RESOLVING DATA-PRIVACY CONFLICTS IN CROSS-BORDER INVESTIGATIONS AND LITIGATION
AUGUST 8 2014

By: Paul Callaghan
1. Introduction

1.1 We communicate, collaborate and conduct business more globally than ever before and increasingly transact business in electronic format over the internet, via telephone, voicemail, facsimile, email, instant messaging, social networks, text messaging, blogs, wikis, and social networks. With such a connected, global economy and the increasing use of the Cloud to store data, U.S. companies are storing more documents than ever before on European based servers. Similarly U.S. employers increasingly operate abroad through subsidiaries, offices, affiliates, secondees and branches notably in Europe. When a U.S. company become embroiled in litigation, inevitably plaintiffs and investigators will seek data and testimony from those European based entities.

1.2 Unfortunately the European and U.S. legal systems unavoidably clash when a U.S. entity is asked to produce documents in the course of litigation that are physically or electronically in Europe. What do you therefore do if your client, a U.S. company, is issued with a non-party subpoena in a U.S. based litigation for documents located on the server of a subsidiary company based in Europe such as Germany or the U.K., countries that are protected by local data protection laws. If disclosed you risk fines for breaching European data protection laws but failure to disclosure will result in the contravention of the Discovery request. This cross-border conflict is not easily resolved due to the protective policies of Europe and refusal by the U.S. Courts to recognise European data protection rules. This paper seeks to highlight the issues with cross-border discovery and suggest practical steps U.S. Counsel should take if they become embroiled in such a situation.

2. Differences between the U.S. and European Discovery Process

2.1 The U.S. Discovery procedure requires litigants to produce any requested information under their control without regard to whether such information originated or is still within U.S. borders. The U.S. rules for disclosure are provided in the Federal Rules of Civil Procedure (the "FRCP") which applies a 'pre-trial Discovery' process to gather evidence once a law suit is filed. This ensures the free flow of information, maximises truth-finding and the exchange of information between parties. Disclosable information does not need to be admissible, just relevant to a party's claim or defence and reasonably calculated to lead to the Discovery of admissible evidence.

2.2 The European system of Discovery is very different fundamentally due to the conflicting common law system of the U.S. and the predominantly civil law systems of Europe. From a European perspective the U.S. approach to Discovery is considered extremely broad which in part explains the European reluctance to participate in U.S. Discovery. Europe considers the U.S. system intrusive and alien particularly given that the parties themselves gather the relevant evidence. Most European countries appoint a Judge to carry out the Discovery process, as he/she is considered sufficiently experienced to identify relevant documentation and information. The contempt that some European jurisdictions have for the U.S. Discovery system, has led to blocking statutes being enacted to specifically 'block' U.S. Discovery applications within its borders.

2.3 Europe has also made it clear that the U.S. lacks sufficient data protection laws. Data privacy is a fundamental human right of citizens residing in the European Economic Area as enshrined by Article 8 of the European Convention on Human Rights. In 1995, the European Union's Data Protection Directive (the "Directive") was issued by the European Union providing that Personal Data can only be gathered legally and under strict conditions for a legitimate purpose (to date, 28 Members States have implemented the Directive). Whilst this was the prescribed minimum amount of data
protection required, it was left to the discretion of each Member State to implement the
Directive and provide for a stricter regime if wanted. Some Member States including
France, Germany and Italy have chosen to implement significantly more stringent data
protection laws than required. This freedom has led to differing data protection
practices across Europe resulting in fragmented European rules on data protection.
Such differences make it more complicated for a foreign entity to understand how to
undertake the process of obtaining documents from Europe for the purpose of a
Discovery process and it is recommended that U.S. based companies check the data
protection rules of each European country in which it stores data through a subsidiary
or otherwise.

3. Data Privacy Laws in the E.U.

3.1 The Directive states as follows:

(a) Member States shall protect the fundamental rights and freedoms of natural
persons, and in particular their right to privacy with respect to the processing of
Personal Data.

(b) Member states shall neither restrict nor prohibit the free flow of Personal Data
between Member States for reasons connected with the protection under
paragraph [3.1(a)] (above).

3.2 The Directive defines 'Personal Data' as "any information relating to an identified or
identifiable natural person", meaning data that allows someone to identify a 'Data
Subject', directly or indirectly. This can include any information about an individual
including family details, medical records, financial information, and (particularly
relevantly) employment information. In addition the Directive provides for a separate
class of 'Sensitive Personal Data'. Sensitive Personal Data is that which reveals "racial
or ethnic origin, political opinions, religious or philosophical beliefs, trade-union
membership, and the processing of data concerning health or sex life".

3.3 The Directive labels any entity that collects and controls Personal Data as a
'Controller'. A Data Controller must comply with a number of principles when
processing Personal Data:

(a) Process the data fairly and lawfully.

(b) Collect data only for specified, explicit and legitimate purposes, and not to
further process it in any manner incompatible with those purposes.

(c) Collect and store data only to the extent that is adequate, relevant and not
excessive in relation to the purposes for which it is collected and further
processed.

(d) Ensure that all data held is accurate and, where necessary, kept up to date.

(e) Not to keep data in a form which permits identification of data subjects for
longer than is necessary for the purposes for which the data was collected or
for which it is further processed.

3.4 In addition, one of the following must be accomplished for the data processing to be
considered legitimate:

(a) The Data Subject must have given their unambiguous consent.

(b) The performance of a contract to which a Data Subject is a party.
(c) Comply with a law.
(d) Protect the Data Subject's vital interests.
(e) Advance public interest or facilitate the exercise of an official authority.
(f) Further the Data Controller or another disclosed party's legitimate interests without infringing the Data Subject's fundamental rights and freedoms.

3.5 The restriction on processing data clearly poses a problem for U.S. litigants that require European based data. Clearly the Directive restricts the scope of discoverable data and data processing includes virtually any steps that a party to U.S. litigation would need to take to prepare for trial.

3.6 In addition there is a general prohibition on the transfer of Personal Data to a country outside the European Economic Area, unless said country provides an 'adequate level of protection'. Though some named countries are deemed to provide an adequate level of protection to European data, the U.S. is not one of those countries. There are times when Personal Data may be transferred outside of Europe which are as follows:

(a) When the data subject gives their consent clearly and freely, though this consent may subsequently be withdrawn.
(b) When the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller.
(c) When the transfer is necessary for the performance of a contract concluded in the interest of a Data Subject between the Data Controller and a third party.
(d) When the transfer is for reasons of substantial public interest. This a high threshold most likely to be met for the purpose(s) of crime prevention.
(e) When the transfer is necessary to protect the vital interests of the Data Subject.
(f) If the data is on a public register, as long as the recipient complies with any restrictions on use of the data.
(g) When necessary in connection with legal proceedings, to get legal advice or to establish, exercise or defend legal rights. On the face of it this exception would seem to provide U.S. Counsel with an opportunity to access Personal Data for litigation purposes. However (as explained later) the E.U. has issued guidance that this provision must be interpreted restrictively and that entities seeking to rely on it must transfer the data through the Hague Convention.

If a non-European country does not offer an adequate level of data protection, Member States are required to take positive steps to prevent the transfer of personal data to such a country.

3.7 The European Union and the U.S. negotiated a 'safe harbour' mechanism by which a U.S. based company could voluntary increase its level of data protection and become eligible to receive data transfers from the European Union. However for our purposes safe harbour is only so useful as it does not cover all sectors of data and imposes restrictions on data processing.

3.8 Each Member State is entitled to lay down its own sanction(s) for a breach of the Directive. Most States have opted to fine those in breach of data protection rules but some have provided for criminal sanctions including possible custodial sanctions for severe breaches. Previous examples of fines have included €100,000 against Google
by the French data protection authority for storing Personal Data in contravention of the Directive, and the U.K. Information Commissioner's Office fine of £440,000 levied against the owners of Tetrus Telecoms. Clearly the consequences for breaching the data protection rules are severe and potentially expensive.

4. European case law

4.1 A recent European case involving Google provides an interesting illustration of the extent to which the European Union will go to protect its citizens fundamental right to privacy. A Spanish national, Mr Costeja Gonzalez, asked Google to remove some personal data previously published by a Spanish newspaper about a now-resolved lawsuit from 1998 that was brought up by typing his name into the search engine. Mr Gonzalez felt this was a breach of his privacy rights and asked Google to remove or conceal the material. Google refused. Mr Gonzalez notified the Spanish Data Protection Authority which also asked Google to remove the material on the basis that search engines are subject to data protection legislation as they do carry out data processing. Google again refused and the matter went before the European Court of Justice which ruled that:

(a) the collection, storage and use of Personal Data was classified as processing of Personal Data and Google was therefore a Data Controller;

(b) Google was subject to the Spanish data protection rules because it had a presence in Spain with which it promotes and sells advertising space and actively targets users in Spain;

(c) in order to comply with the Directive if so requested by the individual Google should remove the results of a search against an individual's name; and

(d) in this instance the individual's rights outweigh the economic interests of Google and the public's interest in finding such information.

4.2 The ruling of the ECJ in this matter made it clear that all European citizens have the 'right to be forgotten', even by a search engine which is displaying information from a third party. Citizens of Europe have the right to have publicly available information removed if it is 'inadequate, irrelevant or no longer relevant', but this right will be balanced against the public interest in the information. Google naturally fear that there will be a flood of right to be forgotten requests, especially considering Google accounts for around 90% of all online searches conducted in the European Union. However, Google will not automatically have to remove information about an individual upon receipt of such a request. The individual will have to show his/her privacy rights triumph any public interest. Nevertheless this case demonstrates Europe's commitment to data privacy and willingness to impose strict rules to protect it.

5. Data Privacy in the U.K.

5.1 The U.K. like the U.S. is a common law jurisdiction. In contrast to other European Member States, it has strict, written rules regarding its pre-trial Discovery or 'disclosure' process. These rules stem from Lord Woolf’s 'Access to Justice Report' published in 1996 in which he suggested a number of reforms to the U.K. Court system. Many of these proposed reforms were incorporated into U.K. law in 1998 by the Civil Procedure Rules (the "CPR"). The overriding aim of the CPR is to deal with litigation 'justly'. This includes ensuring the parties to litigation are on an equal footing. The CPR provides a number of 'Practice Directions' which a party to litigation must follow or face severe costs orders, adverse inference of fact, a Court Order compelling disclosure, a
strike out of a claim/defence, a finding of a criminal offence or a finding of contempt of court.

5.2 The obligation of disclosure in the U.K. is very broad to ensure that parties 'put their cards on the table', in keeping with the key objective of the CPR. A party to litigation must conduct a reasonable and proportional search (the require to act proportionally has been given even greater credence by the 2013 Jackson Reforms which encourage greater costs transparency) for relevant documents that are in their physical control or for which they have a right to possess or inspect, and must then disclose all documents that help and hinder their case. Again this is in contrast to other European States that require litigants to only produce documents upon which they rely. Documents to be disclosed includes electronic documents, indeed anything which records information such as Meta data. A party to whom a document has been disclosed is entitled to inspect that document unless it is no longer in the disclosing party's control or privilege applies. In addition a party may make an application to the Court for Specific Disclosure of a particular document. This duty of disclosure continues until the proceedings are concluded meaning any new relevant material which surfaces or is created by a party must be disclosed, even if the trial has begun.

5.3 Lawyers in the U.K. owe an independent duty to notify their client of the need to preserve disclosable documentation and to ensure that proper disclosure is undertaken by their client(s). When engaged legal representatives should inform their client(s) in writing of their disclosure obligations under the CPR. As soon as litigation is commenced or is 'reasonable anticipated' steps should be taken to preserve relevant information both in electronic and hard copy format.

5.4 Other statutes in the U.K. to be considered for data protection purposes include the Data Protection Act which incorporated the Directive into U.K. law and the Human Rights Act which incorporated Convention for the Protection of Human Rights and Fundamental Freedoms into U.K. law. The Regulation of Investigatory Powers Act 2000 ("RIPA") regulates the power of public bodies to carry out surveillance and investigations, and the interception of communications in the U.K. and was enacted in direct response to the technological changes seen in the last 20 years and growing threat of terrorism. RIPA granted public bodies certain powers when investigating cases involving terrorism, crime and public safety. It granted powers to the government to demand that keys are handed over to access protected information, force internet service providers to fit equipment to facilitate surveillance, and demand an ISP provider provide secret access to a customer's communication. The powers granted by RIPA are clearly not in line with the aims or sentiment of the Directive, but is power that the U.K. government has deemed necessary to protect the country in the event of crime and particularly a terrorist attack.

6. Proposed amendments to European data privacy laws

6.1 In January 2012, the European Commission released a paper called the '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' (the "Draft Regulation") in which it proposed a multitude of reforms to the Directive, primarily seeking to harmonise the inconsistent data protection rules across Europe. It proposed that the Draft Regulation should be automatically enshrined into the law of each Member State, meaning that unlike the implementation of the Directive there will be no opportunity for Member States to adopt different approaches and rules. Data processors are proposed to be specifically included within the scope of the Draft Regulation. This new approach would mean that U.S. companies operating in Europe could no longer pick a regime in which to place its subsidiary on the basis of its favourable data protection laws. Thereby making a U.S.-European Discovery request even more complicated.
6.2 The Draft Regulation provides that Personal Data may only be transferred to a non-European country or to an international organisation on the basis of one of a number of limited conditions, including:

(a) A European Commission finding of adequacy.

(b) If appropriate safeguards, for example, binding corporate rules or standard contractual clauses, are in place.

(c) If one of the following derogations are met:

(i) The individual has consented to the transfer.

(ii) The transfer is:

(A) necessary to perform a contract with the individual, or to take steps at his request with a view to entering into a contract with him, including employment contracts;

(B) necessary for the conclusion of a contract between the Data Controller and a third party that is entered into at the request of the Data Subject; or

(C) in the interests of the Data Subject, or for the performance of such a contract.

(iii) The transfer is necessary for important grounds of public interest (for example, crime prevention or detection).

(iv) The transfer is necessary for the establishment, exercise or defence of legal claims.

(v) The transfer is necessary in order to protect the vital interests of the Data Subject or of another person, where the Data Subject is physically or legally incapable of giving consent.

(vi) The transfer is made from a public register intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest (for example, the electoral roll or the register of companies directors).

(vii) Is a one-off or infrequent transfer which is necessary for the purposes of a legitimate interest pursued by the Controller or the Processor, where the Data Controller or Processor has assessed all the circumstances surrounding the data transfer operation or the set of data transfer operations, and based on this assessment has (where necessary) adduced appropriate safeguards with respect to the protection of Personal Data.

6.3 The Draft Regulation also recognizes a Data Subject's 'right to be forgotten'. This means that an individual would be able to request that a company erases all Personal Data held about him/her. An ex-employer that receives a right to be forgotten request from an ex-employee will face a huge administrative burden in complying. Currently it is not clear from the Draft Regulation how this will work in practice. More interestingly for our purposes, in an instance where a party to U.S. litigation is asked to disclose documents that have been erased by a European subsidiary as a result of a right to be forgotten request, it would be impossible to comply with the Discovery order. Important
employment documentation such as employment contracts, emails, meeting notes, Human Resources records, salary information and other potentially key documentation will all need to be erased upon receipt of a right to be forgotten request.

6.4 The proposed level of sanction for breaching the Draft Regulation will be dependent on a number of factors including the gravity of the breach and whether the breach was intentional or accidental. Initially the following fines were proposed:

(a) Fines of up to €250,000 (or up to 0.5% of the organisation's annual worldwide turnover) for intentionally or negligently failing to operate a proper subject access request mechanism, failing to respond promptly (or in the correct format) to subject access requests, or charging a fee for responding to such requests.

(b) Fines of up to €500,000 (or up to 1% of annual worldwide turnover) for intentionally or negligently failing to respond to subject access requests in a manner which complies with the Draft Regulation. The provision sets out a variety of ways in which an organisation might commit such failure, including by refusing access, providing only partial data or failing to consult with joint controllers of the information.

(c) Fines of up to €1 million (or up to 2% of annual worldwide turnover) for other compliance failures, such as processing without a sufficient legal basis, failing to comply with the more stringent regime applicable to special categories of data, and risky types of processing such as profiling, failing to notify data breaches, transferring data to a territory without ensuring appropriate safeguards or failing to designate a data protection officer.

Since the Draft Regulations were published, it has been suggested that the maximum fine may be increased to as much as 5% of a company’s annual turnover. These higher fines will make the decision as to whether a U.S. party to litigation contravenes European data protection law or a Discovery request even more difficult.

7. Implications of European Data Privacy Laws in the U.S.

7.1 As stated above the strict data privacy rules in Europe are in stark contrast to the broad scope of Discovery in the U.S. The FRCP provide that parties can obtain non-privileged information "relevant to any party's claim or defense", furthermore "the court may order Discovery of any matter relevant to the subject matter involved in the action". A party to litigation is entitled to serve a request on the other side for Discovery of data (including electronically stored information) "in the responding party's possession, custody, or control". U.S. Courts have construed the notion of 'control' widely to include the subsidiaries of a party to litigation. The FRCP imposes the following sanctions for contravening a Discovery request:

(a) directing that the matters stated in the order or other designated facts be taken as established for purposes of the action, as the prevailing party claims;

(b) prohibiting the disobedient party from supporting or opposing designated claims or defenses, or from introducing designated matters in evidence;

(c) striking out the pleadings in whole or in part;

(d) staying further proceedings until the order is obeyed;

(e) dismissing the action or proceeding with them in whole or in part;
(f) rendering a default judgment against the disobedient party; and/or

(g) treating as a contempt of court the failure to obey any order except an order to submit to a physical or mental examination.

Clearly these sanctions are severe for a party unable to comply with a Discovery request.

7.2 There has also been a significant amount of European case law on data privacy, for example in Copland v U.K., 62617/00 [2007] ECHR 253, 42 (3 April 2007), the European Court of Human Rights held that employee emails sent and telephone calls made at work should be private. Monitoring of communications made at work was deemed to be in breach of an employee’s right to privacy. This is particularly relevant for a U.S. company seeking disclosure for employment litigation. Information such as whom an employee communicated with at work, his/her employment contract, his/her appraisals, etc may be documents that are absolutely key in employment litigation. A stark example of the difficulty this creates was seen in the case of In re Advocat "Christopher X", Chambre Criminelle [Cass. Crim.] Paris, Dec. 12, 2007, Juris-Data [No. 2007-332254] in which a French attorney instructed by an American law firm was fined €10,000 in criminal penalties for contravening a French ‘blocking statute’ by attempting to collect data in France for the purposes of U.S. based litigation.

7.3 U.S. Courts have in the main given precedence to the FRCP when there is a clash with European data protection laws. For example, in Société Nationale Industrielle Aerospatiale v. U.S. Dist. Ct. for the S. Dist. of Iowa, 482 U.S. 522 (1987), the U.S. Supreme Court rejected the idea that the Hague Convention was the only legal means of carrying out a Discovery process in a foreign jurisdiction. The Court held that there was no ‘rule of first resort’ to the Hague Convention required to maintain respect to the principle of State Sovereignty. The Court suggested applying the following test to determine issues of international mutual courtesy in litigation:

(a) The importance of the documents or information requested to the litigation process.

(b) The degree of specificity of the request.

(c) Whether the information required originated in the United States.

(d) The availability of alternative means of retrieving the information.

(e) The extent to which non-compliance with the request would undermine the important interests of the U.S. or those important interests of the state where the information is located.

This case has been widely applied by the U.S. Courts and has placed the burden on respondents to persuade a U.S. Court to give precedence to the Hague Convention over the FRCP. There have also been examples of U.S. Courts ordering that Discovery should take place via the Hague Convention, for example in re Vivendi Universal, S.A. Securities Litigation, U.S. District Court for the Southern District of New York.

8. The Hague Convention

8.1 The Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters is a multi-lateral treaty. Signatories of the Convention allow, in varying degrees, the taking of evidence and Discovery of documents on their territory. A party seeking disclosure must send a Letter of Request to the Central Authority of that State.
from their national Court. The Letter of Request will then be sent to the appropriate judicial body which in turn is under an obligation to deal with it expeditiously and is only able to refuse in specific cases. A Letter of Request can only be used if the evidence it seeks is going to be used in judicial proceedings. The Letter of Request must include specific information such as the authority requesting, names and addresses of the relevant representatives and the evidence required, and it must be in the language of the body requested to execute it or with a translation into that language. There are limits on the pursuit of evidence through the Hague Convention, for example Letters of Request cannot be executed if the information is sought for the purpose of obtaining documents for pre-trial Discovery.

8.2 By relying on the Hague Convention a litigant can comply with both the Privacy Directive and U.S. Discovery requirements by lawfully producing only non-personal data or fully producing all relevant information (including persona data) pursuant to the order of an E.U. State. This can be justified when ‘the transfer is necessary...for the establishment, exercise or defence of legal claims’ and personal data is allowed to be requested if ‘necessary for a legal obligation to which the data controller is subject’, i.e. that of the Member State. The personal data would still need to be processed in accordance with the protections laid out above.

8.3 The vast majority of European countries are signatories to the Hague Convention, as is the U.S. It is best practice and highly advisable for the litigant to appoint local Counsel to deal with the Letter of Request, as, for example in the U.K., a Treasury Solicitor will otherwise deal with the matter often with little sense of urgency.

8.4 There are several hurdles to conducting U.S. Discovery via the Hague Convention, as follows:

(a) An entity involved in a Discovery process will still need to persuade a U.S. Court to use the Hague Convention as opposed to the FRCP. Whilst the Hague Convention has been ratified by the U.S. and is therefore U.S. law, it was meant as a supplement not a pre-emptive replacement. A three stage test is applied by the U.S. Courts to determine which process to use, which is as follows:

(i) The particular facts of the case, with particular regard to the nature of the Discovery requested: The Courts tend to favour the Hague Convention when Discovery requires broad, rather than narrow, tailored responses because U.S. Courts will try to avoid an undue burden on foreign litigants.

(ii) The sovereign interests in the case: If the relevant State has previously stated its opposition to the FRCP Discovery method, it is more likely that the Court will use the Hague Convention process.

(iii) The likelihood that the Hague Convention procedures will be effective.

(b) The person(s) whom the executing country needs to gather evidence from may refuse to give the evidence under the law of the State.

(c) If the Hague Convention method is used and the Court is not satisfied with the evidence obtained, the Court can then order subsequent production under the FCRP.

8.5 There are clear drawbacks with relying on the Hague Convention:

(a) The process can take time, as long as 6 – 12 months. Local counsel should be appointed to help speed up this process.
Some signatories to the Hague Convention refuse to execute Letters of Request that seek Discovery pre-trial, as they see this as fishing for information. Some Member States including France, Germany and Spain have in fact made a reservation that the Convention may not be relied upon for pre-trial Discovery proceedings. It may not be used just to find out what documents may be in the possession of the other party to proceedings.

Letters of request are often rejected due to a lack of specificity and/or proper scope.

9. A protective order on the basis of E.U. data protection law

9.1 U.S. Court can sometimes grant a protective order releasing a party from its obligation to produce evidence, if that party can provide evidence of sufficient particularity and specificity to allow the Court to determine whether the Discovery sought is indeed prohibited by foreign law. It is advisable to provide a statement from the relevant country that its law actually bars disclosure of the information. The Court will consider five factors when determining whether a protective order should be granted:

(a) The importance to the investigation/litigation of the documentation sought: A particular consideration is whether the document(s) help or harm the applicants' case. If it is harmful the Court is less likely to grant a protective order.

(b) The degree of specificity of the request: If the request is particularly burdensome on the requestee it is more likely to be refused.

(c) Whether the information sought originated from the U.S.: If the information sought is entirely unavailable in the U.S., a protective order is more likely to be refused.

(d) Whether there are any alternative means of securing the information.

(e) The extent to which refusal to grant the request would undermine interests of the U.S./Member State: The Court will seek input from the relevant foreign jurisdiction on this point and it is advisable for the party seeking the protective order to produce such evidence.

Generally the U.S. Court will look favourably upon an applicant that strives and makes good faith efforts to comply with the Discovery process.

9.2 The Court has significant discretion in granting a protective order, including the power to turn it down even if a conflict exists. U.S. Courts have proved willing to grant protective orders in the past and this can be an effective way to avoid conducting a European Discovery process.

10. Exceptions in the Directive

10.1 If it is unable to obtain a protective order a litigant may seek to rely on exceptions to the Directive in order to comply with a Discovery order. The first step is establishing that there is an exception to the transfer rules in Article 25 that justifies processing. The exceptions to the Directive are stated to be interpreted narrowly and strictly, and should only be relied upon where risk to a Data Subject is small. The exceptions are as follows:
(a) If the U.S. entity to which the data is being transferred is participating in the Safe Harbour programme this creates a presumption of adequate data protection standards and data transfer is allowed. If the litigant is therefore part of the Safe Harbour programme it could receive relevant data from a European entity. However any further transfer to other litigant(s) or the Court would be an additional transfer, something specifically prohibited in the Safe Harbour principles. This method will only therefore be of use in very limited circumstances. Furthermore Member States are entitled to disapply this exception in some circumstances.

(b) The Directive allows a transfer of data where the Data Controller 'adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals', for example contractual clauses and binding corporate rules:

(i) To qualify under this exemption, a contractual clause must document 'how the responsibility for data protection compliance is split between the two parties [and] provide additional safeguards for the data subject made necessary by the fact that the recipient in the third country is not subject to an enforceable set of data protection rules providing an adequate level of protection'. The clause must clearly document how the data will be protected and what action a Data Subject can take in the event the company breaks the data protection requirements. There are standard, template contracts available for this purpose. There must be a supervisory body in the country which is the recipient of the data and the authorities of the relevant country must not be able to access the information beyond that 'permitted by internationally accepted standards of human rights protection'. As above, it is likely that the U.S. would fall short for this second requirement as the civil and common law systems are so opposed and this exception could not therefore be relied upon.

(ii) Binding corporate rules are most suited where the transfer of Personal Data is taking place within one multinational company. The relevant national data protection authority must approve of the transfer, which in turn will only approve the transfer if they are binding in the U.S. There should also be provisions for audits, co-operation with the relevant authorities, a detailed complaint handling department redress mechanisms for Data Subjects and available compensation for Data Subjects whose privacy is breached. As above, the litigant would not be able to transfer data on to a third party such as the U.S. Court and this exception is therefore of little use beyond a multinational building up awareness of what relevant materials it has for litigation.

(c) If the Data Subject gives his/her express consent to the transfer, such a transfer will be legitimate. To be valid consent the following is required:

(i) consent cannot be implied;

(ii) consent can be withheld without the Data Subject coming to harm;

(iii) the Data Subject retains the right to withdraw consent at any point;

(iv) the consent must be specific in regard to the exact data being transferred;

(v) information must be provided to the Data Subject regarding the identity of the recipient and the purpose of the transfer;
(vi) the Data Subject must be made aware of the risk involved with the transfer of the data;

(vii) consent must be given prior to the transfer;

(viii) consent must be obtained from each Data Subject; and

(ix) the consent must be freely given, specified and informed.

If a litigant can obtain consent under the above conditions, it has a legitimate way to obtain data for the purpose of U.S. Discovery. However, the Data Subject is entitled to withdraw their consent at any time and there is a risk that such consent will be withdrawn during the Discovery process, pre-trial or at trial. When such consent is withdrawn all relevant Personal Data must be deleted. U.S. Courts are unsurprisingly reluctant to agree to this and be placed at the whim of a third party. In the past U.S. Courts have stated that releasing documents on the basis of consent is not a valid means of production as it can 'limit the information obtainable'. Consent therefore has limited use for a U.S. Discovery process.

(d) There is another exception for allowing data transfer where it is necessary 'for the establishment, exercise or defence' of a legal claim. The claim must be in motion (not anticipated) and the Hague Convention must be complied with. This exception was intended to cover cross-border litigation, particularly in the example where a U.S. based parent company of an internationally based business is being sued by an (ex-) employee of a European based Group Company. Clearly the same limiting factors apply here.

10.2 If any exception is relied upon by a U.S. litigant, they must still ensure that they do not contravene other parts of the Directive, for example if Data is transferred under the Safe Harbour rules, the processing must still be justified under the Directive requirements. Such justification for the purposes of U.S. Discovery can include:

(a) That it is 'necessary for compliance with a legal obligation to which the data controller is subject', this cannot be a U.S. obligation, it must be enforced by a European authority, usually pursuant to a Letter of Request sent under the Hague Convention.

(b) That there is unambiguous consent of the data subject. As above such consent must be freely given, specific and informed.

(c) The processing is 'necessary for the legitimate interest pursued by the Data Controller', including a multi-national entity that needs to comply with a U.S. Discovery request. The interests of the Data Controller must be more persuasive that the fundamental right of the Data Subject.

11. Blocking Statutes

11.1 Blocking statutes have been put in place by many European countries with civil legal systems. Such statutes limit the requirement to produce documents held in that jurisdiction to foreign courts. Blocking statutes are intended to protect the civil law system and sovereignty of that Member State. Blocking statutes are either procedural (Discovery orders are to be resisted unless they comply with procedures provided by that country such as the Hague Convention), discretionary (a national body can approve or reject Discovery orders), industrial (Discovery orders will be resisted if they relate to certain named industries – often for the purpose of national security) or a mix.
Blocking statutes are in place in Italy, the Netherlands and Sweden, as well as France and Switzerland as discussed below.

11.2 France has executed a blocking statute which criminalizes the act of exporting information about Data Subjects to the U.S. (and other non-European countries) in the course of litigation, seeking to force foreign litigants to respect French sovereignty. It is broad in scope and application, applying to any Discovery process seeking to recover documents located in France. A U.S. party to litigation which has documents in France relevant to a Discovery process should rely on the Hague Convention. Contravention of the French blocking statute can result in imprisonment for up to six months and/or a fine of up to €18,000. The French Courts have proved themselves willing to convict lawyers who breach the blocking statute. It will therefore be extremely difficult for a U.S. litigator to find a lawyer based in France to breach the blocking statute. At the same time U.S. Courts have not looked kindly upon respondents relying on blocking statutes to refuse disclosure. U.S. counsel must therefore be careful to avoid relying on blocking statutes, and to distinguish them from European data privacy rules.

11.3 Switzerland also has a blocking statute in place to protect national sovereignty and avoid any circumvention of international legal aid, by requiring U.S. authorities to engage with Swiss authorities. If a foreign state, foreign official or someone who performs such actions for a foreign party aids or abets the breach of the Swiss blocking statute they will be punished by up to three years in prison or by a fine. So, as detailed above in the event that documents located in Switzerland are demanded by a U.S. court the party has the option of contravening the Discovery request or the Swiss blocking statute. Possibly a party could surrender the documents before the relevant judicial order is issued, as this would not require the disclosure of documents 'for a foreign state'. As above and below, a litigant should plan carefully in the run up to litigation, identifying all data based abroad in order to avoid a catch-22 situation.

12. Article 29 Data Protection Working Party 2009 (the "Working Party")

12.1 The Working Party is made up of representatives from the data protection authority of each E.U. Member State, the European Data Protection Supervisor and the European Commission. The Working Party has been tasked with advising Member States on data protection with a particular focus on harmonising the European approach to data protection. The Working Party believes there are grounds by which disclosure should be legitimate: the consent of the data subject, when necessary to comply with a legal obligation or another legitimate obligation when absolutely necessary. Consent is clearly preferable but true consent from an employee is unlikely to be secured as they will have little or no real choice as to whether disclosure should take place. Clearly there is a balancing act between the two. The Working Party has recommended that in practice, data processing should be restricted to only anonymised, relevant data, with the suggestion of a trusted third party in the European Union being used to hold and transfer the data. An employee should be notified if their data is being processed and if he/she objects on legitimate grounds processing should be stopped. Furthermore where sensitive data is being processed, the consent of the employee should be obligatory. The Working Party has noted that there is inconsistency between the U.S. Discovery process and the E.U. data privacy regulations which needs to be reconciled.

13. Sedona Conference Working Group on International Electronic Information Management, Discovery and Disclosure ("Sedona")

13.1 The Sedona Conference Working Group is a think-tank that seeks to tackle the challenge of developing guidelines for electronic document retention and production. It has described the cross-border Discovery process as a ‘Catch 22’ situation, with the requirement to gather evidence from foreign jurisdictions contravening the blocking
statutes and data protection regulations intended to prevent such disclosure, noting the severe civil and criminal sanctions involved with a breach. Sedona has also noted that the U.S. Courts have little knowledge of E.U. data privacy rules and are therefore sceptical of litigants that use this as an excuse for not producing Discovery. Furthermore, as noted above, the 'expanding global marketplace' has and will continue to lead to conflict. Previous Sedona papers note that 'we communicate, collaborate and socialize faster and more globally than ever before', this leads to more electronic data, hosted internationally and therefore more likely to be stored on servers and with companies based abroad. Furthermore, the public are becoming more concerned with data protection. For example, in the U.S. the increase in personal data thefts for marketing purposes has led to greater awareness of and concern with privacy.

13.2 Sedona emphasises that parties to litigation should demonstrate respect for data protection laws, limiting their search to that which is relevant and necessary to support their position. Similarly, Data Controllers should be able to demonstrate that they have put necessary safeguards in place to protect data subjects and that data has been retained only as long as necessary. On the other hand both Courts and data protection regulators should judge compliance with data protection laws by standards of good faith and reasonableness. Where possible Court Orders should be relied on to minimise conflict. Sedona understands that both sides have a legitimate interest to protect and pursue and wants to reconcile the conflicting requirements of the U.S. Discovery rules with E.U. data protection.

13.3 Sedona has published many reports on conflicting international disclosure rules, many of which have been cited with approval by the European Commission. It has sought to provide a framework for Counsel to work through in the event they have cross-border Discovery conflicts and advice for how to take things forward in such circumstances. The group covers the following points in its' 2008 paper (which can also act as useful considerations for a litigator that has a cross-border conflict): which country has jurisdiction, who can access the data, the character of the data (i.e. whether it is personal data or otherwise), any blocking statutes in place, whether there are ways to legitimately alter the data to make it transferrable, and if there are any useful treaties in place such as the Hague Convention. The 2008 paper published by Sedona is a useful first stop for a litigator that has a cross-border disclosure conflict as it offers practical steps to overcoming such a problem and has been endorsed by the European Commission. The Sedona paper emphasises dialogue with both the U.S. Court and Member States to overcome disclosure hurdles. Litigators should ensure they have identified that there is an issue as soon as they can so that they communicate this issue both with the other side and the U.S. Court as well as suggesting practical solutions where possible.

14. Attorney client privilege

14.1 When coming under the rules of a European Member States, U.S. entities should be careful to check for any nuances in the local law. For example, whilst Ireland, the Netherlands, Poland and the U.K. recognise attorney-client privilege or 'legal professional privilege' for advice provided by in-house Counsel, countries including France, Italy and Austria do not. The European Court of Justice has previously ruled (as recently as 2010), that if an in-house Counsel is involved with a company's commercial strategy, it will compromise his/her ability to exercise professional independence. It is important to clarify with in-house Counsel in each respective European jurisdiction before communicating with them regarding a Discovery process (or any other sensitive issue for that matter). Where privilege is not recognised, it is best to instruct external counsel to provide legal advice and/or minimise written communication with in-house Counsel.
15. **Best practice**

15.1 When a U.S. litigant receives a Discovery order requesting documents based in Europe best practice is to follow multiple strategies as not all are clear cut or guaranteed to provide relief. Sedona suggests considering the following questions:

(a) Does jurisdiction exist

(b) Is a blocking statute involved

(c) What procedural Discovery rules govern?

(d) Is the Hague Convention the exclusive means of cross-border Discovery?

(e) Is personal data involved?

(f) Who controls the data?

(g) Is the personal data protected by a privacy law or other directive?

(h) What analytical test(s) should be applied by Courts to determine if Discovery can process, and the party is entitled to the information they have requested?

15.2 These are useful questions and will help you to identify the key issues and possible solutions. Each situation should be assessed on its own merits, but parties should consider the following generally recommended steps:

(a) Upon your U.S. client receiving a Discovery request, you should establish where the requested data resides and if abroad, whether that jurisdiction places restrictions on data transfer. The sooner you can identify such data, the less likely you will breach data protection issues due to a lack of awareness of them, and the more reasonable you will look when discussing waivers with the other side and the Court. U.S. Courts have looked badly upon parties who have not acted in a timely fashion.

(b) Notify the other party in writing that some of the documents are based in Europe, citing the relevant data protection laws and stating that they cannot disclose a document for data protection reasons. Best practice would be to obtain a sworn testimony or affidavit from an expert in that jurisdiction's data privacy laws, and to identify the specific documents that cannot be disclosed.

(c) If possible, the party seeking to deflect Discovery should seek to show that the relevant documents are not required to protect the interests of the requesting party. Instead the party should suggest alternative ways of establishing the information or determine whether the same information is available elsewhere.

(d) It is good practice for U.S. Counsel to appoint a law firm in the EEA country which the data is stored in to review the relevant documents. Once the relevant documents are identified, there will be a stronger argument that because these documents have been filtered, they are more relevant to the matter and are therefore less likely to contravene data protection rules.

(e) Any statement made to deflect Discovery on the basis of data privacy laws should be specific, naming the document(s)/request(s) that would breach foreign data privacy laws. U.S. Courts do not look favourably upon blanket Discovery refusals. Many Courts like to be presented with a 'privacy log' detailing the specific reasons for protecting each document.
A litigant should in most cases prioritise seeking to persuade the U.S. Court to accept restricted Discovery via a Protective Order. To give a litigant the best chance of success it should consider following multiple strategies:

(i) Not seek to only resist producing documentation that would be damaging to its case.

(ii) Provide evidence that the material originates and is still located in a European Member State.

(iii) Obtain a statement from the relevant Member State that the Discovery request violates the Directive and that State's data protection laws.

(iv) Show an attempt to comply with the Court order in good faith.

Seek to rely on the exceptions in the Directive allowing for transfer in the defence of a claim and/or to achieve the legitimate interests of a Data Controller in complying with a Discovery request. The litigant should first seek approval from the authority of the Member State for this.

Seek to argue that Discovery should be governed by the Hague Convention as opposed to the FRCP. The broad nature of the Discovery request, the Member State's data protection law and the fact than no specific reason exists for the Hague Convention not to be used will exist with this argument. If approved the Letter of Request should then be sent to the relevant Member State. However as discussed above, many U.S. Courts will refuse to recognise the Hague Convention.

16. Conclusion

It may be necessary in some instances for U.S. Counsel to balance the penalties for contravention of a Discovery order against those penalties for contravention of data privacy laws and decide which rule to breach based on the financial and other consequences. However if the Draft Regulation reforms the Directive as anticipated and a fine of 2% - 5% of a company's global revenue is levied against a company that infringes the Directive, it may swing a litigant in favour of contravening the FRCP.

Both the European Community and the U.S. are aware that the current cross-border Discovery system is not fit for purpose and requires reform. With the Working Party and Sedona suggesting practical, balances solutions the conflict will hopefully be resolved and a more transparent and practical process put in place. For now, U.S. Counsel should ensure the very simple, best practice steps are taken to avoid their clients and possibly themselves incurring fines for European data protection or U.S. Discovery breaches.

Paul Callaghan – Partner
Taylor Wessing LLP
Email: p.callaghan@taylorwessing.com
DD: +44 20 7300 4210

© Taylor Wessing LLP 2014
This publication is intended for general public guidance and to highlight issues. It is not intended to apply to specific circumstances or to constitute legal advice. Taylor Wessing's international offices operate as one firm but are established as distinct legal entities. For further information about our offices and the regulatory regimes that apply to them, please refer to: www.taylorwessing.com/regulatory.html