GLOBAL DATA PROTECTION: WHOSE RULES GOVERN?

Dr. Axel Spies, *
Bingham McCutchen LLP,
Washington, DC

1. CURRENT PROBLEMS WITH EXTRA-TERRITORIALITY IN THEORY AND PRACTICE.

1.1 Territoriality Principle: As a general principle, a country applies its data protection/privacy laws on all data over which the country has territorial jurisdiction. In other words, the law of the territory applies where the actual "data processing" (storage, modification, transfer, deletion, etc.) is carried out.

(a) EU law does not distinguish between the citizenships of the individuals (data subjects) or the origin of the data. An exception is usually made for the mere "transfer" (or transit) of the data over a territory, although it is not clearly defined in the laws what a mere transfer/transit is. If the controller is located within the EU/EEA, EU law modifies the territoriality principle. To illustrate this approach, Article 4 EU Directive 95/46/EC stipulates that the national law shall apply where

> "(a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the [EU] Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable;
>
> (b) the controller is not established on the Member State's territory, but in a place where its national law applies by virtue of international public law;
>
> (c) the controller is not established on Community territory and, for purposes of processing personal data makes use of equipment, automated or otherwise, situated on the territory of the said Member State, unless such equipment is used only for purposes of transit through the territory of the Community."

The key term "*controller*" is defined broadly and its definition also depends on the applicable national law: Art. 2 (d) Directive: "'controller' shall mean the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data;

* The author is indebted to contributors Quentin Archer, Carman Baggaley, Lara Ballard, Aurélia Cadain, Cristian Gual Grau, Valerie Lawton, and the Honorable Shira A. Scheindlin, who helped make this article possible.

where the purposes and means of processing are determined by national or Community laws or regulations, the controller or the specific criteria for his nomination may be designated by national or Community law."

EU Directive 2002/58/EC on privacy and electronic communications does not contain a specific conflicts-of-law provision, but refers to Directive 95/46/EC.

The principle which gives rise to this modification is sometimes called "home state regulation", and is designed to ensure that there is no restriction on the movement of goods and services across internal borders within the EU/ EEA by requiring data controllers to comply only with the laws of their home state and not with all Member State laws.

(a) **Germany:** Accordingly, some EU Member States modify the territoriality principle if the data controller is located in another Member State or the EEA in their national laws: Sec. 1 paragraph 5 of the German Federal Data Protection Act contains a provision that German data protection law shall NOT apply where the data controller is located in another EU/EEA Member State and processes data within Germany, unless the controller has a branch in Germany.

(b) **Spain:** Other Member States like Spain have not included similar provisions and have mainly reiterated, sometimes with (apparently) slight differences, the wording of Article 4 of Directive 95/46/EC. The territoriality rule under Article 2 ("*Scope*") of the Spanish Data Protection Act is phrased as follows[1]: "*This Organic Law shall govern any processing of personal data a) when the processing is carried out on Spanish territory as part of* [vs. "in the context of"] *the activities of an establishment belonging to* [vs. "of"] *the person responsible for the processing.*"

(c) **Canada:** In *Lawson v. Accusearch*[2] the Federal Court of Canada confirmed that PIPEDA, Canada's federal private sector privacy legislation, may apply to a complaint about the crossborder flow of personal information if there is a real and substantial connection between the organization and Canada. This means that an organization that collects, uses or discloses personal information in Canada may be subject to PIPEDA even if the information is not "processed" in Canada. Determining whether there is a real and substantial connection must be done case by case, based on an assessment of the specific facts of the case.

(d) **France:** Article 5 of the amended 1978 French Data Protection Act provides that the Act applies to the processing of personal data:

> (a) if the data controller is located on the French territory; or
>
> (b) if the data controller, although not located on the French territory or in any other Member state of the EU, uses means of processing located on the French territory, with the exception of proceeding used only for the purposes of transit through his territory or that of any Member state of the EU.

1 http://www.agpd.es/portalwebAGPD/canaldocumentacion/legislacion/estatal/common/pdfs_ingles/Ley_Orgnica_15-99_ingles.pdf.

2 *See Lawson* v. *Accusearch,* [2007] 4 F.C.R. 314 (F.C.).

For cases falling under the second category, the data controller shall notify the CNIL of the appointment of a representative established in France who shall represent him for the fulfilment of the duties required by the 1978 Act. This appointment does not prevent any legal recourse that could be initiated against the data controller.

1.2 This **mixed approach** leads to conflicts of law (or in opposite cases to a lack of applicable law) because while the modified approach stops at the borders of the EEA, the data flows do not. Once data passes beyond those borders, the territoriality principle is likely to apply again. Significant areas of conflict are:

(a) Cloud Computing: There are different scenarios of Cloud Computing, but some make it difficult, if not impossible to clearly determine where the data is located at any given time. For instance, data sets (or sub-sets) may move from one jurisdiction into another jurisdiction within a millisecond, depending on the virtual space available on a server.

(b) Remote access to EU servers from the U.S. (and vice versa), and

(c) Electronic devices that physically move around the world with a person (e.g., the employee laptops and smart phones).

1.3 Some countries require that certain personal data **must be stored within a country's jurisdiction** and must not be exported without prior permission of the relevant authority.

(a) Germany: One example for this is Art. 146 paragraph 2 of the German General Tax Code (AO) that requires that bookkeeping data that may be relevant for the tax authorities must be kept within Germany. Any electronic storage outside of Germany (even within the EU) requires prior permission. Any electronic storage outside the EU is only permitted in extreme cases.

(b) Canada: There are no requirements at the federal level in Canada that personal information must be stored in Canada or that the Privacy Commissioner's approval is required before personal information may be exported from or transferred to another jurisdiction.

There are restrictions in some provinces, most notably British Columbia, that limit the ability of public bodies to send personal information out of Canada for processing by a third party. The British Columbia law requires public bodies to ensure that "personal information in its custody or under its control is stored only in Canada and accessed only in Canada." It also requires public bodies and their service providers to notify the provincial government if it receives "a foreign demand" for personal information.

(c) United States: In the U.S., privacy law has been implemented at both the federal and state levels and generally in a manner as to address specific elements of the commercial sector, rather than attempting to address all data protection matters with a single omnibus federal statute, as in the EU. Accordingly, it is somewhat difficult to generalize about U.S. privacy law. Nonetheless, generally speaking, U.S. privacy law does not focus on the national territory in which data is being physically located or stored, nor does

it restrict transfers of data to foreign countries based on the "adequacy" (or lack thereof) of those countries' data protection legal regimes. Instead, U.S. law tends to simply hold the data controller accountable under U.S. law, regardless of where the data controller chooses to physically house the data.

For example, the U.S. Federal Trade Commission (FTC) enforces the privacy provisions of the FTC Act (which prohibits unfair or deceptive acts or practices involving the privacy and confidentiality of personal consumer information), the Children's Online Privacy Protection Act (COPPA), the Fair Credit Reporting Act and the Gramm-Leach-Bliley Act. The FTC considers any company that is subject to U.S. law to be responsible for the use and maintenance of consumer information in accordance with these Acts. If a company subject to U.S. law chooses to outsource some of its data processing to a domestic or off-shore service provider, the company does not escape liability for any failure to safeguard the information adequately. In those situations, the FTC would determine whether the company that outsourced the data processing employed sufficient measures to maintain and protect the privacy and confidentiality of the data, and would consider the foreign or offshore service provider to be simply an agent of the U.S. company.

Whether a company is subject to U.S. law generally depends upon whether that company is targeting the U.S. market, rather than where the company is located. For example, a foreign-run website that is directed to children in the United States or knowingly collects information from children in the United States must comply with COPPA.

(d) Poland: A similar rule is to be found in Article 11 of the Polish Accounting Act, which requires books of account of Polish companies to be kept in Poland. However, this does not prevent Polish companies from using overseas service providers and supporting IT systems as long as the main books remain within Poland.

1.4 These legal obstacles and potentially conflicting laws can grow exponentially and become almost unmanageable for a data controller if personal data from various jurisdictions are mingled or are further transferred to third parties over which the data controller has limited or no control, such as:

(a) Cloud Computing: The Data Protection Authority of the German Federal State of Schleswig-Holstein (Unabhaengiges Zentrum fuer Datenschutz Schleswig-Holstein "ULD") recently published a white paper and a presentation that cover various data privacy aspects of Cloud Computing. The opinions expressed in the ULD's paper are not legally binding on companies operating in Schleswig-Holstein or other German federal states, but they reflect the current status of the discussion. In the paper, the ULD expresses concern that many transfers of personal data in connection with Cloud Computing arrangements will not satisfy requirements under German data privacy laws. When personal data is transferred outside of the EU in connection with the Cloud Computing services, in addition to complying with Section 11 of the Federal Data Protection Act BDSG (data processor arrangements), companies or qualified external third parties must exert "regular control" over whether Cloud Computing providers observe the restrictions of the BDSG. A mere EU/U.S. Safe Harbor certification is not sufficient, the ULD argues.

(b) Onward Transfers. The EU has had to tackle the significant problem of ensuring continued protection for EU-origin personal data when it passes outside the EU. It has done this by a mixture of contract (model clauses, BCRs) and regulatory oversight (Safe Harbor). However, this system tends to break down if the data passes into the hands of someone who is not bound by contract or regulatory supervision. Examples are:

(i) The transfer of data from an EU insured person to a US insurer under an insurance contract, which is then passed to a reinsurer in Bermuda and then to a pool of retrocessionaires in various parts of the world;

(ii) Personal data on a "trouble ticket" raised by an IT service user in the EU is transmitted to the service desk in Bangalore, which then passes it to a resolver group (e.g., in South Africa) who in turn pass it to subject matter experts (e.g., in the Ukraine).

While in theory all sub-processors are supposed to be bound by a chain of contracts to the ultimate controller or exporter, in practice this rarely happens, and the data subject has little or no control over what the ultimate transferee does with his data.

On the level of the EU Member States, Article 68 of the 1978 French Data Protection Act, as amended, provides that the data controller can only transfer personal data to a state which is not a Member of the EU only if this state provides a sufficient level of protection of individual's privacy, liberties and fundamental rights with regard to the actual or possible processing of their personal data.

The CNIL has no power to authorize the transfers to countries which have an adequate level of protection. However, the CNIL must be notified of the existence of those transfers. Such notification, however, includes an undertaking that the processing complies with the requirements of the law. When several data processing operations are carried out by the same entity and have identical or interrelated purposes, a joint notification may be acceptable.

Finally, as provided in Article 30 of the 1978 French Data Protection Act, the application to obtain authorization to transfers to countries that do not provide an adequate level of protection, and the request for a ruling the CNIL requires a significant of information:

1. the identity and address of the data controller or that of his representative;

2. the purpose or purposes of the processing, as well as, the general description of its functions;

3. if necessary, the connection, the affiliation, or any other form of relationship with other processing party;

4. the personal data processed, their origin an the categories of data subjects to whom the processing relates;

5. the period of storage of the processed data;

6. the department or unit responsible for the carrying out the processing, the individuals who, due to their functions or due to the needs of their department, have a direct access to the registered data;

7. the authorized recipients to whom the data may be disclosed;

The measures taken to ensure the security of the processing and data should also be indicated. Moreover, when applicable, any transfer of personal data which is envisaged to a country that is not a Member State of the EU in any form, must be mentioned, with the exception of processing that is used exclusively for the purposes of transit through the French territory or on the territory of another Member State (Article 5 paragraph 2 of the 1978 Act).

1.5 Moreover, some European DPAs **impose additional restrictions** on companies under the Safe Harbor Principles ("SHP") Onward Transfer Principles that go beyond the actual wording of the text: In practice, this means that if personal data are transferred from the EU to a company in the United States that is member of the SHP, and the U.S. company then wants to perform an onward transfer of the data to another company (whether inside or outside the United States), a legal basis for the onward transfer would have to be found under the law of the EU Member State from which the data were originally transferred.[3]

Spain: Instruction 1/2000 of the Spanish DPA provides that an importer of personal data must show that it is adhering to the SHP and that it is subject to the jurisdiction of the organisms listed in Annex VII of Decision 2000/520/EC. This has been interpreted to mean that the exporter of data must be able to establish that an importer has complied with these requirements, but does not have to file any document or list prior to the transfer.

France: The French CNIL indicates that where a person in France engages in a "single and non-massive transfer" of data to the U.S., which is necessary or legally required for the establishment, exercise, or defense of legal claims, the company responding to the U.S. discovery request does not need to request the CNIL's prior authorization, but should simply provide advance notice.

By contrast, "massive and repeated" transfers of data require the CNIL's authorization and are only lawful where (i) the recipient of personal data is an entity established in the U.S. that has subscribed to the Safe Harbor Scheme; (ii) the recipient of personal data has adopted standard contract clauses issued by the European Commission; or (iii) the recipient of personal data has a set of strict and binding corporate rules in place providing an adequate level of protection of personal data inside the entity.

The CNIL does not provide guidance regarding the volume of data that would trigger the need for CNIL authorization.

---

3 *Cf.* Christopher Kuner, BNA PSLR Report 2009 at 5.

Data controllers located in France and whose notifications with the CNIL mention the existence of a data transfer to a company that is a member of the SHP must provide the CNIL with the relevant extracts of the "Safe Harbor List," which enable the user to have access to the details of the self-certification of the member company. The CNIL guidelines on international data transfers, released June 2008,[4] generally require companies to file a specific annex on data transfers, which must include a listing of all recipients of the data. The notification form requires a list of all the countries of destination, together with a legal basis for the transfers.

Belgium: Belgium's Privacy Commission (Commission de la protection de la vie privée) has similar notification requirements as the CNIL: The personal data transfers must be declared by indicating the categories of data, the recipients of such data, the protection given to such data. Any transfer pursuant to the SHP would thus require a notification to the Privacy Commission (but not its prior authorization). On a more general level, Belgian law stipulates that sufficient protection for personal data can be granted through a contract between the person sending the data and the one receiving them. Such contract must be authorized by a royal decree, based on an opinion of the Privacy Commission.

1.6 Data Breaches: Lost laptops or other electronic devices with personal data that may trigger data breach notifications and various obligations in various jurisdictions.

2. ANALYSIS OF CURRENT TRENDS.

2.1 New Laws Emerge

There is no clear trend whether new countries adopting the EU model are also adopting its jurisdictional peculiarities:

(a) Mexico: After many years in development, the Mexican federal legislature passed a broad "Federal Law Protecting Personal Data in Private Possession," effective July 6, 2010. Pursuant to its Article 2, the new law covers all individuals and private corporations/ associations (moral persons) who carry out the personal data processing, except: (a) companies processing credit information, and (b) the people who process personal data exclusively for, personal use, and without the aims of spreading them or using them commercially.

(b) Canada: Although there is currently legislation before the Canadian Parliament to amend PIPEDA, the proposed amendments should not have a significant impact on electronic discovery. However, the recent Federal Court case, *State Farm Mutual Automobile Insurance Company v. Privacy Commissioner of Canada*, 2010 FC 736 (CanLII), may have an impact on the extent to which PIPEDA applies to personal information collected, used or disclosed in the context of litigation.

4 http://www.cnil.fr/fileadmin/documents/approfondir/dossier/international/Guide-tranfertdedonnees.pdf at 7, 16.

(c) **Russia:** Russia passed its Federal Law 152-FZ on Personal Data on July 27, 2006. It is modeled quite closely on the EU Data Protection Directive, but the requirement for obtaining the data subject's written consent is broader than in the legislation of most EU countries and has given rise to practical problems for Russian businesses. Like the EU, there is a requirement not to export personal data to any jurisdiction which does not provide adequate protection for those data.

(d) **Israel:** Israel's Privacy Protection Act was passed in 1981 but has since been extensively amended, most recently in 2007. The Article 29 Working Party carried out an extensive examination of Israeli data protection law and found that it guaranteed an adequate level of protection of personal data, even though it was not based on the model of the EU Directive (WP 165 of 1 December 2009). However the ratification of that decision by the European Commission has been the subject of objection following the alleged use by Israeli security forces of personal data of EU citizens in forging passports used for the purpose of the assassination of Hamas operative Mahmoud al-Mabhouh in Dubai in January 2010.

2.2 Criticism from Europe

(a) **Germany:** Mr. Weichert, the head of the DPA of the German State of Schleswig-Holstein, has demanded that the UE/US SHP be terminated because of the lackluster enforcement of the U.S. Government. According to a release issued by Germany's Independent Centre for Privacy Protection (ULD), an Australian study due to be released next month has revealed widespread compliance issues among the 2,170 U.S. companies that "claim to be safe harbor privileged," including lack of information on how to enforce individual rights, high-priced dispute resolution options and a minimal number of U.S. Federal Trade Commission prosecutions for false claims of certification. Also note ULD study on Cloud Computing mentioned above.

In addition, the *Düsseldorf Circle* (a working group of the German DPAs) released a statement in April 2010 that companies exporting personal data from Germany under the SHP must verify that the receiving company (importer) has in fact submitted a self-certification under the SHP rules and that this certification is "valid". German DPAs have criticized the United States in the past that companies that the SHP obligations are not duly enforced against companies that receive personal data from Europe.

(b) **France:** The CNIL's guidelines on e-discovery were published in August 2009 since the CNIL had noted an increase of the requests for transfers of personal data from France to the U.S. over the years. They provide guidance on data transfers in connection with U.S. civil discovery proceedings.

As of this date, the 2009 guidelines have not been followed by any action, notably from the legislator or the CNIL. In 2007, for the first time in France, a French court enforced Article 3 of the blocking statute and imposed a penalty of 10,000 € on a French correspondent of an American attorney for violation of Article 1A for acting outside the scope of the blocking statute, which allows evidence to be taken only as prescribed by applicable international conventions. The French correspondent was not a diplomatic

officer, consular agent or authorized commissioner within the meaning of the Hague Evidence Convention. The lackluster enforcement of the French blocking statutes throughout many years may explain why US courts generally deem the Hague Evidence Convention as not mandatory.

(c) **Hague Convention:** However, that criticism can be confronted with the results of the last questionnaire[5] on the enforcement practice covering the 1970 Hague Convention on the Taking of Evidence Abroad, produced by the Permanent Bureau of the Hague Conference on January 2009. Following the Special Commission's Conclusions and Recommendations of October-November 2003[6] and, to a large extent, the ABA Report on Survey of Experience of US Lawyers with The Hague Evidence Convention (October 9, 2003; section F in particular)[7] there seems to be increasing pressure on the EU Member States to modify or, at least, re-phrase the general and unspecific declarations and reservations under its Article 23, which are still significant. Most Members States have not yet made these changes, but are prepared to take a less radical approach. Spain, for example, left this possibility open in its response to the questionnaire of 2009 and expressly declared, in its previous responses to the 2003 survey, that the existence of internal procedural provisions regarding the so-called "*exhibición de documentos*" could lead to a more flexible acceptance of discovery requests.

The result of this survey also shows that a majority of the states which have made a general declaration pursuant to Article 23 of the Hague Convention seem reluctant to amend their legislation - although most of all responded that this was under review or in progress.

2.3 U.S. Courts on Foreign Data Protection Laws and Blocking Statutes

Using the *Aérospatiale* balancing test, U.S. courts are becoming more or less inclined to respect alleged difficulties in the disclosure of documents caused by data protection laws or blocking statutes; and whether it makes a difference if litigants are overseas defendants (brought unwillingly into common law litigation) or eager claimants.

Moreover, U.S. courts have determined that personal data that a company brings into the United States, for instance for the purpose of complying with SEC or DOJ requests for documents and subpoenas, can be used in a related civil litigation. Once the data is legally in the United States, the company is no longer entitled to rely on the French blocking statute to prevent the information being made available to the US litigants.

(a) *In re Air Cargo Shipping Servs. Antitrust Litig.*, 2010 WL 1189341 (E.D.N.Y. Mar. 29, 2010). Plaintiffs moved to compel defendant French Airline to produce documents. The parties did not dispute that defendant's production of documents would be a violation of France's blocking statute because no discovery request was made pursuant to a treaty. Nevertheless, the court

5 http://www.hcch.net/index_en.php?act=publications.details&pid=4700&dtid=33).
6 http://hcch.e-vision.nl/upload/wop/lse_concl_e.pdf.
7 http://www.hcch.net/index_en.php?act=publications.details&pid=3073&dtid=33.

compelled defendant to produce the documents using the *Aérospatiale* analysis finding that the interests of international comity did not weigh against the entry of the order compelling production.

(b) *Auxer v. Alcoa, Inc.*, 2010 WL 1337725 (W.D. Pa. Mar. 29, 2010). A federal court in Pennsylvania dismissed a tort action for forum non conveniens because the underlying events took place in Australia and nine out of the ten plaintiffs were Australian residents. In looking at private interest factors as part of the forum non conveniens analysis, the court found that it could not compel discovery and testimony from many non-party witnesses in Australia due to limitations in Rule 45(b)(2). Also, resorting to the Hague Convention to request foreign evidence would be a strain on efficiency and court resources because of the large number of witnesses.

(c) *In re Urethane Antitrust Litig.*, 267 F.R.D. 361 (D. Kan. 2010). Defendants objected to plaintiffs' requests to depose witnesses in Germany pursuant to Fed. R. Civ. P. 28(b) because plaintiffs could not show that the witnesses would agree to testify rather than assert testimonial privileges. The court held that the Hague Convention did not require a showing that the evidence will actually be obtained in order to approve a request. In response to further objections from defendants, the court held that the Hague Convention applied the same standards for liberal discovery as do the Federal Rules. Thus, discovery of information which though not itself admissible, may lead to admissible evidence.

(d) *AccessData Corp. v. ALSTE Tech.*, 2010 WL 318477 (D. Utah Jan. 21, 2010). Defendant, a German company, objected to plaintiff's, a Utah company, request for production of documents, including information related to customer complaints and defendant's technical support of non-customers. Defendant objected, in part, on the ground that the requests breached German privacy law. The court rejected defendant's argument because it could not point to a particular provision of German Law that would prohibit the production. The court further reasoned that even if German law prohibited such disclosure, the United States Supreme Court has held that "[i]t is well settled that such [blocking] statutes do not deprive an American court of the power to order a party subject to its jurisdiction to produce evidence even though the act of production may violate that statute." Finally, the court rejected defendant's contention that plaintiff should be required to comply with the Hague Convention's rules regarding the disclosure of private customer information because there was no danger that the discovery was sought for an improper purpose and the cost for transmitting the documents would be "relatively minimal."

(e) *Schindler Elevator Corp. v. Otis Elevator Co.*, 657 F. Supp. 2d 525 (D.N.J. 2009). Counterclaim-defendant refused to produce a witness unless counterclaim-plaintiff used procedures in the Hague Convention. Counterclaim-defendant argued that discovery under the Federal Rules only applies to document discovery, not depositions, and that noticing depositions pursuant to the Hague Convention would not cause a delay. The court held that the Hague Convention applies when a deposition is taken in a foreign country that is a party to the Hague Convention, but Federal Rules can apply when the deposition is noticed to be held in the U.S. (as in this case). The

court also found that the Federal Rules offered a stronger guarantee of promptness, and the differences between Hague Convention depositions and depositions under the Federal Rules "raise legitimate concerns about the sufficiency of a Hague Convention deposition and the specter of prejudice" to the counterclaim-plaintiff.

(f) *Gucci America, Inc. v. Curveal Fashion*, 2010 WL 808639 (S.D.N.Y. Mar. 8, 2010). Plaintiff-U.S. company subpoenaed documents regarding defendants' accounts at a Malaysian Bank from the Bank itself. The Bank refused to produce the documents citing Malaysian law. The court determined that the documents were important to the litigation, the requests were specific, the only alternative means was commencing an action in Malaysian courts which would be expensive and logistically difficult, the U.S. interest in fully and fairly adjudicating matters before its courts outweighed the Malaysian interest in protecting the confidentiality of its bank customers, the Bank had not demonstrated that compliance would impose a hardship, and that, although the Bank did not act in bad faith when it refused to comply with the subpoena, its good faith efforts did not "tilt the balance in its favor." The only factor weighing against the Plaintiff was that the documents originated outside the U.S. As a result, the court ordered the Bank to comply with the subpoena.

(g) *In re Global Power Equip. Group*, 418 B.R. 833 (Bankr. D. Del. Oct. 28, 2009). Bankruptcy claimant Maasvlakte Energie B.V., a Dutch subsidiary of a French company, refused to produce documents and witnesses located in France on the grounds that the French blocking statute prevented production. The bankruptcy court found that a comity analysis weighed in favor of applying United States discovery rules because (1) the discovery sought was "central to resolving the contested matter," (2) the requests were sufficiently specific; (3) there were no alternative means of obtaining the information, even though the party compelled to produce the documents and witnesses could face criminal penalties under the French blocking statute; and (4) the United States has an interest in "securing the prompt, economical and orderly administration of its bankruptcy cases." Because the comity analysis favored United States law and Maasvlakte had presented no evidence that it "face[d] a significant risk of prosecution if it complies with the discovery requests," the Court ordered Maasvlakte to produce the documents and witnesses.

(h) *Calixto v. Watson Bowman Acme Corp.*, 2009 WL 3823390 (S.D. Fla. Nov. 16, 2009). Pursuant to the Hague Evidence Convention, 28 U.S.C. § 1781, and Rule 28(b), plaintiff moved for the issuance of Letters of Request and a Letter Rogatory, applying for international judicial assistance to cause service of subpoenas *duces tecum* on affiliates of a defendant located outside of the United States. While the court determined the information sought by plaintiff fell within the broad scope of discovery, the court held that the information sought was likely duplicative of information already received by plaintiff. As a result and in light of comity considerations that attach to Hague Convention discovery requests, the court denied plaintiffs' request.

(i) *Seoul Semiconductor Co. Ltd. v. Nichia Corp.*, 590 F. Supp. 2d 832 (E.D. Tex. 2008). Pursuant to the Hague Evidence Convention, defendants moved for the issuance a Letter of Request to the French Government for discovery from an individual involved in the prosecution of the U.S. patent-in-suit and its French

counterpart. The court denied the motion in light of comity considerations, holding that defendants could acquire much of the desired information through other means.

(j) *Strauss v. Credit Lyonnais, S.A.*, 249 F.R.D. 429 (E.D.N.Y. 2008). U.S. victims of terrorist attacks by HAMAS sued a French bank under the Antiterrorism Act (ATA), alleging that bank provided material support to HAMAS in the form of financial services. The court denied bank's motion for a protective order compelling plaintiffs to seek discovery of documents related to bank's business with HAMAS through Hague Convention and excusing bank from producing documents protected by French bank customer secrecy laws. Applying factors announced in section 442(1)(c) of the Third Restatement on Foreign Relations Law, *Aérospatiale,* and *Minpeco,* the court held (1) requested information was crucial to litigation; (2) requests were narrowly tailored; (3) discovery originated outside United States; (4) plaintiffs lacked other methods to obtain requested material and did not have to seek material exclusively or initially through Hague Convention; (5) interests of United States and France in combating terrorism supported request, while France's opposing interest in "sovereignty" was only vaguely articulated; (6) bank would not face substantial hardship in complying with request; and (7) bank acted in good faith.

(k) *Astrazeneca v. Ranbaxy Pharm., Inc.*, 2008 WL 314627 (D.N.J. Jan. 29, 2008). Defendant in patent infringement suit sought to depose three witnesses residing in Sweden through Hague Convention procedures after efforts to produce the witnesses through voluntary cooperation between the parties stalled. Court granted defendant's request over plaintiffs' objection, finding (1) more than six months delay, during which plaintiffs promised to but did not produce witnesses voluntarily, warranted initiation of Convention procedures; (2) Swedish authorities were best-positioned to determine whether the scope of defendant's discovery request conflicted with Swedish law; (3) Convention procedures were appropriate because "unless and until the witnesses voluntarily agree to provide the requested discovery, the Hague Convention is the only way to obtain evidence from these individuals."

(l) *Emerson Electric Co. v. Le Carbone Lorraine, S.A.,* No. 05 Civ. 5042, 2008 WL 6042 (D.N.J. Aug. 27, 2008). In this antitrust action, plaintiffs sought to compel defendants, inter alia, to permit the inspection and copying of documents that one of the defendants, Le Carbone Lorraine, S.A. ("LCL"), a French corporation, produced to the European Commission during an investigation of a price fixing conspiracy involving LCL. Defendants opposed the discovery request, arguing that plaintiffs should resort to the Hague Convention for obtaining those documents. The Court granted the motion to compel because defendants had failed to identify any sovereign's interest (i.e., an interest of either France or the EU) that would be offended by the discovery. The Court noted that the scope of discovery did not appear to be so broad as to offend the European Commission or French tribunals as plaintiffs were only seeking information "LCL was already compelled to turn over to the European Commission in a case about [the] same conspiracy."

(m) *In re Aspartame Antitrust Litig*, 2008 WL 2275531 (E.D. Pa. May 31, 2008). In this antitrust class action, Ajinomoto Switzerland A.G., a Swiss corporation, objected to plaintiffs' document requests on the ground that the requests were

not in compliance with the Hague Convention. The Court noted that while Switzerland had an interest in managing discovery within its borders – as expressed by a Swiss blocking statute (Article 271, paragraph 1 of the Swiss Penal Code) requiring use of the Hague Convention – that interest was outweighed by the United States's interest in "enforcing its antitrust laws and managing litigation in the federal courts." The Court noted that "[t]his case, like many other antitrust class actions, require[d] the extensive production of discovery" and that use of the Hague Convention would be inefficient. Accordingly, the Court granted the motion to compel discovery, directing ASAG to file a motion for a protective order if it believed specific discovery requests were inappropriate.

(n) *Buttitta v. Allied Signal, Inc.*, 2010 WL 1427273 (N.J. Sup. Ct. A.D. Apr. 5, 2010). Defendant-Canadian company appealed trial judge's decision to compel discovery and impose sanctions without proper regard for the Quebec Business Concerns Record Act (QBCRA) — a blocking statute. The New Jersey Superior Court, Appellate Division, disagreed with the Superior Court's handling of the third *Aérospatiale* factor — whether the information originated in the United States. The lower court stated that this factor was "inconsequential" in every case. The Appellate Division disagreed with this statement but affirmed the lower court's determination compelling production.

(o) *Enquip Techs. Group, Inc. v. Tycon Technoglass*, S.R.L, 2010 WL 53151 (Ohio App. 2 Dist. Jan. 8, 2010). Defendants appealed the trial court's finding pursuant to the five-factor *Aérospatiale* analysis that European privacy laws (the E.U.'s Privacy Directive) and regulations do not apply to preclude the production and transfer of European documents to the U.S. The appellate court affirmed the trial court's ruling, holding that the Defendants did not meet their burden of establishing that protective order is necessary because they did not specifically identify which information is subject to the privacy laws.

3. EFFORTS TO MITIGATE THE PROBLEMS.

3.1 Sometimes, the Governments themselves recognize the problem and provide relief on **restrictions that data must be stored locally**. For instance, Germany is considering amendments to Sec. 146 AO in its Annual Tax Overhaul Law (*Jahressteuergesetz*) to give a company more flexibility as to where the bookkeeping data is stored, provided that they cooperate with the tax authorities to produce the information without delay when requested to do so.

3.2 The **EU-US co-operation on terrorist financing** is a recent example on how Governments can cooperate on international data transfers that avoids the conflict of jurisdiction. The EU and the U.S. government recently reached an agreement on SWIFT II - the renewed treaty giving the United States access to certain financial information in the EU in order to investigate terrorism. When the SWIFT database was moved to Europe, the EU agreed to allow the U.S. Treasury Department continued access to the information. The agreement was approved by the European Parliament on July 8, 2010, during its plenary session. The agreement is due to enter into force on August 1, 2010, for five years, and will be renewable year-by-year thereafter. The European Commission is also expected to commence work in the second half of 2010 on the creation of the European Terrorism Finance Tracking Program and is likely to publish a progress report within three years.

3.3 **The Art. 29 Working Party** is also in favor of a harmonized data protection regime. Their July 2010 paper on accountability suggests a new worldwide principle on accountability which would require data controllers to put in place appropriate and effective measures to ensure that the principles and obligations under the EU Data Protection Directive are complied with and to demonstrate this to supervisory authorities upon request. In order to achieve this, the data controller would be required to comply with "specific requirements" such as the obligation to perform privacy impact assessments in given cases, or the appointment of data protection officers. This principle may require the "establishment of internal procedures *prior* to the creation of new personal data processing operations (internal review, assessment, etc.)." In addition, the data controller is expected to adopt certain internal policies and processes (e.g., staff training) that are necessary to implement the data protection principles under the Directive. Controllers should also ensure that the practical measures implemented to comply with data protection principles are effective.

3.4 Several members of the **Asia Pacific Economic Cooperation (APEC) forum** have recently developed a cross-border privacy enforcement arrangement. The arrangement provides a framework for participating enforcement authorities, including the Federal Trade Commission and the Canadian Privacy Commissioner, to assist one another with privacy enforcement investigations and enhances information sharing among the participants. More generally, the APEC member economies are developing a self-regulatory framework to protect consumer data transfers throughout the APEC region. This framework is referred to as the "APEC cross-border privacy rules."

3.5 In 2007, the **Organization for Economic Co-operation and Development Council** adopted a "Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy." The Recommendation reflects a commitment by governments to improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities, as well as to provide mutual assistance to one another in the enforcement of privacy laws. The Global Privacy Enforcement Network (GPEN) is one outcome of the Recommendation. GPEN's members, from the Asia-Pacific region, North America, Europe and the Middle East, have agreed to share information about privacy enforcement issues; co-operate on outreach activities; and facilitate effective cross-border privacy enforcement.

3.6 The **FTC** participates in a privacy enforcement cooperation arrangement with authorities of the other members of the Asia Pacific Economic Cooperation forum (APEC). The arrangement provides a framework for participating agencies to assist one another with privacy enforcement investigations and enhances information sharing among the participants. Within APEC, the FTC also actively promotes an initiative to develop a self-regulatory framework governing the privacy of consumer data transfers throughout the APEC region. This framework is also referred to as the "APEC cross-border privacy rules."

3.7 **U.S. Protective Orders:** As the scope of discovery has expanded over the years, the use of protective orders has increased as a counterbalance to the threats such discovery can pose to privacy. For instance, information that is deemed "privileged" (e.g. client-attorney communication) will not be disclosed. In addition, Fed. R. Civ. P. Rule 26(c) provides that a federal court may issue a

protective order "for good cause...to protect a party or person from annoyance, embarrassment, oppression, or undue burden or expense." Such protective orders are frequently used to protect trade secrets (which could include such data as customer databases) and a wide variety of other types of private or sensitive data. The U.S. Supreme Court has held that the "good cause" standard in Rule 26(c) is satisfied if the protective order serves to curb abuse stemming from liberal discovery; it further held that an order protecting privacy establishes good cause and is sufficient to overcome a First Amendment challenge. Sometimes parties can even obtain from a judge an "umbrella protective order" that presumptively protects any data disclosed in discovery that is marked "confidential" by either party. Protective orders can in some circumstances be vacated or superseded through subsequent legal proceedings, and the extent to which this is the case can vary between jurisdictions.

4. CONCLUSION

4.1 The current territoriality regime for personal data leads to a lot of confusion and potentially conflicting laws and regulation. "Accountability", as suggested by the Working Party, means that data controllers put in place "appropriate and effective measures" to ensure that the principles and obligations under the EU Data Protection Directive are complied with. In order to achieve this, they need to know which law applies.

4.2 More uncertainties are added because the term mere "data transfer" (or transit) through a country is not clearly defined and gives room for various (potentially conflicting) interpretations.

4.3 Data processors that use decentralized storage methods (e.g., cloud computing) may face incalculable legal risks, for instance being sued under different national laws where the data is located if a data breach occurs, or being subject to national laws to produce the data for law enforcement purposes. The German ULD proposes new Binding Corporate Rules (BCRs) for Cloud Computing as a solution that may need further discussion.

4.4 One potential solution to be discussed is that the applicable law is no longer defined by the territoriality principle (that is, as described, already watered down in the national laws in the EU), but follows an individual wherever the data and/or the individual moves. This concept is already accepted under various conflicts-of-law provisions for names - potentially the most important datum of an individual. For instance Art. 10, paragraph 1 of the German Amendments to the Civil Code (EGBGB) stipulates that "the name of a person is determined by the jurisdiction of the country to which the person belongs" - the provision also applies to the business name of a company. This principle that the law follows the individual may provide relief in a situation where a business in the EU processes data of an individual who is in a "non-adequate" jurisdiction. Due to the territoriality principle, the personal data of this individual will be protected to the same extent as personal data received from another EU Member State. As a consequence, EU data protection law will apply when the data is repatriated to this country. In other words, the level of data protection may be higher for this individual in the originating country than it would be if the data hadn't been transferred to the EU.

4.5 Before we embark upon a discussion of extraterritorial "jurisdiction" as it relates to personal data, it may be important to clarify which type of "jurisdiction" we are talking about, as the term can mean many different things as it relates to transborder movement of data. Certainly any sovereign nation, within the framework of its international obligations, is entitled to prescribe or legislate on matters that affect its territory. The stumbling block appears to be, how do we enforce these rights?

4.6 The EU and the US Government should try to resolve the differences concerning the differences in the interpretation of the SHP (onward transfer, enforcement of the SHP) as soon as possible, e.g., in the framework of the dialogue on the EU/US Digital Agenda.