THE CONFLICT BETWEEN AMERICAN DISCOVERY
AND EUROPEAN PRIVACY

Tati Sainati
(November 10, 2012)
MEMORANDUM

TO: Ralf Michaels
FROM: Tati Sainati
DATE: Nov. 10, 2012
RE: The conflicts between American discovery and European privacy

I. FAULT LINES

A. Policy Conflict

Issues arise due to the fundamentally different perspectives on privacy and disclosure in the European and American legal regimes. (Alan Charles Raul, Edward McNicholas & Elisa Jillson, Reconciling European Data Privacy Concerns with US Discovery Rules: Conflict and Comity, reprinted from Global Competition Litigation Review, no. 3, at 4 (2009)). To Europeans, privacy is a fundamental human right. (Carla L. Reyes, The U.S. Discovery – EU Privacy Directive Conflict: Constructing a Three-Tiered Compliance Strategy, 19 Duke J. Comp. & Int’l L. 357, 362 (2009)). The EU has adopted an “omnibus approach” to data protections, under which all personal information is protected. Under the 1995 Data Protection Directive, the EU prohibits the unauthorized processing of personal data, defined as “information relating to an identified or identifiable individual.” Processing is viewed with suspicion by regulators, and is prohibited absent consent or specific statutory authorization. Data must be collected “for a specific, explicit purpose,” and individuals implicated must receive “detailed notice.” (Karin Retzer and Michael Miller, The Bureau of Nat’l Affairs, Inc., Mind the Gap: U.S. Discovery Demands versus EU Data Protection, Privacy & Security Law Report, 10 PVLR 886 at 2 (2011)). Nevertheless, European countries have allowed disclosure of personal information where the purpose behind collection of such information outweighs the individual privacy interest at stake. (Raul, McNicholas & Jillson at 6). For example, the French Conseil d’Etat recently upheld disclosure of personal information in the context of counter-terrorism initiatives. (Id.). In contrast, the US approach is narrower. Organizations may process personal data as necessary, even absent statutory prohibitions. (Retzer and Miller at 2). Personal information is also more narrowly construed to include only particularly sensitive information. Thus, American courts may be ill-equipped to understand the competing interests involved in discovery demands where EU conceptions of personal privacy are concerned. (Id. at 2).

Additional problems arise due to the differences in common and civil law approaches to discovery in general. The American notion of pre-trial discovery encourages parties to cast a wide net. (Dan Cooper, e-Discovery and EU Privacy Laws – Part II, 8 Privacy & Data Protection J., no. 7, at 4, 2008, pp. 3-7). The Federal Rules of Civil Procedure require production of any information that may lead to the
discovery of admissible information, (id. at 4), and impose substantial affirmative disclosure obligations on parties to an action. (Id. at 2-3). Thus, US discovery requests may run afoul of EU data protection laws, since EU authorities are likely to perceive such requests as excessive. (Id. at 3). Specific problems arise since the Federal Rules of Civil Procedure allow discovery of documents in the “possession, custody or control” of a party, and “control” has been broadly construed. In the context of affiliate or parent organizations, the “control” test may prohibit a US entity from declining a discovery request, simply because the requested information is in the control of a foreign-located subsidiary or affiliate. In such situations, particularly severe results where courts have imposed “adverse inference” sanctions on organizations which have failed to provide requested documents. (Id. at 3).

The Hague Convention on Evidence was adopted in part in response to these problems. However, it has proved relatively ineffective – in part due to many US courts’ refusal to follow conventional protocols, and in part due to reservations entered by many of the European states’ parties (Id. at 4). Art. 23 of the Convention was proposed specifically to respond to concerns about the overly broad nature of U.S. discovery, since the extraterritoriality of US discovery rules is perceived as a threat to the sovereignty of other states. (Marissa L. P. Caylor, Modernizing the Hague Evidence Convention: A Proposed Solution to Cross-Border Discovery Conflicts during Civil and Commercial Litigation, 28 B. U. Int’l L. J. 341, 344-45 (2010)). American courts have rejected this argument, holding that sovereignty is no bar to discovery since private litigation is not a public matter. Id. at 360. For it’s part, the Supreme Court has held that the Convention is neither mandatory, nor the exclusive mechanism for obtaining information from a foreign jurisdiction during discovery. (Id. at 347).

B. Individual Conflict vis-à-vis two sets of laws

In addition to the European Privacy Directive, several European states have adopted “blocking statutes” designed to impede US discovery. (Retzer & Miller at 4). The Supreme Court has ruled, however, that such statutes do not deprive an American court of the authority to compel production of evidence. (Caylor at 371). In the US, conflicts between US discovery obligations and European privacy laws and privacy statutes are largely resolved in an ad hoc manner by US trial courts. Id. at 5. Although some courts have determined that European privacy laws prevent the release of certain information, most courts continue to compel discovery “even in the face of foreign prosecution.” Id. at 5-6. I

Frequently, even where compliance with both EU and US rules is possible, compliance costs tremendous amounts of time and money. When compliance is impossible, costs – in the form of sanctions, or dismissal of claims - are even higher. (Caylor, at 343). A court in the Southern District of New York held that U.S. courts can impose sanctions on parties for failure to produce requested information, and provide adverse inference instructions to juries. Such decisions have resulted in corporations expending tremendous sums to store, review and retrieve data in preparation for trial. Id. at 368. Individuals are left to choose between sanctions and
adverse inference instructions in the States, or civil or criminal sanctions in the European Union. *Id.* at 369.

C. Conflicting obligations to other parties and clients

Here, common issues include European laws requiring detailed notice to individuals who may be affected by the release of personal information in response to discovery requests (Dan Cooper, *e-Discovery and EU Privacy Laws – Part II*, 8 Privacy & Data Protection J., no. 7, at 3, 2008, pp. 3-7). Such concerns may be addressed by applying anonymization techniques to conceal individual identities. The removal of identifying information may ultimately remove the data from the protections of the EU’s privacy laws. *Id.* at 6. Contractual controls may also be used, which put individual employees on notice of disclosure policies. *Id.* Even within the solutions to notice and consent problems, conflicts between American and European approaches arise. Whereas the United States jurisdictions find general notice acceptable, the European Privacy Directive demands detailed notice to those whose information might be released. Retzer and Miller *at* 2.

Recently, the European Commission identified key reforms to Data Protection, designed in part to strengthen individual privacy rights. Key reforms include the “right to be forgotten,” which will require the deletion of data absent legitimate grounds for retention. European Comm’n, *Why Do We Need an EU Data Protection Reform?* (2012). Consent to the release of data will have to be explicit. Any company offering goods or services in the EU will be subject to these new rules. *Id.*

II. US Case Law


In *Stanford*, the SEC requested information related to a securities fraud investigation from a nonparty Swiss bank, SG Suisse. *Id.* at 326. SG Suisse objected to the request primarily on the grounds that compliance would expose the company to criminal, civil and administrative penalties under Swiss law, and argued that the procedures enumerated in the Evidence Convention were the appropriate mechanism for obtaining the required information. *Id.* at 327.

The district court agreed with SG Suisse, holding that the discovery request should be channeled through the Convention. *Id.* at 326. The court expressly noted the aversion many foreign states feel for American pretrial discovery procedures, necessity “due respect” for the position foreign litigants may find themselves in when confronted with conflicting legal rules. *Id.* at 328. To adequately address the competing interests at stake, the court assessed seven factors: (1) the importance of the requested information to the litigation; (2) the specificity of the request; (3) where the information originated; (4) the availability of alternative ways to access the information; (5) “the competing interests of the nations whose laws are in conflict,”
(6) the hardship imposed on the party from whom discovery is sought; (7) and the good faith of the party objecting to discovery. *Id.* at 330.

Although the court acknowledged that the information requested was important to the pending litigation, *id.* at 331-32, the location of the information in Switzerland required the court to consider the request “in light of Swiss law.” *Id.* at 332. The court also determined that the interests of both Switzerland and the United States were substantial. *Id.* at 335-36. Nevertheless, the court determined that a balancing of these competing interests was unnecessary, since both nations had “spoken [about how they perceived their competing interests] by adopting the Convention.” *Id.* at 337. Additionally, the court noted that Switzerland had not intended to block American discovery procedures in enacting its privacy laws, and that Suisse SG was acting in good faith in denying the requested discovery information. Nevertheless, the court did not preclude the option of resorting to the Federal Rules of Civil Procedure if requests made through the Convention proved fruitless. *Id.* at 342.


In *Credit Lyonnaise,* American victims of a terrorist attack in Israel filed suit against a French bank, Credit Lyonnaise, for allegedly providing support to a terrorist organization. Credit Lyonnaise asked that the request be filed through the procedures in the Hague Convention, and the court excuse the bank from responding to the discovery request due to the privacy protections afforded by French banking laws. *Id.* at 430-31. These French laws made the transmission of the personal information requested a criminal offense. *Id.* at 435.

The court had addressed this “precise issue” in a previous case, holding that the French laws did not provide adequate grounds to refuse a discovery request made pursuant to the Federal Rules of Civil Procedure. *Id.* Credit Lyonnaise argued, however, that this earlier determination was the result of a misapplication and misunderstanding of French law. *Id.* Credit Lyonnaise provided several documents demonstrating the French executive and judiciary positions on their privacy laws and the role of the Evidence Convention in transnational disputes. *Id.* at 436.

Following *Aerospatiale* and *Minepco,* the court assessed Credit Lyonnaise’s objections in light of seven factors: (1) the importance of the information to the suit; (2) the specificity of the discovery request; (3) the jurisdiction in which the information originated; (4) any available alternative ways to obtain the information; (5) the competing sovereign interests of the States concerned; (6) the good faith of the resisting party and (7) the “hardship” which would result from the resisting party’s compliance. *Id.* at 438-39.

In addressing the availability of alternative mechanisms for accessing the information – specifically, the Evidence Convention – the court asserted “that American courts must defer and be subject to internal French law contravenes
American law.” *Id.* at 443. Additionally, the court noted that both the United States and France shared compelling interests in “thwarting terrorist financing,” which “outweighs the French interest in preserving its generally-stated sovereign interest.” *Id.* at 456. Thus, the court ordered Credit Lyonnaise to produce the requested information. *Id.*


In another recent case, a non-party German company received a discovery request in a US civil action for documents located in Germany. *Id.* In the case, the plaintiff alleged that the German corporation had accessed its business secrets, and the discovery request sought evidence in support of this claim.

In response, the Bavarian data protection authority acceded that discovery was necessary, but that certain restrictions prohibited the German company from transferring anything more than “data which corresponded to the criteria of the disclosure request and which were relevant for clarifying the claims of the plaintiff.” Additionally, any documents deemed relevant had to be “manually assessed” in light of the criteria enumerated in the discovery request.

The German company complied with the Bavarian authority’s determination, and submitted both the Bavarian authority’s opinion and the limited documents releasable under that opinion to the court. The court subsequently rejected the plaintiff’s request for broader access to documents, and determined that the plaintiff was not “unreasonably disadvantaged” by the company’s compliance with European data protection laws. No further details of the case, including the identification of the US court, have been published. *Id.* Nevertheless, practitioners note that the approach adopted by the Bavarian data protection authority and accepted by the US court provide guidance on how authorities in the US and Europe can negotiate conflicting discovery and privacy interests. *Id.*

### III. International Attempts to Reconcile Privacy and Discovery


The Council commenced negotiations with the United States on March 28, 2011 to craft an agreement on ensuring adequate protections to personal data transferred in connection with investigations and prosecutions.
The US aims to “achieve mutual recognition of the respective data protection systems (“adequacy”). Id. at 3. The material scope of the agreement is limited to the exchange of personal data between law enforcement and judicial authorities during an investigation, and “program-based” or large-scale data transfers. Id.

The agreement will also deal with data subjects’ rights – although the US intends to act through an executive agreement which will not create any new individual rights. Id. at 4. To date, the parties have discussed the content of fights as follows:

a) **Right to information of data subjects**: the US defended existing notice, and opposed amending legislation to provide for information of data subjects.

b) **Right to access by data subjects**: The US believes that the Freedom of Information Act adequately protects right to access.

c) **Rights to rectification, erasure and blocking**: The Council asserts that the US misunderstands the application of the rights to rectification and erasure – and that there is a need for clarification on this point.

The Council noted that further discussion is necessary “to achieve all objectives identified in the negotiating directives are required, this concerns the content and form of data subjects rights, in particular for judicial redress.”


The Sedona Conference Working Group on Int’l Electronic Information, Management, Discovery and Disclosure (WG6) is comprised of attorneys, officials, consultants, academics and jurists. Id. at 5. The WG6 working paper provides a practical framework to analyze and address legal conflicts stemming from transnational discovery of electronic information. Id. at 6.

The WG6 attributes many of the particular problems arising from cross-border discovery requests to the “special” nature of electronic information. Specifically, electronic data is unlike paper information in six significant respects: (1) volume and ease of replication, (2) persistence, (3) dynamic nature, (4) existence of metadata, (5) hardware & software system dependence and obsolescence, (6) mobility, portability and searchability. Id. at 10.

The paper also discusses the particular problems raised by “blocking statutes.” In a recent case, Christopher X, the French Supreme Court upheld the criminal conviction of a French lawyer for a violation of the blocking statute. Id. at 26. The WG6 committee noted that this conviction could serve as proof to US courts that France enforces its blocking statute. Id. at 27. The conviction “casts in doubt a great
deal of U.S. case law on the issue of cross-border discovery," which has been
premised on the notion that such statutes are seldom enforced.  *Id.* at 32. The
possibility of criminal prosecution may encourage parties to resort to the
mechanisms of the Hague Convention for discovery requests in the first instance.  *Id.*
at 32.

Increasingly, the private sector is acting to mitigate the significant personal
and financial costs from discovery disputes.  For instance, Eli Lilly, an American
pharmaceutical company operating in 50 countries is currently working with data
commissioners in the EU to formulate a plan for handling the competing interests of
discovery and privacy rules.  *Id.* at 33.

For its part, the WG6 identified seven factors to be considered in adequately
balancing the needs and burdens of discovery against the privacy rights protected in
European states:  (1) the nature of the privacy obligations in the jurisdiction where
the information is located; (2) the duties of the responding party to preserve and
protect relevant information under the laws of the state where the claim is filed, and
under the laws where the data is located; (3) the "purpose and degree of custody and
control of the responding party over maintaining the requested information; (4) the
nature and complexity of the case; (5) the amount in controversy; (6) the importance
of the information to addressing critical issues and (7) the burden resulting in
producing and processing the requested information.  *Id.* at 34.

   http://www.hcch.net/upload/wop/2008pd10e.pdf

The Permanent Bureau of the Hague Conference on Private International
Law addressed the question of the mandatory (or non-mandatory) nature of the
Hague Convention in light of disputes between States Parties.  *Id.* at 3. Additionally,
the Bureau addressed the question of whether, if the Convention is not mandatory, it
should still be the first resort for States Parties in discovery request.  *Id.* at 3. To
assess these issues, the Bureau analyzed responses to a survey sent out to the member
states.

The Permanent Bureau noted that opinion regarding the character of the
Convention divided, with common law countries believing the Convention to be
non-mandatory, and civil law countries asserting the mandatory character of the
Convention.  *Id.* at 3.  The Bureau describes the principle arguments for and against
making the Convention mandatory, without taking sides in the debate.

   Authorities Call for Strict General Privacy Agreement with United States* (Nov. 19, 2010),
   available at
The Article 29 Working Party, an independent advisory body on data protection and privacy established by the Data Protection Directive, addressed the initiative for an agreement between the EU and the US on data protection in discovery. The Party emphasized the necessity of including protection safeguards in the final future agreement, including “full, effective and enforceable rights . . .”. Additionally, the party requested “very strict rules for the onward transfer of EU-originating data to other countries,” as well as the establishment of “a system of evaluation and joint review of . . . the future agreement . . . and . . . the underlying bilateral and multilateral agreements. The Party appeared particular concerned about ensuring these protections in light of the “unsatisfactory [data protection] result[s]” in the wake of TFTP II negotiations, which allowed the US access to information on international bank transfers.