CROSS-BORDER E-DISCOVERY IN THE PRIVACY ERA

Brian L. Bank Rivkin Radler LLP

A practical overview of relevant considerations for companies engaging in e-discovery collection and production from foreign offices for use in U.S. litigation

In today's global economy, it is not uncommon for U.S. litigation to include either foreign parties or domestic parties with offices abroad. When U.S. litigation counsel is tasked with representing such a party in domestic litigation, counsel must consider how to preserve, collect, transfer, and produce documents and data belonging to foreign custodians and/or maintained on foreign soil. As foreign data privacy laws and other foreign laws addressing document and data disclosure become more commonplace and more diverse, and the penalties for noncompliance become more severe, U.S. litigation counsel must be sure to keep their eyes on the big picture, carefully balancing the liberal scope of discovery applicable in most U.S. jurisdictions with controlling foreign restrictions on document and data preservation, collection, and transfer. In most instances, U.S. litigation counsel will need to plan early, oftentimes at the outset of litigation or even before, in order to ensure that a proper balance is struck. This article presents a high-level overview of what U.S. litigation counsel should consider in striking this balance.

ASSESS THE NEED FOR CROSS-BORDER DISCOVERY EARLY

As an initial matter, in order to properly plan for cross-border discovery, U.S. litigation counsel must determine early on in their assignment (i) whether the case will potentially require a need to preserve, collect, and produce documents and data either belonging to a foreign custodian or maintained and/or backed up in a foreign country, and, if so, (ii) which of the foreign laws (as well as any corporate document and data disclosure policies) may apply to the preservation, collection, and transfer of such documents and data, and the requirements thereof.

While custodian identification should be a familiar process for U.S. litigation counsel, the need to conduct this analysis early in the proceeding becomes all-the-

more critical in situations potentially requiring cross-border discovery. This is in order to ensure that the party can identify and consider which foreign laws may apply and what they require. While some foreign data privacy laws are well-covered in U.S. legal circles, such as the European Union's ("EU") General Data Privacy Regulation ("GDPR"), others – including local data privacy laws enacted by EU members and other countries that, in certain instances, impose more stringent requirements than the GDPR – are less-known. Furthermore, some countries also have blocking statutes and other laws (such as telecom or bank secrecy laws) that also impose restrictions on document and data transfer that must be considered and addressed when formulating a game plan. Thus, it is important for U.S. litigation counsel to identify precisely which foreign laws apply before engaging in efforts to collect and transfer custodial data housed in a foreign jurisdiction.

The importance of conducting this assessment early on in a litigation assignment cannot be overstated, as some foreign laws, such as the GDPR, apply not just to the collection and transfer of documents and data, but also to their preservation. When coupled with the standard for document preservation typical in most U.S. jurisdictions, this means that a party's obligation to comply with foreign data privacy requirements may arise as soon as the prospect of litigation becomes reasonably foreseeable. Since document and data preservation is generally one of the earliest tasks a party must undertake, it is critical for U.S. litigation counsel to understand whether and how foreign laws may impact the party's performance of this important obligation, and to incorporate any foreign data privacy requirements into their preservation plan.

ACKNOWLEDGE WHAT YOU DON'T KNOW

Given the potential complexities in tracking and interpreting foreign laws that may impact document and data preservation, collection, and transfer, in most instances it is strongly advisable (and in some cases required) for U.S. litigation counsel to engage local counsel and/or a local e-discovery vendor to assist in identifying and ensuring compliance with all such applicable laws. In addition, to the extent that the party has a data privacy officer, U.S. litigation counsel should also consult that individual. These experts can be crucial to aiding U.S. litigation counsel in determining: (i) which foreign laws apply to relevant documents and data; (ii) whether there is a legal basis to preserve, collect, and transfer such documents and data to the United States for use in litigation; (iii) the restrictions, if any, that apply to the format and timing of any such transfer; (iv) whether a data transfer agreement or other documentation is required and what must be included therein; and (v) how to document the preservation, collection, and transfer process for potential use by U.S. litigation counsel in the proceeding.

STRIKING A BALANCE BETWEEN FOREIGN DATA PRIVACY LAWS AND U.S. DISCOVERY OBLIGATIONS

Of course, complying with foreign data privacy law is only half the battle. Once U.S. litigation counsel, with the aid of local experts, has identified the requisite steps to preserve, collect, and transfer documents and data to the United States for use in litigation under applicable foreign data privacy laws, counsel must then consider how best to balance those requirements against the party's discovery obligations in the litigation. This includes assessing the relevance of the documents and data to the claims and defenses of the action, and, depending on the state or federal jurisdiction, whether they are proportional to the needs of the case. In this regard, U.S. litigation counsel will often be well-served (and depending upon the controlling procedural rules, may be required) to raise cross-border data privacy concerns and requirements with the court and opposing counsel early in the proceeding, thus proactively managing expectations and framing the forthcoming meet-and-confer dialogue.

DOCUMENT YOUR EFFORTS

U.S. litigation counsel should also be sure to identify and comply with documentation requirements for cross-border transfer. Depending on the applicable data privacy law, this could include sign-off by all data controllers and processors to a contractual arrangement in which the receiving controllers and processors contractually bind themselves to the data privacy obligations of the foreign custodian. This may also require certification by either the party or local counsel that the party complied with all applicable data privacy requirements and/or that the documents to be transferred have been properly sanitized of non-essential personal information.

Full compliance with the documentation requirements set forth in applicable foreign laws not only protects the party, but it also serves to highlight any obligations assumed by U.S. litigation counsel vis-à-vis the protection and use of the documents and data post-transfer.

EARLY PLANNING CAN REDUCE HEADACHES

Given the potential complexities in identifying and complying with foreign data privacy laws and other foreign laws addressing document and data disclosure, and the tension between the limitations imposed by such laws and the relatively liberal disclosure standards common in U.S. jurisdictions, U.S. litigation counsel should be prepared to carefully consider how best to manage the discovery process to minimize potential exposure under foreign laws. This could include, among other things: (i) exploring whether the party maintains the same or substantially similar documents and data through a domestic custodian or on a domestic server or back-up system; (ii) reducing the volume of documents and data for transfer through the use of analytics and other technology-assisted review tools; (iii) conducting a responsiveness review pre-transfer, thus reducing the overall volume of documents and data for transfer; (iv) using anonymization and/or redactions to sanitize non-essential personal data from documents and data identified for transfer; and (v) carefully negotiating the scope of discovery with opposing counsel to ensure that the party need only transfer those documents that are truly relevant to the claims and defenses of the action.

CONCLUSION

U.S. litigation counsel engaging in cross-border discovery must carefully consider the data privacy obligations imposed by the laws of the foreign jurisdiction in which the custodian resides and/or where such documents are maintained and/or backed up. In doing so, counsel must strike a balance between the requirements imposed by such foreign laws and the liberal discovery obligations common to U.S. laws. This can often be a complex and expensive proposition, but a necessary one considering the sometimes harsh penalties for non-compliance under certain foreign data privacy laws. As such, U.S. litigation counsel should plan early and enlist local counsel and other experts to ensure that the party's interests are protected both in the foreign jurisdiction and in the pending litigation matter.

Brian L. Bank is a partner in the Commercial Litigation; Employment & Labor; Compliance, Investigations & White Collar; and Privacy, Data & Cyber Law practice groups at Rivkin Radler LLP in Uniondale, New York.