Vol. 44 No. 3 Spring 2018

Litigation

American Bar Association

The Journal of the Section of Litigation

Sacred Cows

A Modest Proposal to Address the Costs of the Attorney-Client Privilege

Top 10 Mistakes in Internal Investigation Reports

Nine Tips That Help Junior Associates Become Successful

iWitness

GDPR AND OVERCOMING CHALLENGES TO OBTAINING DIGITAL DISCOVERY FROM EUROPEAN ENTITIES

YURI MIKULKA

The author is a partner at Manatt, Phelps & Phillips, Costa Mesa, California, and is an associate editor of LITIGATION.

You are an associate in a law firm in New York assigned to a breach of contract case involving a winery client headquartered in Bordeaux, France. You are assigned to collect your client's emails and data to respond to your adversary's request for production of documents in the case, which is pending in a New York federal court. You have 30 days to respond and produce documents. You figure you will start collecting documents via email and produce them electronically. Is it that simple? Not at all.

Even setting aside the recently implemented General Data Protection Regulation 2016/679 (GDPR), the challenges of obtaining litigation-related data from European companies are many. They range from differences in cultural norms to differences in the legal system and privacy laws between the United States and Europe that limit what can be collected and transferred to the United States. At the very least, you can expect resistance from your French client, who will consider the request to be unnecessarily intrusive. Even if cooperative, your client may get into serious trouble by producing and transferring data in a manner that violates European privacy laws, which are ever-evolving. This article describes those challenges and offers tips for obtaining digital discovery from European companies.

One challenge is that European companies will resist producing data because discovery is an entirely different concept in Europe. In the United States, litigants are required to produce any non-privileged material that is relevant to any party's claim or defense and proportional to the needs of the case. In contrast, most states in the European Union (EU) operate under a civil law legal system in which pretrial discovery is not common. Hence, European clients may be baffled by your request that they search through and download years of emails and data on dozens of topics to produce for a case thousands of miles away.

A second challenge is that your ability to collect and transfer data for U.S. litigation will be limited because EU privacy laws largely restrict digital discovery. Under EU law, entities may not transfer personal data to countries deemed to have lower privacy standards, such as the United States, unless they have legal contracts in place or have permission from the person whose data are at issue. On May 25, 2018, the EU's GDPR went into effect to replace the old European Council Directive 95/46. The GDPR provides a more unified law directly binding all 28 EU member states. Among other things, a company's failure to comply with this regulation could lead to fines of as much as 4 percent of a company's global annual revenue. The GDPR also contains new provisions addressing litigation-related international data transfers, including the transfer of personal data from the EU to the United States for use in discovery. The provisions include, among other things, a 72-hour data breach reporting requirement and a new requirement that a data controller show consent with "clear affirmative action" before processing data. Despite these obstacles, a U.S. court may order the European entity to produce emails and data located in Europe or face discovery and evidentiary sanctions.

What is our associate to do under the circumstances? The following nine-step plan is a place to start.

Step 1. Remind the opposing counsel and court. If you are representing a European company, it is best to alert the opposing counsel and disclose this issue in a Federal Rule of Civil Procedure Rule 26 report and discovery plan at the outset of the case. This way, no one is surprised about the extra hurdles in obtaining discovery. If you are adverse to a European company, it is best to narrow the scope of your requests to avoid seeking discovery that may be deemed personal data and

to leave plenty of time to obtain data and seek judicial relief as necessary.

Step 2. Get your client's buy-in. Many European companies unaccustomed to U.S.-style discovery will be reluctant to comply with your request to produce emails and digital data. Therefore, invest in obtaining their understanding and collaboration at the outset, and provide concrete examples of potential adverse consequences should they fail to comply.

Step 3. Assess the legitimacy of the discovery request. Determine whether you can justifiably challenge the document request. Is it proportional to the needs of the case as required by the amended Federal Rules of Civil Procedure? Conduct diligence on what systems, agreements, and practice your client has in place, to demonstrate the burdensome nature of the production.

> European companies will resist producing data because discovery is an entirely different concept in Europe.

Step 4. Identify the nature of the data. Does the information requested involve "personal" data? While Americans typically think of personal data as being limited to health information, financial data, or Social Security numbers, the term "personal data" is more broadly defined in Europe, encompassing any information relating to an identified or identifiable natural person ("data subject"). An identifiable person is "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. . . ." Council Directive 95/46/EC, art. 2(a). This can even include an email address if it can be used to identify the person's name, location, occupation, gender, a physical factor, and/or health-related data.

Step 5. Confirm the rules. In addition to being mindful of the most recent EU directives, it is important to confirm the rules, laws, and protocols for the specific country where the data are based. Consider engaging local counsel to help you navigate the laws and rules of the particular European country involved.

Step 6. Devise a strategy to comply. Determine whether there are safe harbor schemes, standard contractual clauses to facilitate data transfer, or binding corporate rules in place, some of which are discussed below.

- **Binding corporate rules (BCRs).** BCRs are internal policies and enforcement mechanisms that have been formally "approved" by European data protection authorities, which a company can voluntarily create and adopt. The corporation may then freely transfer data within its own corporate entities subject to the terms of the BCRs.
- **Model contract clauses.** Entities can enter into a data transfer contract that includes model clauses approved by the European Commission. While this option is not a quick fix, it can be more appealing when the transfer of data is between two related entities (e.g., a European subsidiary with a U.S. parent).
- **Safe harbor scheme.** Consider the safe harbor scheme between the U.S. Department of Commerce and the European Commission. It allows U.S. corporations that are subject to the jurisdiction of the Federal Trade Commission or the Department of Transportation to receive data from the EU if they are publicly listed on the safe harbor list and voluntarily adhere to seven specified safe harbor privacy principles: (1) notice, (2) choice, (3) onward transfer (i.e., data transfer to third parties), (4) access, (5) security, (6) data integrity, and (7) enforcement. (For additional details on the seven principles, see U.S.–EU Safe Harbor Overview, https://build.export.gov/main/safeharbor/eu/eg_main_018476.)

Step 7. Streamline. Streamline the data by filtering out any unnecessary personal information. Then strategically employ redaction, pseudonyms, and anonymization of information negotiated with your opposing counsel. You can explain to opposing counsel that this step will help manage the scope and breadth of discovery to be proportional to the need, as required by the amended Federal Rules.

Step 8. Protect the transferred data. Once the data from your European client are transferred to the United States, make sure the data are adequately protected, i.e., that the client complies with the BCRs or model contract clauses described in step 6. Ensure that the protective order you negotiate addresses any additional protection you need.

Step 9. Log it. Log and memorialize each step of the process to prepare for future inquiries from adversaries, the court, or government entities.

Our New York associate will no doubt face insurmountable challenges in meeting the 30-day deadline to produce and will likely need to seek an extension or file a motion for a protective order to properly protect the client's data. While technology makes it easier than ever to collect and transfer digital data from our clients, privacy laws and cultural norms in Europe make it harder than ever to collect data from European companies. Therefore, it's important to consider the above factors at the inception of the case to try to minimize the hurdles of conducting discovery when working with European companies. ■