



Vol. 1, No. 11

E-Discovery Basics: Cross-Border E-Discovery

This is one in a series of brief introductory guides to practical issues in electronic discovery. To subscribe to future installments of E-Discovery Basics, if you have not already done so, please [click here](#).

In previous installments of E-Discovery Basics, we discussed each of the stages in the e-discovery life cycle—starting with litigation preparedness, legal holds and preservation, and proceeding to processing, review, production, admissibility and presentation of electronically stored information (“ESI”). Here, we discuss issues that may arise when ESI relevant to U.S. proceedings is located in foreign jurisdictions.

When litigation and investigations involve cross-border discovery—*e.g.*, discovery in a U.S. proceeding of information located in non-U.S. jurisdictions—additional legal and logistical challenges emerge, especially where the jurisdiction has a strong data privacy framework. In many non-U.S. jurisdictions, including European Union (“EU”) member states, some Asian nations, and a few Latin American nations, data privacy is viewed as a fundamental right and personal data is afforded greater protection than we are accustomed to in the U.S. Many non-U.S. jurisdictions have enacted, or are in the process of enacting, comprehensive data privacy legislation.

As an example, EU member states have established requirements for how private information can be collected, processed and transferred. Each EU member state has the obligation to enact national legislation that is consistent with the principles of the Treaty of Lisbon and the Data Protection Directive 95/46/EC (the “EU Directive”). The EU standards place a variety of obligations on those who control and process data. Generally, data may freely transfer only to nations with “adequate protections” ensuring protection of personal information. Only a handful of non-EU nations, such as Australia, Canada, and Switzerland—which have data privacy requirements and enforcement mechanisms similar to those of the EU—have been deemed to have “adequate protections.” In the case of Switzerland, its data privacy standards are, arguably, stricter than those of EU member states. The EU and U.S. have established a “safe-harbor” framework for the transfer of information in the commercial context, but this framework is limited to those U.S. entities that have subscribed to the U.S. Department of Commerce Safe Harbor Scheme.

GIBSON DUNN

Data privacy frameworks are also in place in some Asian and South Asian jurisdictions, including Japan, Hong Kong, Korea and India. In India, for example, to collect sensitive personal information, a company must adhere to standards requiring (1) that the company must ensure that the person providing it with sensitive information knows that the information is being collected, the purpose for which it is being collected, and the intended recipients of the information, including the name and address of the agency that is collecting and will retain the information; (2) that the company must only collect and use the information for a lawful purpose; (3) that the company must obtain the informed consent of the provider of the information; (4) that the provider of the information must be given an opportunity to review the information and correct any inaccuracies; and (5) that the information can only be retained for as long as is required for the purpose for which the information was collected. (For more information regarding India's recently enacted data privacy rules, see Gibson Dunn's client alert, available [here](#).) A number of Asian nations are currently working through the Asia-Pacific Economic Cooperation forum ("APEC") and the Data Privacy Pathfinder Project to develop clear guidance for the cross-border flow of personal information.

Latin American countries, including Argentina, Chile, and Columbia also have data privacy laws in effect. In Brazil, where data privacy is recognized as a right under the national constitution, comprehensive privacy legislation is currently being considered. A few African nations also have data privacy laws, such as Morocco and South Africa. The status of data privacy law is currently in flux throughout the world, so it is important to routinely review applicable data privacy requirements.

Because the U.S. does not have a corollary to the data privacy regimes in other countries, many foreign nations, particularly EU member states, do not view U.S. data protections as adequate to allow unrestricted export to the U.S. Consequently, when a non-U.S. entity (or a U.S.-based company with overseas operations) is involved in litigation in the U.S. or in an investigation by U.S. authorities, counsel often must navigate a complex web to fulfill its discovery obligations while not running afoul of the Data Protection Authority ("DPA") in the non-U.S. jurisdiction. The "data controller" in the non-U.S. jurisdiction, often a local subsidiary, must ensure that data is not being treated in a manner inconsistent with the obligations and requirements imposed by that nation's data privacy framework. A party that discloses private information in violation of data privacy legislation may face fines, or even criminal charges. But, a party that fails to adhere to a U.S. discovery order can face a variety of sanctions, including contempt or an adverse judgment.

Other confidentiality protections or restrictions on the transfer of ESI may apply in certain jurisdictions. For example, Swiss bank secrecy laws protect the identity of bank clients. In transferring ESI out of the People's Republic of China, one must be cognizant of a number of national and local restrictions, including the State Secrets Law, the Anti-Unfair Competition Law, the Archives Law and Computer Information System Regulations. Employees also may benefit from additional protections imposed by local employment laws that are entirely separate from a nation's data privacy requirements. In Germany and France, for example, it may be necessary to inform or consult with the local works council before copying and reviewing emails. In some jurisdictions, including France, "blocking" statutes may prohibit and impose criminal penalties for exporting certain information for use in non-U.S. litigation. (See Gibson Dunn's client alert regarding the French Supreme Court's decision upholding the criminal conviction of a French lawyer for violating the French blocking statute [here](#).) U.S. courts have generally declined to defer to such prohibitions, at least in part based on a perception that they are not regularly

enforced. This stance may have spawned a backlash, as some jurisdictions have more actively enforced their blocking statutes following U.S. judicial decisions citing a lack of enforcement.

The EU's Article 29 Working Party Opinion 1/2009 (available [here](#)) highlights the differences in the extent of discovery obligations between the common law jurisdictions (such as the U.S.) and the civil law jurisdictions (including most EU member states), where the extent of discovery is far more restrictive. The Opinion recognizes the legitimate interest in retaining, reviewing and disclosing relevant documents, but provides that the interests of the parties in litigation must be balanced against the rights of data subjects. It envisions a culling exercise where consideration is given to the relevance of personal data, consequences to the data subject and the possibility of redaction.

If redacting or removing the protected information is not an option, there may be other alternatives, such as obtaining the consent of the data subject, or, if engaged in civil litigation, having a court issue a "letter of request" under the framework of The Hague Evidence Convention. Although consent is a ground for processing under the EU Directive, it can be problematic in practice. First, the consent of each data subject is required and data subjects may include customers, third parties and ex-employees. Second, in the case of employees, it may be questionable whether consents are freely given. The recent Article 29 Working Party Opinion 15/2011 issued on July 13, 2011 (available [here](#)) provides that for consent to be valid, data subjects must have an ability to fully comprehend how their personal information is being treated before they can give "unambiguous" consent.

Some have argued that obtaining consent or using the procedures from The Hague Evidence Convention can be costly, inefficient, and impractical. Therefore, if a company is subject to cross-border discovery, it can be important to think of creative and pragmatic solutions. A work in progress of The Sedona Conference® may ultimately provide some assistance. Its cross-border discovery working group is developing a set of principles for how parties, courts and DPAs should address issues of cross-border discovery. These guidelines will be available for public comment later this year.

In addition, being prepared for cross-border discovery, communicating where necessary with the relevant DPAs, and making use of procedures in U.S. courts to appropriately limit discovery can have a significant impact.

Preparedness for Cross-Border Discovery: Being prepared for cross-border discovery is of critical importance for any company with overseas operations and ESI located in non-U.S. jurisdictions. Steps that companies may consider include the following:

- First, companies should be aware of the types and location of ESI under their control. Developing a data map with this information in advance can be very valuable, particularly as the time and resources usually required to create one can make it difficult to do so while embroiled in litigation or an investigation.
- Second, companies should develop an understanding of and familiarity with the data privacy and other restrictions on the processing and transfer of data in the jurisdictions where their ESI is located. Before processing or transferring ESI, companies should consider obtaining the advice of local experts regarding data privacy and other restrictions.

GIBSON DUNN

- Third, companies should review their records management practices to ensure that ESI is not unnecessarily being transferred to jurisdictions where the ESI will be subject to data privacy or other restrictions, making it difficult to transfer the ESI in the event of litigation or an investigation.
- Fourth, companies should consider reviewing their data security measures to ensure that they are taking reasonable steps to safeguard personal data. Companies should satisfy themselves that they have selected appropriate application and storage vendors and that appropriate contractual protections are in place. In addition, consideration may need to be given to the possible notification of data subjects and the rights of access, rectification and erasure enjoyed by data subjects.
- Fifth, companies should consider whether they have appropriate policies, notices and consents that clearly set out how they process personal data and that envision up front the possible future need to disclose personal data in the context of litigation and in internal or governmental investigations.
- Sixth, companies should consider the legal and logistical issues in advance and have a plan in place for the implementation of a legal hold and the collection, review and production of documents in a cross-border context. For example, if a company's ESI is located in several European member states, it may make sense to transfer the data to one central location within the EU, where it can be stored, processed, culled and reviewed. Culling and review can significantly reduce the amount of ESI that must be transferred and can thus decrease the burden of actions needed to comply with data privacy restrictions (such as removing personal information from the ESI).

Communication with DPAs: Where compliance with data privacy or other restrictions would be difficult or impossible, it may be helpful to have a channel of communication with the local DPA or other relevant authority. For example, if a company can demonstrate to the DPA that the information will be treated in a secure and protected manner in U.S. litigation—for example, pursuant to a protective order requiring confidential treatment—then the DPA may be more willing to show some flexibility or leniency. Additionally, some U.S. courts have been willing to consider affidavits or amicus briefs from DPAs expressing a strong national interest in protecting the privacy of the information and demonstrating a realistic likelihood of punishment if the data is transferred to the U.S. Contacts with DPAs will not always be beneficial, however, as DPAs in some jurisdictions tend to focus attention most on those whose arrangements they are aware of rather than actively investigate those companies that have not put their “head above the parapet.” In those circumstances, a company may be better off complying with the applicable data privacy requirements without actively involving the DPA.

Limiting Discovery: Companies may make use of the procedures available to them in U.S. litigation to attempt to avoid or limit the need to produce restricted information from non-U.S. jurisdictions. For example, it can be useful to raise issues pertaining to discovery of information located in non-U.S. jurisdictions at an early stage with litigation opponents and the court—for example, in the discovery planning process provided for in the Federal Rules of Civil Procedure. It may also be effective to pursue strategies such as phased discovery, where information is first produced from U.S.-based sources, or from locations without data privacy restrictions. If the information is available in the U.S., it may not be necessary to take the same information out of another nation. Also, phased discovery can give the parties an opportunity to target key issues. If a company can limit the scope of documents to be collected from a non-U.S. jurisdiction, it may be able to make a more compelling argument to the DPA that the transfer is necessary and reasonable.

GIBSON DUNN

In conclusion, cross-border discovery can involve myriad challenges and implicate a number of different laws and regulations in the jurisdictions in which relevant ESI is located. Obtaining the assistance of counsel with expertise in the local requirements and experience in handling cross-border discovery should be an important part of a company's strategy in addressing these challenges.

Other installments in our E-Discovery Basics series are available [here](#).

*If you would like to **subscribe** to future installments of E-Discovery Basics, and have not already done so, please [click here](#).*

If you would like to suggest topics for future installments of E-Discovery Basics, please [click here](#).

Lawyers in Gibson Dunn's Electronic Discovery and Information Law Practice Group can assist in implementing defensible and proportionate approaches at all stages of the e-discovery process. For further information, please contact the Gibson Dunn lawyer with whom you work or any of the following Chairs of the Electronic Discovery and Information Law Practice Group and attorneys in our European offices:

United States

Gareth T. Evans - Practice Co-Chair, Los Angeles/Orange County (213-229-7734, gevans@gibsondunn.com)

Jennifer H. Rearden - Practice Co-Chair, New York (212-351-4057, jrearden@gibsondunn.com)

G. Charles Nierlich - Practice Co-Chair, San Francisco (415-393-8239, gnierlich@gibsondunn.com)

Farah Pepper - Practice Vice-Chair, New York (212-351-2426, fpepper@gibsondunn.com)

Europe

Patrick Doris – London (+44 207 071 4276, pdoris@gibsondunn.com)

James A. Cox - London (+44 207 071 4250, jacox@gibsondunn.com)

Daniel E. Pollard - London (+44 207 071 4257, dpollard@gibsondunn.com)

Andrés Font Galarza - Brussels (+32 2 554 7230, afontgalarza@gibsondunn.com)

Bernard Grinspan – Paris (+33 1 56 43 13 00, bgrinspan@gibsondunn.com)

Jean-Philippe Robé – Paris (+33 1 56 43 13 16, jrobe@gibsondunn.com)

Michael Walther - Munich (+49 89 189 33-180, mwalther@gibsondunn.com)

Mark Zimmer - Munich (+49 89 189 33-130, mzimmer@gibsondunn.com)

Robert C.J. Heymann (+49 89 189 33-130, rheymann@gibsondunn.com)

Asia

Kelly S. Austin – Hong Kong (+852 2214 3788, kaustin@gibsondunn.com)

Jai S. Pathak – Singapore (+65 6507 3683, jpathak@gibsondunn.com)

Priya Mehra – Singapore (+65 6507 3671, pmehra@gibsondunn.com)

Latin America

Lisa Alfaro—São Paulo (+55 11 3521 7160, lalfaro@gibsondunn.com)

© 2011 Gibson, Dunn & Crutcher LLP, 333 South Grand Avenue, Los Angeles, CA 90071

Attorney Advertising: These materials have been prepared for general informational purposes only and are not intended as legal advice.

E-Discovery Basics 11-Cross-Border EDiscovery.doc

