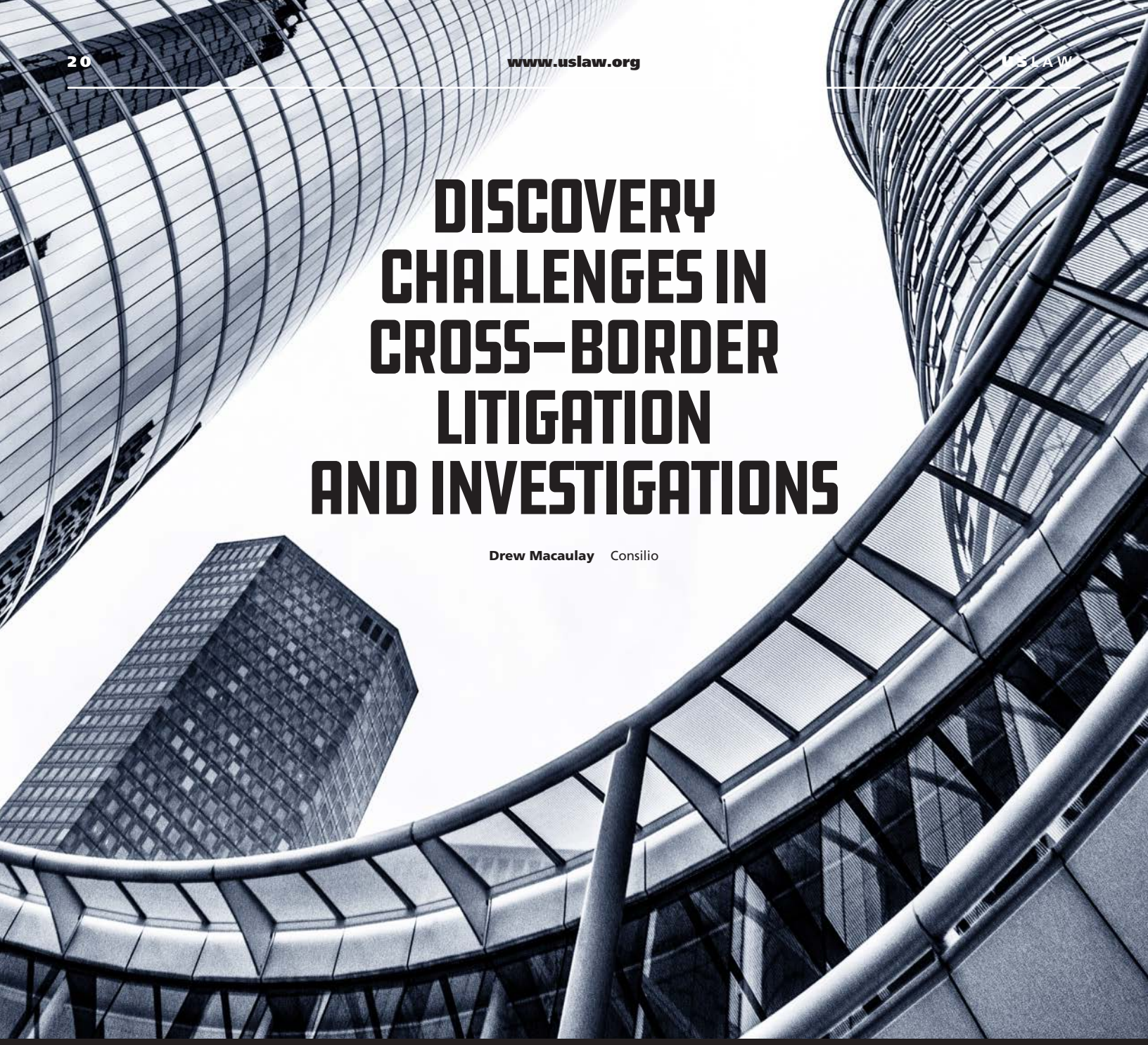

DISCOVERY CHALLENGES IN CROSS-BORDER LITIGATION AND INVESTIGATIONS

Drew Macaulay Consilio

INTRODUCTION

The need for multinational corporations to gather and review documents from different jurisdictions for investigation and litigation purposes is not a new phenomenon, but the associated challenges continue to intensify. Corporations that operate across borders must be ready to overcome a variety of legal, logistical and linguistic hurdles, and all too often in circumstances where time is tight, and budgets stretched

BETWEEN A ROCK AND A HARD PLACE

Legal challenges to conducting discovery exercises overseas include personal data privacy, banking secrecy, "blocking" statutes and state secrets legislation. Of these, data protection legislation is the most commonly encountered issue, where the data that the company needs to collect, review and produce originates in a jurisdiction where the rights of the data subject (most often an employee) are protected in relation to data that identifies them. Again, this is not a new challenge, but one where the risks of non-compliance have dramatically increased in Europe with the introduction of the General Data Protection Regulation and its associated fines based on a percentage of global turnover.

It is not only personal data privacy that causes delays and additional cost in cross-border discovery exercises. In some jurisdictions, notably Switzerland and Singapore, legislation has been enacted to enforce the protection of data concerning legal entities such as corporations. Depending on the jurisdiction, this can include information about the company's customers and other third parties and as such, names, signatures, bank account details and contact information (for example, email addresses or telephone numbers) may also be deemed private and protected from disclosure.

In addition, corporations with overseas subsidiaries are expected to provide discovery even when the act of doing so may conflict with a local blocking statute, such as the French Blocking Statute of 1968 (as amended in 1980). In the case of France, the criminal sanctions for contraventions of the Blocking Statute are significant but

are rarely enforced, so while the chance of a fine or imprisonment is low it remains a difficult decision to make for a corporation when a U.S. court expects discovery of documents originating in France.

In each of these contexts, conflicts arise because the ability of the company to collect and transfer data to another jurisdiction are limited by law, even though there are pressing legal reasons to follow that course of action. When these legal restrictions are raised as an objection to providing discovery from a particular jurisdiction, U.S. courts are frequently unsympathetic, and will often decide that the interests of the U.S. justice system override any risks borne by the company providing documents.

Corporations undertaking cross-border discovery exercises will find that deadline pressures can be exacerbated by delays while they take advice from data privacy counsel, the company's data protection officer or, in certain situations, negotiate with a works council. If it is subsequently decided that the data cannot leave its country or region of origin to be processed elsewhere then a corporation will normally have to contract with a local service provider for eDiscovery services and potentially document review. Under GDPR, the contracting process for engaging a supplier to which data is going to be transferred would need to include creating a Data Processing Agreement, a Record of Data Processing and reviewing the potential supplier's "Technical and Organizational Measures" to ensure that data that moves to the provider is adequately protected both contractually and from unauthorized access. Finally, while it is not always necessary, transfers of documents containing personal data outside the EU frequently necessitate redactions of that personal data. All of the above points lead to an increase in overall cost and the time required to complete the exercise which can be in short supply during an investigation or litigation.

LOGISTICS AND LINGUISTICS

It is not just legal restrictions on movement of data that stand in the way of a company trying to comply with U.S. discovery obligations that involve overseas data. The discovery process requires the cooperation of a range of stakeholder groups, including corporate IT, internal and external counsel, data protection officers, information security teams, eDiscovery specialists and others.

Where an exercise involves data across a number of countries and time zones the coordination of each of these groups becomes much more challenging, particularly since members of the project team (such as local IT staff) may be unfamiliar with discovery processes and/or may not speak English as their native language, increasing the chance of key information being lost in translation and mistakes being made.

Staying with the languages theme, the existence of documents in multiple languages in the data to be collected, searched, reviewed and produced will add further complexity to an already challenging process. While the "lingua franca" of many U.S. corporations is English, it remains normal to see collected data in non-English speaking countries contain many different languages. While processing software has evolved to the point where searches can be run in almost any language, choosing the words to search for remains a challenge. It is not simply a matter of translating specific search terms in English into a range of target languages as in many cases a literal translation will not accurately retrieve potentially relevant documents (for example "backhander" in English could mean a blow with the back of the hand, an uncomplimentary remark or a bribe).

Picking the right translation for the specific context requires a more sophisticated approach, in which linguistic and legal experts collaborate to define the best search strategy to retrieve documents of interest. Again, this process adds time and expense to the overall budget. Once potentially relevant non-English documents have been identified, sourcing lawyers proficient in each language to review them can be a final challenge.

PLANNING IS EVERYTHING

Corporations that regularly come up against these issues will usually have a defined set of processes for discovery exercises. Often termed a "playbook," this document will guide project stakeholders through the company's preferred workflows for identifying, preserving, collecting, processing, hosting, reviewing and producing documents. Where particular jurisdictions present a challenge for data privacy reasons, the playbook can include company policies, arrived at through consultation with privacy counsel, that define how personal data will be treated in each jurisdiction. This may include determinations of whether or not consent is to be sought (and it is not always necessary or advisable to do so) as well as the processes which the legal team and any external service provider will follow to minimize the impact of the exercise on the rights of the data subject, such as in-country processing, hosting and review or agreed measures for filtering and redaction of personal or sensitive personal data. In situations where banking secrecy is an issue, similar approaches to managing personal data can be used, but it is worth noting that the redaction stage can be even more extensive (and therefore time consuming and costly) than simple personal data redactions.

The playbook will usually be distributed to key personnel across the enterprise as well as "go-to" outside counsel in the relevant jurisdictions. Follow-up training sessions can help to ensure that concerns are addressed and those who are unfamiliar with the eDiscovery process have a chance to learn and ask questions in a less pressured situation than a live project. In this way, the playbook and associated rollout training sessions ensure that all participants have a common understanding of approved project workflow and their role within the process as well as any interdependencies that may exist between stakeholders' roles.

The playbook will also normally contain contact details for key members of staff in different departments and jurisdictions at the corporation, facilitating project start up, communication and ongoing management. It may also extend to include contact details for the corporation's approved service providers for data collection, eDiscovery processing and hosting, translation services and document review.

CONCLUSION

With increasing globalization and the focus of data protection authorities on ensuring data subjects' rights in relation to their data are enforced, the challenges of cross-border eDiscovery will continue to intensify over time. Corporations that invest the time in building internal processes and procedures to respond to these challenges will be able to significantly reduce the risk and cost involved in handling these exercises, as well as increasing the speed with which they can respond. An effective global discovery playbook will guide project stakeholders through the options for data collection, processing, hosting and review, ensuring that best practices adopted by the corporation are used consistently on a global basis or adapted for a specific jurisdiction where necessary.

Drew Macaulay is a managing director at Consilio in London, where he advises the firm's global clients on the technical and workflow aspects of large scale regulatory and internal investigations and litigation disclosure exercises, as well as compliance with the relevant privacy legislation and procedural rules.