An Update on GDPR and Discovery

Matt Borick
Downs Rachlin Martin PLLC
June 6, 2019

You may recall from last year's TDLA Annual Meeting that I presented on the General Data Protection Regulation (GDPR), a mandatory and comprehensive privacy regulation passed by the European Parliament and Council of the European Union that became effective May 25, 2018. One of the issues discussed was how the GDPR might affect discovery in U.S. litigation in view of the regulation's many restrictions on the processing and transfer of personal data, as well as data subjects' rights regarding their personal data.

Up to now, the prevailing view on this issue has been driven by the U.S. Supreme Court's language in *Societe Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for So. Dist. of Iowa*, 482 U.S. 522, 544 n. 29 (1987), in which the Court observed that "[t]he French 'blocking statute,' . . . does not alter our conclusion. It is well settled that such statutes do 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." The Court also quoted the Reporter's Notes from the Restatement of Foreign Relations Law of the United States (Revised) § 437: "[W]hen a state has jurisdiction to prescribe and its courts have jurisdiction to adjudicate, adjudication should (subject to generally applicable rules of evidence) take place on the basis of the best information available. . . . [Blocking] statutes that frustrate this goal need not be given the same deference by courts of the United States as substantive rules of law at variance with the law of the United States."

Other factors have also contributed to the limited deference U.S. courts have given to foreign laws and directives protecting the disclosure of information, including that prosecutions and other enforcement actions under such laws and directives historically have been rare. But the GDPR is backed by a much stronger policy and purpose, and also has much bigger "teeth." For that reason, some

commentators have theorized that the GDPR might shift the prevailing view in U.S. courts.

The GDPR's impact was tested earlier this year in the case of *Finjan, Inc. Zscaler, Inc.*, 2019 WL 618554 (N.D. Cal. Feb. 14, 2019), a patent infringement case filed in the U.S. District Court for the Northern District of California. Among the key witnesses in the case was a U.K. citizen who had previously directed plaintiff's U.K. sales and subsequently began working as the director of defendant's U.K. sales. Plaintiff sought production of the witness's e-mails, but defendant resisted on the grounds that the production would violate the GDPR. Specifically, defendant contended that the production would include personal data covered by the GDPR that would need to be anonymized at great expense. Plaintiff objected to anonymization because it would have impeded the review of the emails, and argued that defendant could comply with the GDPR by producing the emails as "Attorney's Eyes Only" under the parties' existing protective order.

The court in *Finjan* found that the GDPR did not preclude it from ordering production of the emails in their unredacted form under the existing protective order, and therefore ordered defendant to produce them. The court applied a number of factors in reaching its decision:

- Importance of the information requested to the litigation. Here, the emails were directly relevant to several issues in the case. Defendant argued that the emails could be duplicative of information available from domestic custodians, but had not actually verified that.

- Degree of specificity of the request. The court found that plaintiff's request was appropriately limited to critical terms.

- Whether the information originated in the United States. The court did not address this factor specifically, but rather observed that although the witness was in the U.K., defendant was an American company subject to American discovery law.

- Availability of alternative means of securing the information. The court considered whether a "substantially equivalent alternative" existed, but found none. Again, defendant had not done a search of the witness's emails nor verified that the same information would be provided from domestic custodians. The court also observed that redacted documents were not substantially equivalent to unredacted documents, given the relevance of the redacted information.

- Extent to which noncompliance would undermine important interests of the United States. The court described this as the most important factor. Here, the court concluded that the "strong American interest in protecting American patents" outweighed the U.K.'s interest in protecting the privacy of its citizens, particularly because there was a protective order in place under which documents could be marked as highly confidential. The court also observed that because the emails were directly relevant, their production "would appear to not violate the GDPR."

- Extent and nature of the hardship that inconsistent enforcement would impose upon the person, and extent to which enforcement by action of either state can reasonably be expected to achieve compliance with the rule prescribed by the state. The court again pointed out that the production would not necessarily violate the GDPR. The court also observed that defendant had not provided any information on the extent or likelihood of enforcement.

As *Finjan* makes clear, the facts and circumstances are critical to determining the extent to which the GDPR might affect discovery in U.S. courts. The court's decision in *Finjan* certainly could have come out differently had defendant been able to make certain showings, such as the availability of alternative information that served the same purpose as the U.K. emails. At bottom, the GDPR is still very new, and thus whether other courts come out the same way on GDPR issues remains to be seen.