GlobalCo’s general counsel, Erica Lee, closed the door and stopped to think about how to share her concern with her team. Since GlobalCo’s IPO in the United States, Lee had faced down every legal challenge, but this one caused her a dread she had never before experienced. A whistleblower told the SEC that GlobalCo salespeople in some of the company’s European, Latin American and Asian sales offices were bribing public officials to obtain government contracts after lavish parties and evenings of entertainment.

The assembled legal team in the conference room fell silent as Lee faced them. “I need to tell you something, and it’s not going to be pleasant,” she began. “The SEC is threatening to bring a civil enforcement action against us in federal court.”

The discussion turned towards the whistleblower’s allegations of corruption on a widespread scale. GlobalCo had already begun an internal investigation of the claims, but an enforcement action meant discovery. And discovery involves facing the challenges of cross-border discovery conflicting with information governance limitations.

The Sedona Conference calls it a “catch-22.” Once a suit is filed and discovery begins, GlobalCo will have an obligation to gather and review relevant evidence from its worldwide offices and produce responsive, non-privileged information to the government in its civil enforcement action. At the same time, however, privacy laws and so-called “blocking statutes” may prohibit responding to that discovery. GlobalCo may face civil and even criminal sanctions for complying with its discovery obligations in the enforcement action.

The cross-border catch-22
Here is how the catch-22 might work. The government serves requests for production of documents to GlobalCo seeking, among other things, documents relating to the entertainment, accounting records, and internal communications about the efforts to court public officials and obtain government contracts. GlobalCo might object to these requests, saying that they are prohibited by local law from responding to the requests because of blocking statutes in certain countries that restrict the disclosure of information for use in foreign legal proceedings. France is an example of a country with blocking statute. The government, in turn, might file a motion to compel production of the information.

When faced with such a motion to compel, federal courts commonly grant relief to the requesting party. Yet, GlobalCo local counsel could be prosecuted for providing information to trial counsel in the United States. One question that comes up is whether there is a realistic likelihood of an actual prosecution of local counsel for assisting in a discovery response. A US court may be skeptical about the actual likelihood of prosecution under a foreign blocking statute. On the other hand, GlobalCo could point to at least one actual prosecution under a foreign blocking statute.

In addition to blocking statutes, GlobalCo will have to overcome local privacy laws, which may strictly limit the cross-border transfer of personal data. In GlobalCo’s case, a government request for production about bribery and entertainment may involve personal data about payments, including payment card information, and perhaps even special categories of sensitive personal data that raise heightened scrutiny. Accordingly, in the case of data in the European Union, absent an exception, US Department of Commerce Safe Harbor protection, the proper contractual clauses in an agreement, or binding corporate rules,
GlobalCo would be barred from transferring responsive documents outside the European Union. GlobalCo could argue that collecting and reviewing the data is necessary for compliance with a legal obligation to which it is subject, and that transferring the data to the United States is “necessary” and legally required for the defense of its legal claims, which are exceptions to limitations in the EU Directive. The ability to use this defense will depend on the interpretation of “necessary” and whether additional safeguards are necessary to prevent onward transfer of the information or data breaches.

Similar defenses exist under privacy laws to justify the collection of information in Japan and Korea. These laws arguably permit use and disclosure, notwithstanding the fact that the data subject has not provided prior consent. In particular, GlobalCo could justify use of personal information collected in Japan for discovery purposes by saying the use and disclosure are based on and necessary pursuant to laws and regulations. Likewise, in Korea, GlobalCo could point to provisions of its privacy laws permitting uses where necessary to attain the justifiable interests of GlobalCo that are explicitly superior to the data subjects. Also, GlobalCo could justify disclosure of personal information for discovery purposes because it is necessary for a court to proceed with a case. Again, however, the success of these defenses would depend on how a local court would interpret the term “necessary.”

Local counsel can help GlobalCo identify these catch-22s. In addition, local counsel will be useful in identifying possible applicable exceptions to laws restricting transfer of information and negotiations with data protection authorities. Ultimately, however, there may be unavoidable conflicts.

Sedona Conference suggestions
In 2008, the Sedona Conference wrote a paper covering the catch-22 of cross-border discovery and offering some suggestions for
a responding party to both US discovery requests backed by the sanctions power of the courts, and foreign blocking statutes and privacy restrictions. Among other things the Sedona Conference suggested was a dialogue among “all concerned parties” to resolve the conflicts using “communication and collaboration” to “seek a way forward in good faith.” The Sedona Conference hoped courts would be able to balance a number of factors to achieve a fair resolution of discovery disputes, including the nature of privacy obligations, the importance of the information sought to resolving issues in the case, and the burden of producing the information. From the perspective of the litigants, the Sedona Conference cited the example of pharmaceutical company Eli Lilly, involved in a similar dilemma. Eli Lilly started talking with European data protection authorities to cover, among other things, pre-filtering personal data collected from EU countries to ensure that only relevant information is transferred, creating a special designation for EU Confidential data, and including provisions in protective orders in US courts to enforce additional privacy and security procedural safeguards.

Despite laying out what it thought of as a way forward to resolve cross-border discovery issues, the Sedona Conference cited a number of continuing, urgent issues. One of these challenges is “ensuring that the amount of personal data collected and the extent of its use in litigation is proportional to the actual issues in legitimate controversy.” It cited two other related concerns: ensuring the integrity and security of collected personal data, and preventing the unauthorized onward transfer and use of personal data. The question then arises as to whether technology advances since 2008 help a litigant minimize the risk of information governance liability when responding to discovery in US federal or state courts. We believe the answer is yes.

Technology to mitigate liability

How can a litigant narrow and reduce the amount of information it needs to gather from foreign countries? In 2008, technology included keyword searching, concept clustering, de-duplication and e-mail chain analysis. These techniques helped reduce the volume of data gathered, but were limited in effectiveness. Literature and case law on keyword searching, for instance, notes that it can produce more “junk” than responsive documents and, therefore, may not narrow the universe of potentially responsive documents effectively.

Enter technology-assisted review (TAR), also known sometimes as computer-assisted review or predictive coding. TAR involves software “that uses sophisticated algorithms to enable the technology to determine relevance, based on interaction with (i.e., training by) a human reviewer.” Reviews using TAR involve the creation of a seed (random sample) set of known relevant documents, which are inputted into the software. Reviewers then conduct a number of training rounds in which the computer tries to code documents and human reviewers provide feedback to ensure the computer is learning what is relevant. Once sufficient training occurs, the computer can be used to review the remaining documents in the universe in an automated fashion.

TAR is an important new technology increasingly used in domestic discovery practice to find responsive documents among a universe of documents, or to conduct a privilege review. TAR can narrow down the universe of potentially responsive documents in a much more effective way at significantly lower cost. If GlobalCo uses TAR in countries with blocking statutes or privacy restrictions, it can enter into a dialogue with data protection authorities armed with a means of making a real difference in culling down the universe of documents. Consequently, TAR may help GlobalCo give data protection authorities the comfort they need to comfortably permit the gathering of information for purposes of responding to discovery in the United States.
The second cross-border challenge mentioned above is ensuring the security of collected personal data, and preventing the unauthorized onward transfer and use of personal data. Another technology advance since the Sedona Conference Framework is the increasingly common use of digital rights management systems. Using digital rights management, a business like GlobalCo can use technical safeguards focusing on control of the information to enforce restrictions on use and sharing of information under protective orders to a business’s own internal security practices. For instance, certain services would allow GlobalCo to provide file access only to certain users; limit the ability for users to copy, print or forward files; revoke access to a file; set expiration dates on access to files; and create an audit trail showing who did what actions to a file, and when. The ability to control information can follow files even if they leave GlobalCo’s network or a user’s device.

If GlobalCo uses digital rights management systems when collecting personal data in countries with blocking statues or privacy restrictions, it can point to its systems in negotiations with data protection authorities. Digital rights management supplements the procedural controls of special coding, data segregation and protections in protective orders. It would enable GlobalCo to enforce these procedural controls, and associated audit controls could hold personnel accountable if they were to violate procedural restrictions. Such technology would help GlobalCo reassure data protection authorities that it is maximizing the protection of personal data.

Use available tools
GlobalCo’s legal team faces a cross-border discovery challenge of collecting information from its foreign offices, some of which may be in jurisdictions that block the transfer of data for use in US court proceedings, or GlobalCo’s ability to protect the privacy of personal data. There is no easy answer to these conflicts, but technology-assisted review and digital rights management technology provide GlobalCo with additional tools for negotiations with local data protection authorities. These tools would help GlobalCo to argue that it is minimizing the information it needs to gather from respective countries, and maximizing the protections it offers to the information once it reaches the United States.

For more information, visit www.ubicna.com, or contact UBIC at 877-321-8242 or by email at info@ubicna.com.

NOTES
2 French Penal Code Law No. 80-538 (French blocking statute prohibiting “requesting, seeking or disclosing in writing, orally or in any other form, documents or information of an economic, commercial, industrial, financial or technical nature for the purposes of constituting evidence in view of foreign judicial or administrative proceedings”).
5 In re Advocat “Christopher X” Appeal No. n 07-83228 (Cour de Cassation, French Supreme Court Dec. 12, 2007).
7 Binding corporate rules are codes of conduct to handle the cross-border transfer of personal data.
8 See EU Directive, supra, art. 7(c).
9 Id., art. 26, sec. 1(d).
10 See Sedona Conference Framework, supra, at 12.
12 Korean PIPA, supra, art. 15(1)(6).
13 Id., art. 18(2)(B).
14 Id. at 1, 27 (describing the catch-22).
15 Id. at 30.
16 See id. at 29.
17 See id. at 28.
18 Id. at 23.
19 See id.
21 Id. at 29.
22 See id.
USING TECHNOLOGY TO MINIMIZE INFORMATION GOVERNANCE LIABILITY DURING CROSS-BORDER DISCOVERY AND INVESTIGATIONS