *et al*., 183 F. Supp. 3d 409 (S.D.N.Y. 2016) (addressing UK data privacy act).

EU Draws a Line in the Sand

As U.S. litigants have gotten comfortable that they would be successful in obtaining EU-based data with little delay, the EU has been moving toward a more heavy-handed approach. In 1995, the European Parliament and the Council of the European Union adopted the Data Privacy Directive. The objective of the directive was to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data." *See* Council Directive 95/46, on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of Such Data, Art. (1)(1), 1995 O.J. (L 281) 31. To that end, the directive prohibited the transfer of personal data originating within the EU to foreign jurisdictions that lacked adequate data-protection standards. Initially labeled as a jurisdiction lacking adequate data-protection standards, the United States developed a series of data-protection principles and legal transfer mechanisms designed to allow for the free flow of data between the EU and the United States in compliance with EU data-protection laws. As a result, the EU Commission released the "Safe Harbor" decision in 2000, indicating that data transfers could be made to the United States pursuant to the principles. *See* European Court of Justice 2000/520/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC. Following the Safe Harbor decision, personal data was generally allowed to be transferred from the EU to the United States for a period of 15 years pursuant to the Safe

Summer 2019, Vol. 27 No. 4

Harbor principles, which were regulated and enforced by the U.S. Federal Trade Commission.

However, in part due to U.S. district courts regularly ignoring EU data-protection laws in U.S. litigation matters, the Safe Harbor program was largely ineffective in ensuring that EU data-protection laws were enforced when EU personal data was transferred to the United States. The ineffectiveness of the Safe Harbor framework eventually resulted in the European Court of Justice overturning the Safe Harbor decision in the landmark *Schrems v. Data Protection Commissioner* decision. *See* (C-362/14) EU:C:2015:650 (06 October 2015). On the heels of the *Schrems* decision, the EU has doubled down on its efforts to ensure U.S. compliance with EU data-protection laws by: (1) aggressively insisting that the United States develop new data-protection principles that are actually enforced (the "Privacy Shield" framework) (*see* Commission Implementing Decision (EU) 2016/1250 of 12 July 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-US Privacy Shield (notified under document C(2016) 4176)); and (2) implementing the General Data Protection Regulation (GDPR), which supersedes the directive.

The GDPR regulates the processing by an individual, a company, or an organization of personal data relating to individuals in the EU. It defines "personal data" broadly to include any information relating to an identified or identifiable natural living person. GDPR, Article 4(1). More specifically, "personal data" includes a wide range of information such as a name, home address, email address, driver's license or passport number, internet protocol (IP) address, cookie ID, phone number, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

In U.S. litigation, "data processing" is something wholly different than it is elsewhere. Generally, U.S. litigators consider "data processing" to be the process by which raw, native data is made useable, typically by e-discovery software. In contrast, "data processing" under the GDPR covers a wide range of operations performed on personal data, including: preservation, collection, organization, storage, alteration, use, dissemination, erasure, or destruction. GDPR, Article 4(2). And the penalty for violating the GDPR? In addition to compensation to any person who has suffered material or non-material damage as a result of an infringement of the GDPR (GDPR, Article 82), companies are now faced with an administrative fine of up to 20 million euros or four percent of gross turnover (whichever

Summer 2019, Vol. 27 No. 4

is larger) for failing to comply with EU privacy and cross-border data-transfer standards. GDPR, Article 83.

Back to *Salt River*

With the GDPR set to go live just a few months later, *Salt River* threw up a warning shot against what appears to have been extreme favoritism toward U.S. litigants. In *Salt River*, the plaintiff, Salt River Project (SRP), sought discovery from both a French corporation, Trench-France, S.A.S., and a Canadian corporation, Trench Limited. 303 F. Supp. 3d at 1005. The suit was subject to the Mandatory Initial Discovery Pilot (MIDP) project that requires parties to produce documents or electronically stored information (ESI) that "may be relevant to any party's claims or defenses." Trench-France asserted that this requirement obligated it to produce documents and ESI maintained in France, which would violate the French Blocking Statute if produced outside of the Hague Convention procedures.

Remarkably, the court accepted Trench-France's argument that production of documents and ESI required by the MIDP would violate French law and conducted the "particularized analysis" set forth in *Aérospatiale*. The court analyzed the *Aérospatiale* factors and ultimately found that the application of every single factor weighed in favor of requiring the parties to use the Hague Convention procedures.

In weighing national interests, the court found that France expressed an "emphatic" sovereign interest in controlling foreign access to information within its borders by enacting the Blocking Statute. Conversely, U.S. interests in vindicating the rights of the plaintiffs and preserving fairness in litigation would not be impaired by using Hague procedures because Trench-France had agreed to expedited production procedures. Trench-France also successfully argued the potential criminal penalties under the French Blocking Statute were severe.

In making its findings, the court made a precedent-shattering move away from U.S. courts' usual requirement that parties comply with U.S. discovery despite a blocking statute or similar barrier. In addition, the ruling hints that the court was aware of the EU's increased focus on enforcing its data-protection laws and was looking to shield the parties from potential EU monetary and criminal penalties. Indeed, there is a real possibility that *Salt River* may eventually become the seminal case relied on by parties and litigators when they

Summer 2019, Vol. 27 No. 4

wish to avoid conducting discovery in the United States and foreign data-protection and/or privacy laws are implicated.

The Hague Convention Procedures from *Salt River*

In its motion for protective order and to appoint commissioner for discovery in France and for issuance of request for international judicial assistance under Chapter II of the Hague Convention (filed February 21, 2018), Trench-France contended that under the Hague Convention, the following events would occur:

1. The court would appoint a French attorney to oversee discovery in France, pending the approval of the French Ministère de la Justice, to (a) receive from Trench-France documents and ESI that are produced in this action and (b) transmit those documents and ESI to counsel for the parties;
2. The court would issue a formal request to the French Ministère de la Justice to appoint the specified French attorney as the commissioner and authorize the commissioner to collect documents and ESI from Trench-France; and
3. Upon approval of the request by the French Ministère de la Justice, the commissioner would arrange to receive documents and ESI from Trench-France in France, and then transmit that material to SRP and the other parties.

Trench-France was prepared to facilitate the procedure and bear the associated costs. It also believed it could produce documents under this procedure without substantial delay to the existing discovery schedule and without any substantive limitation on the scope of documents it would otherwise produce.

In issuing its order, the *Salt River* court ignored that SRP would be required to hire a French attorney, increasing its costs, and that the use of the Hague procedures, despite Trench-France's contentions, would very likely delay the litigation. *Salt River* was settled by the parties in March 2018 (and dismissed in May 2018) so we are left without any further guidance on whether the Hague procedures really are as efficient as Trench-France claimed.

Best Practices for U.S. Litigants Following *Salt River*

Now that following Hague Convention procedures is a viable possibility for U.S. litigants, what do we do both as litigators and as a profession?

Summer 2019, Vol. 27 No. 4

As litigators, we should:

- become familiar with the GDPR (and its restrictions on the transfer of personal data), the *Aérospatiale* factors and the blocking statutes that may prevent the transfer of EU data altogether;
- be prepared to hire local counsel if the Hague Convention procedures end up being used;
- plan on incurring increased costs and delays if a private commissioner (or discovery master) is appointed;
- consider narrowing the focus of discovery to avoid addressing EU data-privacy laws altogether, if possible; and
- discuss all of these issues and potential complications with clients when EU data is in play.

As a profession, we should seek clarification on the *Aérospatiale* factors. As discussed in an amicus brief filed by some of the country's leading e-discovery practitioners and professors in the *US v. Microsoft* Supreme Court matter (584 US __ (2018)), the judiciary needs to provide further guidance on the appropriate considerations of international comity to be weighed when dealing with a cross-border discovery dispute, as originally set forth in *Aérospatiale*. Unfortunately, the *US v. Microsoft* matter was dismissed as moot prior to any further clarity being provided. Absent further guidance, the *Aérospatiale* factors will remain as they are and the *Salt River* analysis may become the new norm. The ensuing added time and cost that will surely result will not likely be welcomed by U.S. litigants or U.S. courts. Indeed, these are the precise problems formerly inherent in U.S. discovery that the revised Federal Rules of Civil Procedure sought to fix.

Craig D. Cannon is a partner and e-discovery team leader; James J. Hefferan Jr. is senior e-discovery attorney; Katie King is e-discovery of counsel; and Virginia D. Ring is senior e-discovery attorney at Kilpatrick Townsend & Stockton LLP.