doi:10.1017/amp.2023.2

TRANSNATIONAL DISCOVERY OF E-EVIDENCE: IS THERE A BEST PRACTICE?

This panel was convened at 3:30 p.m. on Friday, April 8, 2022, by its moderator Rekha Rangachari of New York International Arbitration Center, and Carrie Shu Shang of California State Polytechnic University, Pomona, who introduced the speakers: Vivian Curran of University of Pittsburg School of Law; and Megan Crowley of Covington & Burling LLP.

Remarks by Carrie Shu Shang

Increasingly, issues are arising regarding transnational access to evidence in electronic formats in dispute resolution proceedings. Currently, there is not a comprehensive solution to cross-border gathering of electronic stored information and regulations in the area remain a patchwork of divergent instruments. Over the past few years, private practitioners and in-house counsel have had to familiarize themselves with various discovery rules, data privacy laws, and data localization laws to ensure that they transfer data in ways that are compliant with strict cross-border data transfer requirements. Further, the current private international law framework seems outdated for the rapidly changing transnational e-evidence discovery needs. This Panel, organized by the ASIL Private International Law Interest Group (PILIG), addressed issues concerning cross-border conflicts of e-evidence in party-managed processes and whether there is a "best practice" for adjudicators and parties to co-develop such a protocol. As the Co-Chair of PILIG, I had the pleasure of moderating the Panel.

I. The Problem

To identify the problem, it needs to be recognized that the conflict between U.S. and foreign laws in areas of cross-border e-discovery is real. First of all, discovery in U.S. federal courts is usually much broader in scope than in other countries and is primarily conducted and controlled by parties, rather than by judges. This is in contrast with civil law countries that generally allow little or no pretrial discovery. Most civil law systems require heightened specificity in discovery requests while U.S. courts usually issue discovery requests that utilize broad language. Since *Société Nationale Industrielle Aérospatiale v. U.S. District Court*, U.S. courts have largely concluded that foreign restrictions for taking discovery (e.g., the Hague Convention) and data privacy laws do not displace the Federal Rules of Civil Procedure (FRCP), rendering many substantive conflicts unavoidable.

However, foreign data privacy statutes are on the rise in recent years. These emerging foreign privacy and data protection laws impose restrictions on the collection, review, and dissemination of various forms of "personal data." In many foreign laws, personal data is defined broadly enough to include business emails with identifiable email addresses—one of the most voluminous forms of e-discovery. At the same time, the number of data localization measures has roughly doubled in the past five years. Localization can result either from explicit legal rules or *de facto* rules, by making cross-border data transfers more complicated, expensive, and uncertain. The General Data

Protection Regulation in EU law could be considered as a type of localization statute.[1] China, a rising power, for instance, has also enacted several blocking statutes, such as its Cybersecurity Law (effective June 1, 2017), which imposes data protection and cybersecurity obligations for all "network operators."[2] Over the past four years, China has issued several regulations and national standards to implement high-level requirements stipulated in the law. The Data Security Law (effective September 1, 2021) focuses on regulating data from a national security perspective and emphasizes protection of "important data."[3] The newly enacted Personal Information Protection Law (effective November 1, 2021) is the first comprehensive law regulating personal information protection in China and personal data that may travel across Chinee borders. These three pieces of legislation together will form the future regulatory framework for data governance in China, but other laws and sectoral rules (like the Encryption Law, sectoral requirements in the financial and healthcare sectors) have also emerged to make data compliance in China increasingly more complex.

This conflict between U.S. and foreign laws has created high economic stakes for litigating parties. In the United States, a court may bar or limit the use of wrongfully obtained electronic evidence. Another court may impose sanctions if one does not comply with discovery obligations. Violations of the U.S. Stored Communications Act may result in criminal or civil liability. In foreign jurisdictions, businesses could face potentially enormous fines for violations of data privacy laws. Parties located in China, for example, cannot sit for depositions that will be used in foreign proceedings, or else these parties may face prosecution in China pursuant to the new Anti-Foreign Sanctions Law.[4] In addition, the large amount of electronically stored information adds to the burdens imposed on litigants. Nowadays, businesses generate staggering amounts of electronic data—including emails, presentations, reports, accounting records, and spreadsheets. Responding to e-discovery requests accurately and completely can be very time-consuming and require substantial resources. The complexities of cross-border e-discovery, particularly when it implicates cloud computing, are enormous and evolving rapidly. Some of the problems are caused by a lack of clarity in exiting jurisdictional rules. Data accessed in one jurisdiction may be housed on servers in another country (and therefore subject to data privacy laws in another country). The increasing amount of data is subject to concurrent jurisdictions. So far, current private international law framework has not offered effective solutions for the rapidly changing transnational e-evidence discovery needs.

II. "Best Practices"

Based on the problems identified above, attorneys should immediately identify possible issues by conducting early case assessments that address cross-border data collection and production. For example, lawyers need to make sure that they understand where custodians are located/reside, where data is located, stored, and backed up, and what the applicable foreign data protection laws are. Attorneys should also consider whether notification or approval of a data privacy request is required in respective jurisdictions. The answers to those questions often depend upon the local

[1] General Data Protection Regulation, Regulation (EU) 2016/679, Art. 44.

[2] Wangluo Anquan Fa (网络安全法) [Cybersecurity Law], Art. 21 (promulgated by the Standing Comm. Nat'l People's Cong. Nov. 7, 2016; effective June 1, 2017).

[3] Shuju Anquan Fa (数据安全法) [Data Security Law], Arts. 21, 27, 30 (promulgated by the Standing Comm. Nat'l People's Cong. June 10, 2021; effective Sept. 1, 2021).

[4] Fan Waiguo Zhicai Fa (反外国制裁法) [Anti Foreign Sanctions Law], Art. 14 (promulgated by the Standing Comm. Nat'l People's Cong. June 1, 2021; effective June 1, 2021).

https://doi.org/10.1017/amp.2023.2 Published online by Cambridge University Press

data protection law and certain other factors, including the mechanism chosen for the transfer, numbers of transfers (single or repeated), and the amount of data.

Early engagement of in-house counsel (in multiple jurisdictions) is also necessary. Outside counsel should educate themselves on how their serviced corporations are structured (operations, and how parents, subsidiaries, and related companies interact) to determine whether data is in their possession, custody, or control. They should also educate relevant attorneys at companies regarding obligations, red flags, and/or decision points, such as whether a legal hold should be put in place with regard to custodians and data categories, and the relevant time frames. Attorneys also need to remember to destroy their copies of data or return it at the end of matters, and to lift the legal hold.

Engagement with opposing counsel in a timely manner is also becoming more necessary. Opposing teams should meet early to negotiate cross-border discovery protocols, which may include phased discovery. For example, parties may agree to review U.S. production requests first. Afterward, parties may be able to agree whether further production from non-U.S. custodians is unnecessary, or can be limited. Counsels should build in additional time for cross-border requests, and should limit the number of countries they will collect from as well as the scope of foreign collection. If protected, attorneys should work together to consider safeguards to limit production, such as producing data in anonymized or redacted forms. Attorneys should also meet to negotiate confidentiality agreements, which can limit the number of people allowed to view the protected data, and impose immediate destruction requirements on protected data. They may also choose to include information security provisions in confidentiality agreements, and to have such agreements or protocols memorialized in a court order.

In early stages, attorneys should assist courts in understanding the relevant discovery issues (e.g., via expert affidavits) and in creating reasonable discovery plans. Attorneys can: conduct responsiveness and privilege reviews abroad; consider whether home country custodians can provide identical/similar documents; consider whether documents are hosted in a home country; and consider the use of artificial intelligence tools to filter out privileged information; etc. They should also consult with local privacy counsel, outside e-discovery counsel, and technology vendors to consider additional available review options and to ensure such options are technologically feasible and compliant with local data privacy regulations.

III. The Explosive Use of 27 USC § 1782

As a side matter, the use of 28 U.S. Code § 1782 in connection with foreign legal proceedings has exploded in cross-border e-discovery. Usage of this statute starts with filing a request with the federal district court where the discovery target is located. That request is usually entertained and granted with minimal judicial activity and on an *ex parte* basis. The target of the request is then subpoenaed and ordered to produce discovery according to the scope and practices of the FRCP. By relying on Section 1782, the foreign opposing party and the foreign tribunal might never know that one side of the case was built using different discovery practices than those governing the remainder of the dispute.

In accordance with the Supreme Court's 2004 decision in *Intel Corp v. Advanced Micro Devices, Inc.*, discovery needs not be discoverable abroad for it to be discoverable under Section 1782. Generally, requests made under Section 1782 have a high grant rate, but there are still fractures in lower courts' implementation of the statute. Courts of Appeal disagree on whether the statute can be used to compel discovery in aid of foreign commercial arbitrations.[5] There is also a split in

[5] The Circuit split has since been resolved in the consolidated decision of *ZF v. Luxshare* and *AlixPartners v. Fund for Protection of Investors' Rights in Foreign States*, where the U.S. Supreme Court held that judicial assistance afforded under 27 USC § 1782 was not to be extended to foreign commercial arbitration proceedings. ZF Automotive US, Inc. v. Luxshare, Ltd. (argued Mar. 23, 2022, opinion delivered June 13, 2022).

https://doi.org/10.1017/amp.2023.2 Published online by Cambridge University Press

lower courts regarding whether Section 1782 can be used to compel documents physically located abroad but under the possession, custody, or control of a U.S. entity. Due to the lack of input from foreign tribunals and foreign opposing parties in Section 1782 proceedings, and the open-ended nature of these factors, numerous district courts have evolved simplified tests that lead to reflexive grants of foreign discovery requests.

This Panel presented a wonderful summary of timely issues rising in conflict-of-laws and practical difficulties concerning cross-border e-discovery. Looking forward, neither our Panel nor this Article could address all of these important questions in depth. But raising them is a first step to designing better transnational e-discovery and data transfer in light of rising privacy statutes in the future.

https://doi.org/10.1017/amp.2023.2 Published online by Cambridge University Press