CURRENT APPROACHES TAKEN IN U.S. LITIGATION TO COMPLY WITH POTENTIALLY CONFLICTING U.S. DISCOVERY OBLIGATIONS AND EU AND OTHER FOREIGN DATA PRIVACY STATUTES

David W. Ichel, Simpson Thacher & Bartlett
Peter J. Kahn, Williams & Connolly
Theodore Edelman, Sullivan & Cromwell
(November 2012)
Current Approaches Taken in U.S. Litigation To Comply with Potentially Conflicting U.S. Discovery Obligations and EU and Other Foreign Data Privacy Statutes

The increasing globalization of commerce has placed front and center in federal and state commercial litigation today the potential for conflict between broad U.S. discovery obligations and foreign privacy protection laws that are much more restrictive than those in the U.S. Moreover, U.S. counsel face these same issues in responding to investigative subpoenas and demands from U.S. federal and state agencies or in conducting internal investigations that call for foreign located documents.

We believe that it will be useful to share with the Conference some current approaches taken by counsel and judges in addressing these situations—and questions and judgment calls we confront-- and to call upon Conference participants to add their additional approaches with the hope that these will help lead to discussion of some “best practices,” some potential proposals for change and/or for helping educate the broader judiciary on potential solutions to address these issues.

I. Framing the Issue Faced By U.S. Litigants

Litigating counsel or government agencies seeking discovery of foreign located documents cannot simply rely on _Aerospatiale v. U.S. Dist. Court of Iowa_, 482 U.S. 522 (1987), and assume that a court always will enforce broad U.S. discovery against a foreign party or non-party that seeks narrowing or other relief from those requests due to conflicting foreign data privacy protection laws or similar legislation. Although _Aerospatiale_ held that a litigant need not rely exclusively on Hague Convention Letters Rogatory for discovery from foreign sources and
upheld U.S. discovery requests over the French blocking statute\(^1\), the Supreme Court in that decision made clear that a court faced with a conflict between U.S. discovery obligations and applicable foreign law proscribing all or part of such discovery must as a matter of comity provide “due respect to for any special problem confronted by the foreign litigant on account of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state.” 482 U.S. at 546, 556. In particular, the court should weigh those public and private interests against the U.S. discovery interests using a five-factor test. In certain situations, this balance might ascribe greater weight to a litigant’s fairly framed discovery objections founded on a foreign privacy law or on a blocking statute, such as the French blocking statute addressed in *Aerospatiale*, than to the broad discovery standards that are the hallmark of U.S. jurisprudence.

Moreover, the whole thrust of the recent amendments to the Federal Rules of Civil Procedure is to attempt to reduce discovery burdens that have been magnified in the age of electronic communication. Fed.R. Civ. P. Rule 26 (b) (1) now presumptively limits discovery to information “relevant to any party’s claim or defense.” Consistently with that standard, Rule 26 (b) (2) (C) mandates that the Court restrict discovery that is duplicative, cumulative, can be obtained by other means or the cost and burden of which outweighs its likely benefit. Rule 1 requires that the Rules be “construed and administered to secure the just, speedy and inexpensive determination of every action and proceeding.” These limitations can be implemented through various tools, such as confidentiality protective orders, case management orders, counsel negotiated “legitimization plans” and judicial intervention to encourage narrowing of discovery

---

\(^1\) French Penal law No. 80-538 (July 16, 1980), which prohibits “any person to request, investigate or to communicate in writing, orally or by any other means, documents or information relating to economic, industrial, financial or technical matters leading to the establishment of proof with a view to foreign administrative or judicial proceedings or as a part of such proceedings.”

The opinions expressed herein are those of the authors and not of their Firms or their clients.

U.S. counsel and judges that have been facing this issue therefore have had both rules and tools to address these issues, although we leave for later panel discussion proposed improvements that might be warranted both in U.S. courts’ and in foreign data protection authorities’ approaches to these issues. Even when counsel today can engineer the harmonization of U.S. discovery obligations with foreign data privacy protection laws, there is still the problem of finding solutions that are cost effective. Just by way of example of costs entailed in such a “marrying” process currently, redacting every name and private personal data in a multi-million page electronic data-set located in Europe, and creating a log of all such redactions, is enormously burdensome, time-consuming and expensive as is requiring only local in-country initial review and culling of documents.

II. **Dealing With the U.S. Preservation Obligation**

The first time a potential conflict with foreign data protection laws will likely surface is before there is an actual litigation or agency investigation. When litigation or an agency demand is reasonably anticipated to be likely, U.S. law requires the preservation of documents that are potentially relevant. Yet, it is clear from the text of the EC Data Protection Directive 95/46/EC that preservation of documents constitutes “processing” that triggers the provisions of the Directive and specific Member State Data Protection Acts. Fortunately, the Article 29 Working
party Opinion 2009/1, expressly recognizes the necessity of Data Controllers preserving documents in the circumstances of an actual or imminent litigation. Working Document at 8. Counsel rely on that Working Document opinion, as well as on the grounds of “compliance with a legal obligation” and “legitimate interests pursued by the controller” under Article 7 (c) and 7(f) of the Data Protection Directive itself in taking preservation steps. ²

However, local counsel in each potentially applicable foreign jurisdiction should be consulted at this stage to ensure that specific preservation methods will not infringe that country’s applicable Data Protection Act or other laws. For example, data authorities in many countries with a data privacy law take the position that no “culling” or “reviewing” of documents should take place outside of that country.

Since as part of the preservation process, employees (or agents) with potentially relevant documents must be provided with a “Hold Notice” to retain documents, in certain investigation or litigation “hold” contexts, it may also be a good time to consider using this as an opportunity to obtain “consent” for use of the documents in responding to discovery and for any trial, fully describing the nature of the potential use, the fact that efforts will be made to obtain a confidentiality protective order protecting the documents and providing for the right to withdraw the consent. We will discuss more about “consent” below.

While preservation steps typically are taken at the outset of threatened or actual litigation, it is also the time to begin the process of developing a proposed privacy law “legitimization” methodology for handling the U.S. mandatory disclosure and discovery collection and transfer obligations.

² The Article 29 Working party has taken the view that the Article 7 (c) ground to allow processing of “compliance with a legal obligation” “may” apply only to EC Member States and suggests reliance instead on the “legitimate interest” ground of Article 7 (f), but this narrow view of Article 7 (c) has not been court tested.

The opinions expressed herein are those of the authors and not of their Firms or their clients.
For certain criminal investigations or those involving national security or defense, the EC Data Protection Directive (Article 13) recognizes that there will be occasions when employees should not be notified of a proceeding or government document demand because it could compromise the investigation. Again, local counsel’s input will be essential.

III. **Initial Disclosures, Document Requests, Interrogatories and Subpoenas**

Requirements of foreign data privacy protection laws also likely will be implicated even as early as the deadline for exchanges of Rule 26 (a) Initial Disclosures of witnesses with relevant knowledge that include foreign individuals. These laws will certainly be implicated by document demands, Interrogatories, subpoenas and Civil Investigative Demands, as well as internal investigations. For example, for EEA countries\(^3\), the EC Data Protection Directive must be satisfied, including (1) the requirements for reviewing and culling documents for potential production (\(e.g.,\) Articles 6, 7 and 8), (2) the requirements for data subject notice, access and opportunity to object (\(e.g.,\) Articles 10-14) and (3) the requirements for safeguarding and transfer of the documents to the U.S., which is considered a country without adequate data protection safeguards under the Directive. (\(e.g.,\) Articles 17, 25, 26). The Article 29 Working Party 2009/1 Opinion, read together with the Sedona Working Group Principles, provide a useful road map for a potential legitimization plan. The Article 29 Working Party 2009/1 Opinion recognizes that relevant information and documents can be produced in U.S. litigation so long as there are adequate privacy protection safeguards that comply with Data Protection Directive.

---

\(^3\) The European Economic Area (EEA) comprises the countries of the European Union, plus Iceland, Liechtenstein and Norway.

The opinions expressed herein are those of the authors and not of their Firms or their clients.
A. **Local Counsel**

Here, again, local counsel in each potentially applicable jurisdiction should be consulted concerning how to approach the U.S. discovery and disclosure from that country in compliance, where possible, with local law and to understand fully the risks of non-compliance.

B. **Local Review**

Most countries with broad data privacy protection laws require that the review and culling of data for production and removal of personal information be done locally in the applicable country. The Article 29 Working party recommends that these activities be conducted by a trusted local party. This seems an unwarranted and expensive requirement that should be examined for change, but data protection authorities base it on the concept that after documents leave the country, there is no means for local control and enforcement.

C. **Immediately Involve Experienced Data Production Consultants, Company IT Supervisors and Data Privacy Officers**

Counsel should set up a working group of outside and inside counsel (U.S. and local), company IT and privacy officers and engage experienced document discovery consultants who can help manage the process and offer potential cost effective solutions. This will include a data processing firm with local capability and good technical knowledge about potential solutions for cost effective document review, redaction, logging, storage and production. Some of the international accounting firms have developed expertise and capabilities in this area.

D. **Consent**

Consent of the data subject is one of the permissible grounds for “processing” of personal data under Article 7 (a) and for “transferring” the data under Article 26(1) (a) the EC Data Protection Directive.
Protection Directive. To qualify, the consent must be fully informed, non-coerced and allow for withdrawal. Although the Article 29 Working Party Opinion 2009/1 counsels against reliance on consent because of the difficulty in meeting these requirements, it can be an effective way of easing mandatory disclosure and discovery burdens in certain investigations and litigations. The key to effective use of consent is to develop a written form with local in-country counsel (usually electronic--in the language used by data subjects) that fairly describes the litigation/investigation, the foreseeable uses and recipients of the documents, the confidentiality protections that will be applicable under a confidentiality stipulation or protective order and the time frame of the consent (e.g., until the end of the litigation, investigation, at which time the documents will be destroyed or returned), an undertaking, where possible, to redact personal-life communications (if that is the case), the freedom of the data subject to withhold or withdraw consent without risk of adverse employment action, and the data subject’s right and to review his/her documents that will be produced. The data subject is asked to “tick” a box indicating consent. A record is then kept of the consents for use in the event of inquiry by a local data protection authority.

Coupled with the opportunity of company supervisory personnel, data privacy officers and/or counsel to speak with employees, this can be a practical approach to reach most relevant employees and even former employees. For those persons that cannot be reached or who decline to consent, their names or other personal identifying information can be redacted as required to satisfy the data privacy law.

The potential problems with attempting to use consent include (1) situations where emails and other documents include identification of significant numbers of identities of non-employee customers or other third persons subject to the protections of the data protection law, (2) whether the disclosures in the consent form can be made sufficiently detailed to provide for authorization.
that would be considered legally valid in the applicable country, (3) whether the process actually saves costs versus an identity redaction program, (4) whether the process would enable a small minority effectively to exercise a “veto” over an elaborate compliance process by withholding consent that a substantial majority has accepted as prudent and sufficiently protective, and (5) the uncertainty engendered by the prospect that consent providers may withdraw a freely-given consent after recipients reasonably have relied on it in the conduct of significant activities in connection with a litigation, investigation or other actual or threatened proceeding.

E. **Redactions and Redaction Logs**

Redactions and redaction logging is one of the standard methods by which compliance with data privacy protection laws can be effected. However, it can be expensive and may be viewed with suspicion by opposing litigants, regulators and even courts and other tribunals. Since documents must be reviewed in any case and redactions will be made for privileged information in any case, it can be argued that the additional cost of this process for data privacy protection is not as great as some would posit.

F. **De-Duplicating**

This will reduce the number of documents.

G. **Obtaining a Court Order**

Counsel representing a client subject to foreign data protection laws will often want a court order mandating the discovery so that it can be shown to foreign data protection authorities as proof that the discovery produced was truly in compliance with a legal obligation and “proportional” to the case needs. First through the Rule 26 (f) conference and other negotiating efforts with opposing counsel, and then through either a proposed consent order or through a contested motion or motions, counsel will seek to (1) narrow to the extent possible the discovery

The opinions expressed herein are those of the authors and not of their Firms or their clients.
demands to those that are targeted in scope and limited in numbers of custodians through which searches must be made and to (2) provide for the sequencing of discovery to minimize potential conflict with applicable foreign data protections laws, leaving potentially duplicative foreign sources of discovery to later showing of need.

In the agency investigation context, counsel will generally be looking to show cooperation with the agency and hence minimize the prospect of resort to the courts, in part, by trying to negotiate a document production plan that will comply with applicable foreign data protection laws. Those plans may include such terms as confidentiality stipulations, sequencing of foreign custodian searches or productions, foreign located review and provision for redaction and redaction-logging of personal information.

H. **Using the Hague Convention**

The use of Letters Rogatory under the *Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters* (March 18, 1970) issued by the court presiding over the litigation to the foreign government-designated authority is one means in which discovery can be obtained in signatory foreign countries. It can be useful in certain countries for targeted party discovery, particularly when both sides see it in their interest to cooperate, and it is sometimes the only means by which discovery can be obtained from a non-party that is not present in the U.S. The draw backs encountered with this device include (1) potential delay by foreign designated authorities, (2) possible judicial challenges to the process in the foreign country that can delay the process even beyond the U.S. trial date, (3) the foreign authority requirement for rigorous specificity in document requests and (4) opt-outs by certain signatory countries for common law discovery. These contingencies can be reduced and the utility and efficiency of the Hague process can be enhanced if the parties agree on a program for consensual conduct of that
process, typically with the involvement of a jointly-proposed commissioner (under Chapter II of the Hague Convention) in the relevant foreign jurisdiction.

I. Providing For Data Security and Data Transfer to the U.S. and U.S. Recipients

One of the pillars of most foreign data privacy protection laws is the requirement for data security limiting disclosure of, or access to, personal data to unauthorized third parties in the data collection, data storage and data transfer process. This is another reason for the continued involvement of company data privacy officers and IT leadership in the discovery response and processing effort and the use of experienced litigation data consultants, along with local counsel, to attempt to ensure data security. The confidentiality order is one important means by which these protections can be addressed, but additional agreements containing “Model Contractual Clauses” can be employed for compliance with some country data protection laws before a data transfer is made to a U.S. data repository, U.S. counsel and regulator or tribunal. Protection for data transfer is a necessary part of any “legitimization” plan proposal made to U.S. opposing counsel and/or to the court.

J. Nothing Should Prevent Fair Discovery Needed

Nothing in these approaches should be used to prevent or hide legitimate discovery. As in all aspects of discovery, good faith is required by counsel and the parties on both sides.

K. Negotiating the “Legitimization” Protocol (if possible) and Obtaining a Court Order Providing For Appropriate Data Privacy Protections

As noted above, counsel should—very early in the case—attempt to obtain adversary counsel’s agreement (if possible) and the U.S. court’s order providing for a disclosure and discovery protocol that will satisfy to the extent reasonably practicable the provisions of

The opinions expressed herein are those of the authors and not of their Firms or their clients.
applicable foreign data privacy laws without compromising legitimate needs for discovery in the
case. Provisions in such a protocol and order typically include:

1. **Confidentiality Stipulation/ Protective Order**

   This would look a lot like the standard confidentiality stipulations and orders used in
domestic litigations, except that it would add, as applicable, (1) a “Protected Data” definition
and provisions for information claimed to be subject to data protection laws and similar
legislation to be included within the confidentiality protected information, (2) a provision
providing for redaction and logging of redactions for such “Protected Data,” (3) a provision for
notice and access to produced documents by data subjects where required (See EC Data
Protection Directive, Article 12), (4) trial use protections and/or (4) a requirement that recipients
enter into EC “standard contract clauses” for data security protection.

2. **Narrowing Discovery Demands to Reasonably Specific and Identifiable Categories and Custodians**

   By agreement or motion, the parties to the litigation or other proceeding should agree to
narrow discovery to specifically targeted requests and a limited group of custodians. Where local
country counsel deems it important, the parties should seek an Order requiring the discovery as
narrowed. There should be provision for de-duplicating materials provided in discovery.

3. **Case Management Sequencing Order**

   Both the Article 29 Working Party 2009/1 Opinion and the 2011 Sedona Principles
suggest implementation by stipulation or order of a two stage document production plan that
envisages a first stage of production that will, where practicable, “anonymize” most documents
(e.g., by redaction) and that will in the first instance be more limited in scope to allow both sides
to see whether domestic sources of discovery will render further burdensome foreign discovery

The opinions expressed herein are those of the authors and not of their Firms or their clients.
unnecessary. Further discovery may be sought as of set time based on good cause shown after both the domestic and first-stage foreign productions have been reviewed.

4. **Transfer**

Articles 25 and 26 of the EC Data Protection Directive govern the requirements for transfers of personal information out of the applicable EEA country to ensure that the transferee country “ensures an adequate level of protection” (Article 25.1), and individual countries have their own requirements. Read literally, the Article 26 allows a “derogation”—exception—from the Article 25 data transfer requirements “for the establishment, exercise or defence (sic) of legal claims.” Article 26 (1) (d). Nevertheless, a 2005 Article 29 Working Party opinion, *A Common Interpretation of Article 26 (1) of Directive 95/46/EC* (adopted Nov. 25, 2005), read this “derogation” as still requiring that the data controller ensure adequate data protection safeguards and even limiting transfers to those allowed under the Hague convention. 2005 Opinion at 15.

The Article 29 Working Party Opinion 2009/1 states that data transfers to countries such as the U.S. that have not established EC–recognized “adequate levels of protection” may be undertaken if:

a) *The recipient has subscribed to the Safe Harbor Scheme Managed by the U.S. Department of Commerce.* Note that this self-certification scheme is available only to companies under the jurisdiction of the Federal Trade Commission or the Department of Transportation. Some data storage and data consulting vendors have self-certified.
b) *The recipient has entered into a contract with the data transferring company with “standard contract clauses” provided by EC Decisions June 15, 2001 and December 27, 2004.* This will apply to law firms, consultants, storage providers or experts who see the documents. This procedure has been required by company clients in various countries, such as Germany, as a prerequisite to transferring personal data consistently with national data protection laws. These clauses require submission to EC country jurisdiction or agreed-arbitration to address data subjects’ breach of data security claims.

c) *The recipient has EC Country approved “Binding Corporate Rules” to ensure an “adequate level of protection.”* The current requirements for “binding Corporate Rules” approval are so onerous that very few companies are compliant, and accordingly this has not been a widely used option. There are proposed amendments to the EC Data Protection Directive that would make the process more realistic.

It should be noted that the Article 29 Working Party Opinion 2009/1 also seems to allow for the “derogation” of Article 26 (1) (d) to permit a “single”—not repetitive—transfer of all relevant responsive data where “necessary or required for the establishment, exercise or defence (sic) of claims” in U.S. litigation. Opinion at 13. This alone arguably might be relied upon, along with adequate confidentiality order protections; but, because of the attendant uncertainties and significant sanctions for non-compliance, some clients and local counsel in some EEA countries have insisted on using approved “standard contract clauses.”

The opinions expressed herein are those of the authors and not of their Firms or their clients.
Article 29 Working Party Opinion 2009/1 also states that Hague Convention transfers from signatory countries will be compliant under Rule 26 (1) (d).

IV. **The Judicial Role**

Judges play a key role in addressing party issues with the requirements of foreign data protection law while ensuring effective and efficient conduct of necessary and appropriate discovery in U.S.-based proceeding. This requires that counsel as early as possible in the case inform judges of these issues and adequately explain both the law and the practical difficulties.

Some current useful approaches and questions are:

A. Requiring that the Parties raise foreign data protection issues early, including Hague Convention Letter Requests and other foreign discovery proposals.

B. Requiring that the Parties address these issues in proposed Case Management orders.

C. Requiring that the Parties attempt to negotiate a proposed “legitimization” protocol allowing for necessary discovery while seeking to promote compliance with legitimate foreign data protection laws and to bring to the court those areas that remain in dispute.

D. Determining appropriate remedies for refusal to produce due to claimed foreign data protection law requirements.

E. Use of Confidentiality and Discovery Sequencing Orders to address these issues.

F. Addressing “Sunshine Law” issues and open trial issues.

The opinions expressed herein are those of the authors and not of their Firms or their clients.