Cross Border Discovery

History, Analysis and Current State

By Stacey Blaustein,
Attorney- IBM Corporate Litigation

The Cross-Border Litigation Forum
September 12, 2012

Disclaimer. Not opinions, information from IBM Corp.

Cross Border Discovery- What is it?

- Cross Border Discovery is the discovery of information for litigation, investigation or proceedings from one geographical territory to another and the consideration of all the rules, policies, regulatory environment for the countries at issue.
- Conflict arises in the context of US Cross-Border Discovery when seeking documents/information.
- The Federal Rules of Civil Procedure- Rule 26- calls for broad discovery of anything "potentially relevant" to the claims and issues in a litigation.
- EU Data Privacy Laws prohibit the turnover and production of much information/documentation as it is deemed "protected" by the EU Data Privacy Laws. EU countries have a more restricted view of disclosure. UK disclosure obligations, for example, only allow the production of documents on which your case relies and upon which other cases rely- NO BROAD DISCOVERY.
- Problem- multi-national corporations, cross-border investigations, individuals, corporations, corporate employees who, for US litigation purposes, may have relevant information but restrictions on discovery because of privacy and personal data protections.

- Conflict- US Discovery/EU Data Privacy Laws- US courts sanction parties if do not produce discoverable material; imposition of costs, adverse inferences allowed. EU threatens and proceeds with criminal sanctions for producing and processing Personal Information of documents with personal information.

TYPE OF PROTECTION FOR DATA PRIVACY

I. EU DIRECTIVE 95/46/EC

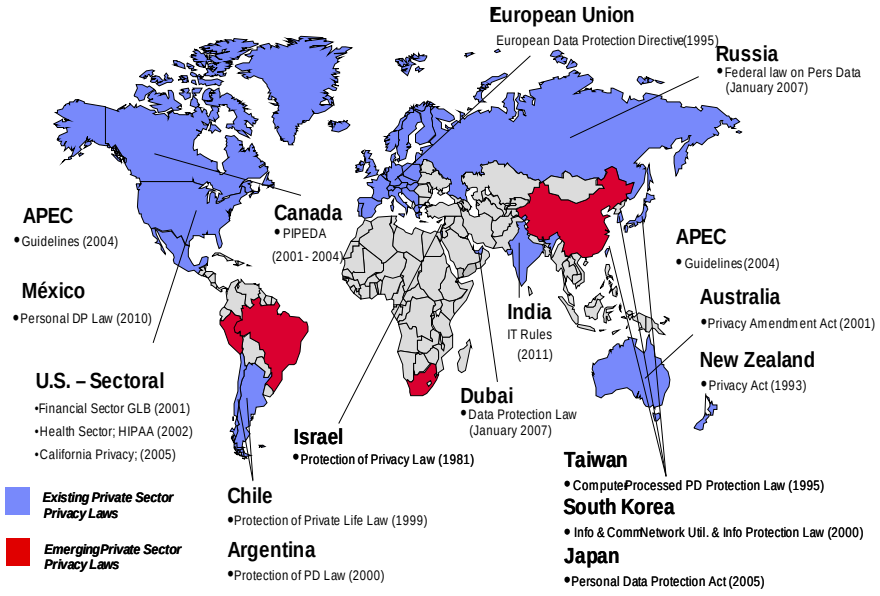
- Currently- the umbrella EU Authority known as DIRECTIVE 95/46/EC of the European Parliament and of the Council of 24 October 1995 - Directive of processing of personal information and on the free movement of such data (effective 1998)
- History behind Directive- driven by inter alia, atrocities of WWII, confiscation by Nazi regime of personal property traced through disclosure of personal information.
- Factories and property confiscated, anything of value taken and traced through mandatory disclosure of personal information. No restrictions historically during WWII time on disclosure of personal information.
- Fundamental right to privacy in constitution of EU; In US, privacy segmented by industries-healthcare (HIPAA), education (FERPA), finance (GRAMM, LEACH, BILLEY)
- PRINCIPAL POINTS OF DIRECTIVE- “PERSONAL DATA” is defined as any information relating to an identified or identifiable natural person (‘data subject’) ; e.g. id numbers, addresses, union membership, physical, psychiatric attributes;
- “IDENTIFIABLE NATURAL PERSON/DATA SUBJECT”- a person who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factors specific to his physical, physiological, mental, economic, attributes cultural or social identity.

- Qualifications- E-mail is considered “Personal Data” by EU Commission and subject to all restrictions on transfer in the Directive and Member States’ enabling legislation, including possibility of criminal sanctions.
- Preserving Data is technically considered “processing.”
- Culling requirement directs review to get rid of irrelevant information or sensitive personal information. The higher the materiality, the more can be done for processing and transferring.

REQUIREMENTS OF EU DIRECTIVE 95/46/EC

- Prohibits transfer of “PERSONAL DATA” to non-EU* nations that do not meet European adequacy standards for privacy protection. *EU nations that are signatories to directive; 27 countries- UK;Sweden;Spain;Slovenia;Romania;Portugal;Poland;Netherlands;Malta;Luxumbourg;Lithuania;Latvia;Italy;Ireland;Hungary;Greece;Germany; France; Finland; Estonia; Denmark; Czech Republic; Cypress; Bulgaria; Belgium; Austria.
- Similarly there are several non-EU nations with similar or emerging data privacy laws, e.g. China; India; Israel; Mexico, Canada, Japan, Russia, Dubai, Chile, Argentina, Taiwan, Australia, New Zealand, South Korea.
- Requires each member of EU to pass Data Protection Laws that comply with Directives’ minimum standards but inconsistency among signatory states.
- Data Privacy Laws- protects disclosure of personal and private data.
- Blocking Statutes- blanketly prohibit the transfer of certain categories of data out of country under any circumstance and carry threat of criminal sanction.
- Prohibits transfer of Personal Data beyond European Economic area to country of lesser standards* of personal data protection without the consent of the data subject, unless certain protections in place, such as those afforded by the US Safe Harbor Program (negotiated with EU authorities) or in model clauses approved by all EU Member states in data transfer agreements.
- SAFE HARBOR- US Department of Commerce in consultation with European Commission developed a “Safe Harbor” framework that allows organizations to join in order to enable transfer of personal data under certain criteria.
- *EU currently considers only five countries to have acceptable standards of data protection and privacy- e.g. Argentina, Canada, Israel, Switzerland, Uruguay- US is not among list.

Privacy Law and Legislation



II. **EUROPEAN COMMISSION PROPOSAL FOR A REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA AND ON THE FREE MOVEMENT OF SUCH DATA.**

- DIRECTIVE 95/46/EC to be superceded by newer EU Authority- European Commission Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Brussels January 25, 2012.
- Prompted by expressed need for reform of existing rules- particularly Directive 95/46- by individuals, companies, data protection authorities and governments.
- Prompted by Treaty of Lisbon entered on December 1, 2009 which brought major constitutional changes in the legal structure of the European Union and includes mention with Article 16 of the Treaty of the Functioning of the European Union that everyone has a right to data protection, elimination of EU's separate country pillar structure, increased oversight and participation in data protection policy, 'making' mention of data protection as fundamental right in Charter of Fundamental Rights of EU and obligation to accede to the EC on Human Rights.
- Desire for harmonized EU data protection framework in order that data protection rights can be enforced seamlessly across EU.
- Currently in state of revision process- will become effective 2 years after its approval not likely to be until end of 2012.

KEY FEATURES OF EUROPEAN COMMISSION PROPOSAL

- Would provide as near complete harmonization under EU law.
- Would make companies with operations in multiple EU member states subject to jurisdiction of single Data Processing Authority ("DPA") based on main place of establishment in EU.
- Would make legal certainty of "adequacy" decisions. Standard contractual clauses for transferring data outside of EU would be increased.
- DPA's would be forced to cooperate and work together with other DPA's.
- Commission would be empowered to issue EU-wide interpretation of important provisions.
- Use of consent for legitimizing data processing would be significantly restricted especially in employer/employee context.
- Companies with more than 250 employees would have to appoint a data protection officer.
- Regulators and affected individuals would have to be notified of data security breaches.
- Some simplification of the procedures for transferring personal data outside of EU.
- Independence of DPA's strengthened.
- Fines for data protection violations could range up to 2% of company's annual worldwide income.
- Regulation has general and direct applications and becomes part of national legal system vs directive which requires implementation by EU member states.

Chapters of Proposed Regulation

I. General Provisions
II. Principles
III. Rights of the Data
IV. Controller and Processor
V. Transfer of Personal Data to Third Countries or International Organization
VI. Independent Supervisory Authorities
VII. Cooperation and Consistency (of Data Processing Agents)
VIII. Remedies, Liabilities and Sanctions
IX. Provisions Relating to Specific Data Processing Situations
X. Delegated Acts and Implementing Acts
XI. Final Provisions

JURISDICTION BY US COURTS OVER CROSS-BORDER DISCOVERY ISSUES

- Historically, Hague Convention principals laid the groundwork and procedures to follow to get discovery overseas.
- 1987 Supreme Court case- SOCIETE NATIONALE INDUSTRIELLE AEROSPATIALE v USDC SD of IOWA, 482 US 522 (1987) – seminal case where French blocking statute at issue- decision announcing allowance of either means to pursue overseas discovery- via Hague Convention or balancing test applied by Federal Courts, which "Aerospatiale' analysis applied prevalently in US courts today.
- Supreme Court held Hague Convention not intended to establish exclusive or mandatory provisions- 2 options- analysis or Hague convention procedures.
- Aerospatiale Analysis- "[T]he concept of international comity requires in this context a more particularized analysis of the respective interests of the foreign nation and the requesting nation than petitioners' proposed general rule mandating resort to Hague Convention procedures in the first instance] would generate."
- "American Courts, in supervising pretrial preceedings, should exercise special vigilence to protect foreign litigants from the danger that unnecessary, or unduly burdencome discovery, may place them in a disadvantageous position…In addition, we have long recognized the demands of comity in suits involving foreign states, either as parties or as sovereigns with a coordinate interest in litigation. American courts should therefore take care to demonstrate due respect for any special problem confronted by the foreign litigant on accord of its nationality or the location of its operations, and for any sovereign interest expressed by a foreign state. 482 US 522, @543-S44.

Comity Analysis Set Forth in Aerospatiale

- Factors to consider in determining if overseas discovery is necessary
- (1) The importance to the litigation of the information requested;
- (2) The specificity of the request;
- (3) Whether the information originated in the US;
- (4) Whether alternative means exist to obtain the information;
- (5) Whether the interests of the US outweigh the interests of the foreign jurisdiction in maintaining confidentiality
- ADDITIONAL FACTOR ADDED- (6) Potential hardship that a producing party might suffer from compliance with discovery requests.

CASES ON CROSS-BORDER DISCOVERY

- In re *Vitamins Antitrust Litigation*, No. 99-197 2001 US Dist. Lexis 8904 (D.D.C. June 20, 2001) Court held that discovery request can overcome foreign legal barriers provided that the requested information is "necessary" but warned to apply reasonable deference to and respect to foreign countries' laws, policies and regulations of possible while seeking discovery.
- *In re Payment Card Interchange Fee and Merchant Discount Antitrust Litigation* 2010 WL 3420517 (EDNY August 27, 2010) In an unusual opinion, the Court held that the EU's interest on confidentiality outweighed the plaintiff's interest in discovery of the *European litigation documents.*
- *Strauss v Credit Lyonnais*, SA. 242 FRD 199 (EDNY 2007) American court rejected the French blocking statute as basis to preclude discovery via US proceedings and ordered the defendant to produce documents in accordance with FRCP despite defendants objection that doing so would subject the defendant to penalties under French Privacy Law and defendant was find by French authorities for complying.
- *In re Advocat "Christoper X" Cour de Cassation.* Appeal No 07-83228 (Dec. 12, 2007) French Supreme Court upheld the criminal conviction and fine of a French lawyer for violating the blocking statute.
- *Access Data Corporation v. ALSTE Technologies GmbH-* A German company refused to produce documents in a breach of contract action. The German company held that production of such documents would reveal third parties identities and violate German Data Protection Law and the German Constitution. The Court ordered such production relying on *Aerospatiale*, claiming that the German Laws do not deprive US Courts of power to produce evidence even though party may violate foreign statute.
- *Pierre B. v Epsilon Composite,* Court d'appel Bordeaux, March 27, 2012; French court hold that employer's interest in confidential data triumps French workers right to privacy.

WHERE ARE WE NOW?

- Global economy/ multi-national companies/global communications/ cloud technology emerging.
- Still no clear articulation on reconciling broad US federal & state discovery rules (applicable to E-Discovery as well as paper discovery) and foreign non-disclosure law (EU directive and proposed regulation.)
- EU proposed regulation broader and more current than EU Directive 95/46/EC and considers data privacy and protection as a "fundamental human right." (can expect a revised regulation in next few year.
- Still in US two main sets of rules under which US courts may enforce discovery laws against foreign companies- Hague Convention and Aerospatiale analysis (fed. rules).
- Use of Aerospatiale analysis favored; Hague unduly long to obtain result.
- Issues when evidence gathering under either Hague Convention or FRCP and domestic law of foreign country does not provide for allowing document collection and production.
- Solution-Risk assessment usually performed for collecting documents, taking potential evidence weighing numerous factors to determine exigency, fairness, reasonableness of discovery.
- What our hopes are- reconciliation of Data Privacy Laws and US Discovery in context of global market taking into account all parties' and countries' interests and needs for information data documents.