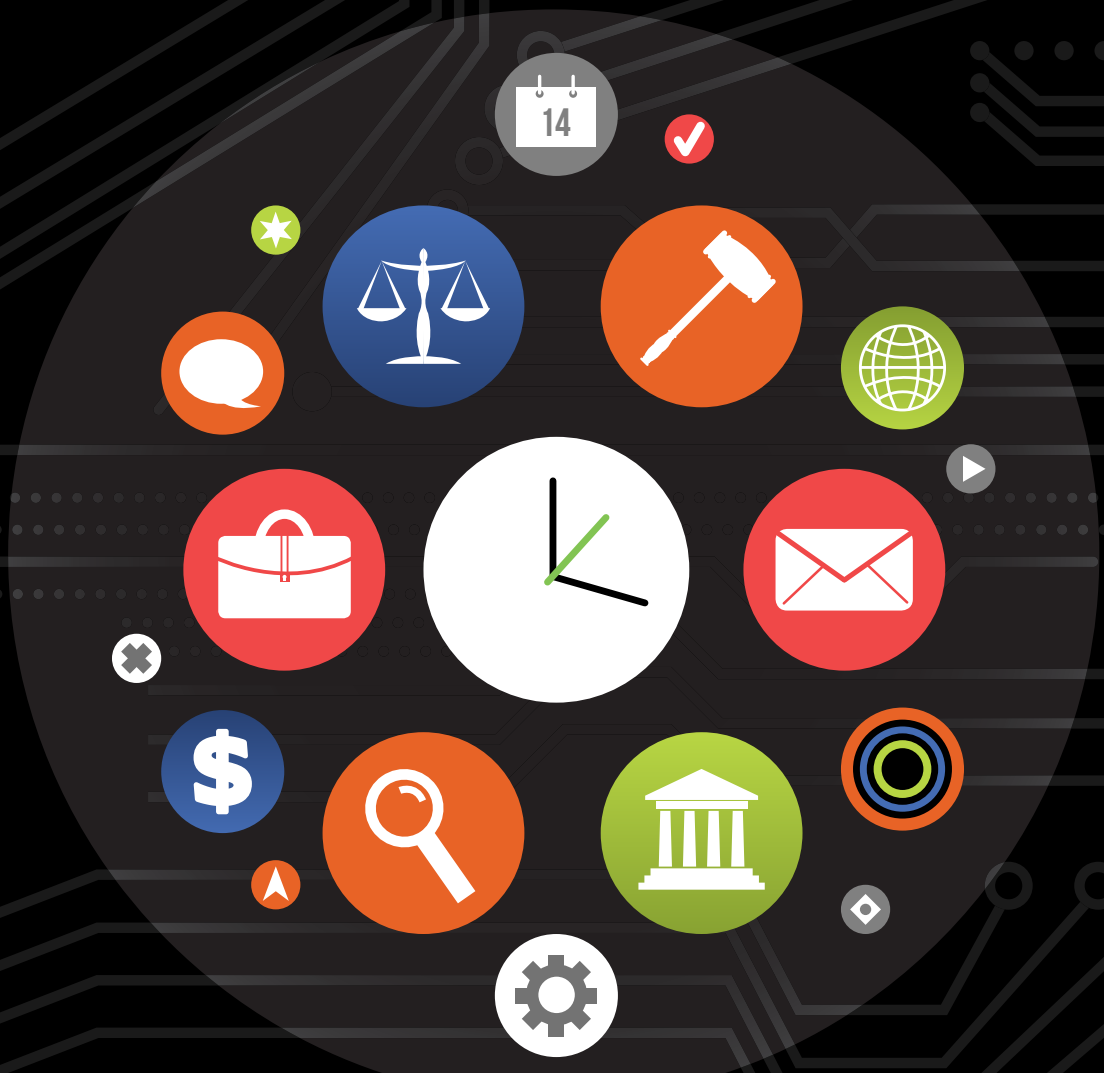
- 2016 -

LEGAL TECHNOLOGY UPDATE



Law Bulletin Publishing Company
Supplement to the Chicago Daily Law Bulletin®

CHICAGOLAWBULLETIN.COM

CROSS-BORDER E-DISCOVERY:

Using Intelligent Workflows and Emerging Technology to Navigate Conflicting U.S. and Foreign Data Obligations

By Daniel Meyers, Esq.
President of Information Governance at TransPerfect Legal Solutions

Over a decade has passed since Judge Shira Scheindlin issued the first of her Zubulake decisions, ushering into common legal parlance the phenomenon known as "e-discovery." Since that time, the domestic e-discovery market has matured into a streamlined, quasi-commoditized industry. Cross-border e-discovery, however, remains a confusing bed of thorns for many law firms, corporations and e-discovery service providers alike.

Comprehensive U.S. discovery obligations often conflict with foreign data privacy and information security laws, resulting in seemingly irreconcilable priorities when confronting transnational litigations and investigations. The intersection of these contrasting legal regimes often results in expensive motion practice, significant litigation delays, and inadvertent breaches of foreign law. Fortunately, advances in technology and intelligent processing workflows empower practitioners to significantly ameliorate these pain points. This article takes a high-level view at how proactive planning and cutting-edge technology helps to remain compliant while meeting the needs of each case.

Plan Early, Plan Carefully

At the onset of a dispute, most attorneys—whether in-house or outside counsel—typically react with a narrow focus on the merits. What are the claims and defenses? What's the exposure? How do I begin witness interviews?

Continued on page 14

Continued from page 12

In the digital age, however, early merits planning simply is not enough. Both federal and state rules of procedure require that promptly after the pleadings are filed, discovery meet-and-confers and court conferences occur. These conferences are not only an attorney's first and best opportunity to raise issues concerning the discovery of electronically stored information ("ESI") —they are the legally required time to do so under the rules of civil procedure. Compliance with this requirement is particularly important when relevant ESI exists in a foreign jurisdiction whose laws can block or significantly delay U.S. discovery.

The failure to raise such issues in a timely manner can have drastic consequences. In a recent decision out of Nevada, Jacobs v. Las Vegas Sands, et al, Index No. 10-A-627691 (Dist. Ct. Clark Co., March 6, 2015), substantial sanctions were imposed against one of the defendants in connection with its efforts to navigate the data privacy laws of Macau. In the decision, the court went out of its way to chastise counsel for failing to raise such data privacy laws or their impact on discovery during the parties' Rule 16 meet-and-confers or in the joint stipulation on discovery resulting therefrom.

The lesson from Las Vegas Sands is that counsel and its client must identify any foreign sources of potentially relevant ESI at the earliest stages of a dispute. To the extent that the foreign jurisdiction in which such ESI resides has a privacy statute or other regulation prohibiting the transfer of that data to the U.S., counsel should identify a workaround promptly (using the techniques described below) and proactively raise the impacts of those workarounds with its adversary and with the court.

Amongst other issues that should be raised—and ultimately addressed in the resulting discovery stipulation and/or court order—are the following.

- A rolling production schedule to buy time for the foreign ESI to proceed through the necessary approval and/or processing workflow.
- Confidentiality and information security provisions, including permission to file documents with personal information under seal and provisions governing how the receiving party will protect personal data. Such provisions will prove invaluable when seeking the approval of data subjects, foreign regulators, and Works Councils to transfer the relevant ESI to the U.S.
- Agreements on the use of redactions to anonymize personal data in order to mitigate the impact of foreign privacy laws.

Choose the Right Service Provider

In the domestic e-discovery market, it is often difficult to differentiate service providers. Pricing is highly standardized across the industry and most vendors offer the same software platforms, so decisions often come down to subjective personal preferences, rather than competitive pricing or qualitative differences in technology features.

By contrast, the differences between service providers in the cross-border e-discovery market are not only objective but material. While the 1995 EU Data Protection Directive (Directive 95/46/EC), for example, prohibits the transfer of personal data from an EU member state to the U.S., it does not prohibit such transfer to another EU member state or to any other foreign country that provides an "adequate level of protection." Thus, vendors that offer processing facilities in jurisdictions providing an adequate level of protection (e.g., England) can offer immediate solutions.

Even better, service providers that can go to the client's foreign data centers/facilities and establish a temporary, on-premises EDRM environment offer the ability to collect, process, host, review, and redact documents in-country in full compliance with applicable privacy laws.

Lastly, look for a vendor with data privacy consulting expertise. In the complex and nuanced intersection of U.S. and foreign legal obligations, your service provider should be your partner and trusted advisor, not merely a resource to execute tasks on command.

Use Emerging Technology

Finally, take advantage of cutting edge technology that can be introduced into the e-discovery workflow to effect a streamlined, cost-efficient process. For example, regular expression scripting software empowers you to automate searches for personal information within the data set. Once identified, such data can be set aside for a separate privacy review, redaction, or approval from data subjects or foreign regulators. Meanwhile, the remainder of the data set that did not "hit" on the personal data script can be transferred immediately to the U.S. for a traditional e-discovery workflow and rolling production.

Emerging technologies also facilitate the automated redaction of certain types of personal information. This results in a far more efficient and reliable privacy review. Through redaction, the data set can be anonymized of personal information rendering it outside the scope of foreign privacy law altogether.

Navigating foreign prohibitions on the transfer of ESI can be daunting in the face of broad U.S. discovery obligations. The use of intelligent workflows and technology is not only wise, but necessary to avoid running afoul of U.S. courts and foreign regulators.

Daniel Meyers, Esq., is the President of Information Governance at TransPerfect Legal Solutions. Prior to joining TransPerfect, Dan was a litigation Partner at the law firm formerly known as Bracewell & Giuliani LLP. Dan also formed and Chaired Bracewell's E-Discovery & Information Governance practice group. Dan is a certified privacy professional by the IAPP and a certified e-discovery expert by ACEDS.