ARTICLE:

REMOTE ELECTRONIC DISCOVERY

By **Gib Sorebo**

Introduction

In the realm of civil discovery ('disclosure' in some jurisdictions) most attorneys in the United States tend to adopt a flexible approach to discovery, because the rules tend to encourage cooperation and give parties significant flexibility to jointly agree on a set of discovery practices. In general, this practice makes sense, because courts only become involved when there is a dispute. Otherwise the parties conduct discovery in a manner that fits the case and the resources they have available. However, the process presumes that attorneys for both sides are qualified to address the numerous issues that arise during discovery. While it is true that clients are ultimately responsible for the competency of their attorneys, it is also true that the legitimacy of our litigation process is undermined each time attorneys conspire, usually unwittingly, to impose unnecessary costs and an unreliable discovery process on their clients due to their lack of understanding of the information they are seeking to discover, the tools that are available to them, and the potential consequences to third parties.

Such a scenario is a daily occurrence in the area of e-discovery where attorneys for each side will negotiate away large swaths of data repositories within a company, accept data without any chain of custody, ignore meta data, and show no concern about the format that the data is produced. All this is not designed to limit discovery to what is important and to control costs. Instead, it is designed to keep matters on a level that they can understand and that their frequently underfunded and litigation support team that does not have the necessary skills can accommodate. Anecdotal comments from judges bear out the fact that such practices are common, and if both attorneys agree, there is little judges can do other than offer advice. Where this behaviour affects only the two parties, it is fair to say that there are more important things to worry about. However, litigation rarely occurs in a vacuum. Third party interests are often implicated. In discovery, all documents in the possession of each party are usually open to being seen by the other side. This could potentially include third party information that may be more valuable to the third party than the litigants. Additionally, privacy laws frequently limit the purposes for which such information can be used and require special authorization for use in litigation, particularly when the subject or data owner is not a party to the case.

As technology evolves, the implications for litigation must also evolve. Traditionally, discovery meant that a requesting party requested information relevant to the litigation with some degree of specificity, and the responding party then set about finding, collecting, and ultimately producing that data after reviewing it for relevancy and privilege. The process was fairly straightforward and limited by how the information was collected. Because the traditional method involved paper documents that were typically in the possession of a single person, usually known as the document custodian, it made sense that attorneys would simply issue a legal hold memorandum to such persons notifying them of the litigation, identifying the kinds of documents that would be relevant, requesting such documents be preserved, and providing a mechanism to deliver the documents or have them photocopied. In most cases, it was the document custodian who searched and delivered the relevant documents. Whether he or she was also responsible for doing the photocopying, sorting, or delivery, the law understood the location of the document custodian and the location of the documents to be synonymous. Discovery rules focused on the fact that a person under the jurisdiction of the court, usually as a function of their being the employee of one of the parties, was under an obligation, and sometimes compelled, to produce the documents. The document reviews, photocopying, Bates stamping, sorting, packaging, and delivery are all

support functions that flow from the obligations of the custodian of the document.

While courts may not always have direct jurisdiction over custodians of documents, particularly if they reside in another state or a foreign country, they still impose the obligation on the custodian indirectly through the jurisdiction they assert on the custodian's employer. The court will require the employer to direct its employees to produce a particular document. In addition to producing a clear chain of responsibility, it also allows any assertions based on privilege, privacy laws, export controls, or a sovereign's outright rejection of the litigation to be heard with respect to the document being requested. Because the same sovereign has immediate jurisdiction over both the custodian of the document and the document itself, it is in a good position to restrict its transfer and eventual production. Until recently, the same concept applied to electronically stored information. While the internet has provided people with instantaneous access to information world-wide, the data most frequently requested in litigation is still modeled after the paper method. The custodian of the data, usually a system administrator or designated data owner, is still requested to produce the information, and significantly, that custodian is usually located within close proximity to where the data is stored. Such proximity may be in another room or another building, but there is a good chance that it is still within the same jurisdiction. Moreover, based on the method typically used to collect the data that is discussed below, the litigation support team, in conjunction with the custodian, usually collects the data directly from the computer that it is stored on or over the network on a computer nearby. Either way, those collecting the data for the purposes of discovery are usually present in the jurisdiction where the data is stored even if it is collected and then loaded onto a repository in another jurisdiction.

What this article seeks to examine is the changing nature of both e-discovery and how data is stored. As new e-discovery technologies are deployed, the potential for widespread collection using remote means not facilitated by a local data custodian is becoming a reality. Because discovery in the United States does not typically involve the court for matters relating to the collection of discoverable material by the producing party, case law is rather limited and discussions about the significance of the location of electronically stored information and any possible restrictions on remote collection are non-existent. In fact, 'no court has squarely addressed where electronic materials are "located" for discovery purposes.'[1] Because jurisdiction and the ability to effectively adjudicate discovery disputes involving both litigants and third parties is generally a product of location in most common law countries, it is important that the law catch up with the technology.

Framing technology issues

The gathering of evidence for litigation is typically directed by counsel whereby the likely locations of relevant information and their custodians are identified. Then legal holds are issued to the custodian who can include both the imputed data owner, which may be a business manager charged with overseeing the business processes that generated or collected the data, and potentially a data custodian, who may be an IT manager or system manager but who is just as likely to be an employee who is simply storing the relevant data on his or her desktop or laptop. Similarly, in the physical world, there are imputed document owners and document custodians. In both situations, both the custodian and the data owner are frequently situated at the same geographic location and usually in the same jurisdiction. In some cases, centralized mainframe computers had required some physical separation. However, in discovery matters, the person physically co-located with the system was usually the person given the task with extracting the data that was required. Additionally, despite the ability to obtain access to the date remotely, there was little question of its location.

The only type of remote discovery that has been considered somewhat routine, is the collection of publicly available information available on the internet. In this case, production is hardly necessary, because the requesting parties can simply search the internet to collect whatever information they choose. Consequently, for the purposes of this article, remote discovery involves the collection and eventual production of non-public information. This includes desktops and laptop computers, servers with directly attached storage, storage area networks, and removable media. Almost by definition, remote access to these storage devices involves some sort of network, either through a traditional circuit-switched telephone network, or dial-up, and, more typically, via a packet-

[1] *Gary B. Born and Peter B. Rutledge, International Civil Litigation in United States Courts (4th edition, Wolters Kluwer Law and Business, 2007), 930.*

based network such as the internet or similar sub-networks within an organization with connectivity being provided locally by the organization or over long distance using internet or private leased line connectivity. In either case, higher level protocols using encryption, circuit virtualization, authentication, and other means can ensure that such connectivity remains private. Within these private networks, the conventional notions of storage and application services are radically changing. No longer is storage tied to a single processing device. It can serve multiple application servers all at once. Moreover, the storage can be distributed across national boundaries as needed. Using sophisticated data mapping technology, what appears to an end user to be a single file or directory at one location could actually be bits stored on multiple devices in several different countries. Moreover, the application retrieving the file for processing and eventual output to the user could also have components residing in multiple locations and potentially owned by a third party. These are called cloud computing applications. While in essence they are a throw-back to mainframe computing concepts of shared processing, cloud computing will probably revolutionize computing and fundamentally alter the notion of electronically stored information. The change is not so much that remote discovery is now possible. In some form, the potential for remote discovery of electronic data has existed as long as there have been computer modems. Instead, the fundamental change is that some discovery can only be achieved remotely, given how some applications and their data are now structured.

Even if the notions of cloud computing and geographically distributed storage are yet to become commonplace, other factors are making remote discovery an all but unavoidable scenario in litigation. Due to the globalization of many corporations and the need to collaborate, the operation of largely autonomous subsidiaries organized by country has largely vanished. High network bandwidth over long distances has meant that information technologies can simultaneously use data stored in multiple places and the need to have 'local' copies of all data needed by the local users has all but vanished in many large organizations. Moreover, enterprise search technologies are being deployed in a way where data owners can authorize data custodians to grant access to appropriate parties and refrain from overseeing such access. They are no longer the go-between in satisfying requests for data. Instead, once access is granted, the data can be available world-wide, subject to export control and privacy laws. Individuals often have no concept of where the data is physically located, nor do they care. They may be aware that a particular document was written by an employee residing in another country, but they have no way of knowing if it was actually drafted in that other country. Also, in the spirit of collaboration, documents are routinely edited and data is supplied from a number of countries. This means that to argue that the data falls under the sovereignty of a particular nation or US state based on the nationality of the author or the location of authorship is a misnomer. While privacy and export control laws may dictate some degree of data segregation by country, such laws are rendered otiose by the vast amount of data involved in commercial litigation that does not fall into those categories. Additionally, with the Safe Harbor provisions,[2] privacy laws, arguably, may no longer require that covered data honour national boundaries.

Traditional legal issues with cross border discovery

Aside from the logistical challenges brought by new technology, legal issues also present challenges of their own. Because there is limited legal precedent for remote discovery, the focus will be on drawing parallels with cross border discovery decisions. From a statutory and administrative perspective, discovery is the same whether the activity is conducted in the United States or abroad. Unless a judge is asked to compel discovery, litigants are free to request and conduct depositions and request production of information wherever it might reside.[3] When a court orders foreign discovery, additional considerations may need to be addressed. As described below, the court jurisdiction will usually be the primary arbiter in deciding whether discovery can be compelled. The potential interests of third parties, when

[2] *Under provisions of Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L281, 23.11.95, p. 31 (EU Data Protection Directive), and its national implementing laws, countries such as the United States may be allowed to hold private data on European citizens if the country provides for legislation that legally obligates organizations receiving such data to follow the provisions of the Data Protection Data Directive and guidance from individuals nations with respect to dissemination and uses for that data. U.S. Department of Commerce, Safe Harbor Privacy Principles (July 21, 2000), http://www.export.gov/safeharbor/SH_Privacy.asp.*

[3] *Fed. Rule Civ.Proc. Rule 28(a)(1) provides for depositions in a foreign country and may require some notice depending upon how the deposition is procured.*

When used effectively, discovery can be the mechanism that unearths corruption, holds large organizations accountable, and gives litigants with limited means the opportunity to make their case.

no challenge is raised, are usually not considered in the absence of a third party being added to the proceedings. Because most discovery efforts are carried out with little or no public notice, third parties typically have no way of effectively intervening. This presents some interesting privacy and sovereignty considerations that are discuss below.

Ultimately, the issue is often that non-US jurisdictions find the American discovery process unwieldy and fundamentally flawed. They see its stated goal of learning the truth through exhaustive review of all relevant information as simply a charade meant to mask the true intent of the litigants, which is to conduct fishing expeditions designed to increase the other party's costs, expose embarrassing facts that are only tangentially related to the matter at hand, and engage in countless acts of gamesmanship and chest thumping to distract the fact finder from the case and enhance the image of the attorneys. While the statistics that show only a small percentage of cases reaching trial would seem to support the claim that the American litigation system is unwieldy, it is misleading to suggest that such an outcome is based on the system's overwhelming discovery burdens or the publicity sought by attorneys. When used effectively, discovery can be the mechanism that unearths corruption, holds large organizations accountable, and gives litigants with limited means the opportunity to make their case. While true smoking guns are rare, discovery often forces settlement because the information produced by each side provides overwhelmingly evidence that favours one party or the other. The fact that litigants in civil proceedings routinely produce incriminating information that it likely to be used against them is a testament to not only the effectiveness of the discovery process, but of their adherence to ethical conventions and the rule of law. That said, the process is not without its faults. The process can certainly be expensive and unwieldy, with many of its failures not a product of its fundamental principles, but rather adherence to inefficient processes and poor use of technology. Nonetheless, as the processes and revised and the technology is improved, it must be recognized that streamlining processes to more efficiently adhere to these principles may have the unintended effect of denigrating the principles that others hold dear. While compromising principles may not be an option, the methods chosen can be open to compromise.

E-discovery issues

State level

While most legal issues with remote electronic discovery involve the movement of data across national borders, there are a few issues that are relevant between US states. While states are typically obliged to honour requests made by courts of other states and generally show deference to depositions and document productions that originate from litigation in another state, it remains the expectation that some protocol should be followed. For example, where a judge authorizes a party to seize evidence from the other litigant in another state, it is expected that local law enforcement will be engaged and perhaps even local courts will enforce the order.

Recently, some states have passed laws requiring that computer forensics examinations that are part of litigation be performed by licensed private investigators.[4] While this particular requirement is problematic on a number of levels, it does reflect states' desire to assert some quality controls over the process of collecting evidence and to retain oversight over the process. However, the laws are unclear whether they

[4] *2008 American Bar Association Section of Science & Technology Law, Report to the House of Delegates 301, available at http://www.abanet.org/scitech/301.doc (noting specific PI licensure requirements for performing computer forensics in Illinois, Texas, Michigan, Georgia, Rhode Island, South Carolina, North Carolina (pending), Massachusetts, Nevada, New York).*

would apply to remote electronic discovery. While the South Carolina Attorney General has asserted that any computer forensic examinations performed in other states must be conducted by a South Carolina licensed private investigator when the evidence is gathered to be used in a South Carolina court proceeding, there is no such guidance for evidence remotely gathered using a computer forensics process on a device located in a state with such a private investigator requirement where the information is to be used in a matter outside that state.[5] This is despite the fact that some of these states have asserted that licensed private investigators be used when computer forensics is performed in their jurisdiction regardless of where the evidence will ultimately presented and even applies if no litigation is anticipated. It is one of many examples where laws are written too simplistically to resolve a perceived problem rather than to address the true objectives of the situation. The quality of computer forensic examination is certainly an issue that needs to be addressed. However, the solution proposed and implemented is not always the most appropriate. Rather than passing a law that is enforceable in the least costly manner possible but ineffective at accomplishing the objective, states should recognize that the true solution may be to learn more about the problem, seek consensus where possible, and regulate last. Failing to do so simply leads to circumvention and higher costs and ultimately causes more harm to the very people it seeks to protect.

Aside from forensic examinations, the very notion of remotely collecting data in other states raises a number of issues relating to the state's desire to accord privileges to its citizens. Because most state privacy laws target personal data about its citizens without regard to location, the privacy aspects seem not to be implicated. Moreover, constitutional protections of interstate commerce would seem to preclude a state from restricting the flow of such data. However, because this data may be destined for a court, practitioners should be wary of state specific privileges that may arise. Conflict of law principles are far from settled in this area as it is unclear whether privileges apply to data at the point it is generated or in the state where the court is located.

International

By far the most significant legal issues with remote discovery involve data that passes across international borders. Because remote discovery typically does not require anyone in the foreign country to facilitate the data transfer, such transfers can be transferred with relative ease. Typical foreign discovery challenges usually involve conducting depositions in another country or requesting someone in that country to produce a document. For the most part, there is little authority on the issue of whether the fact that no one involved in the discovery need be present in that country raises any concerns. The typical remote discovery scenario would be where relevant information resides on a server in a branch office of a multi-national company that was outside the United States. Assuming that personnel in the United States already have remote access to the data, then a foreign government has limited ability to prevent access, because it cannot sanction anyone under its jurisdiction for the immediate transfer. After all, '[t]he location of the person, not the document, is also a hallmark of discovery under the Federal Rules of Civil Procedure: "Persons resident or found within the United States may have in their possession or under their control evidence located abroad. It has long been recognized that such persons may be required to produce such evidence in courts in the United States."'[6] However, if a local employee of the company is required to grant access or otherwise facilitate the transfer before it can be sent, then foreign law may pose some challenges depending upon the data at issue, because the facilitator risks violating their own law or causing their employer to violate US law.

Beyond the unique circumstances associated with remote discovery, the challenges posed by discovery of information in a foreign country for use in a US proceeding can be daunting. As mentioned above, many countries, particularly those using the civil law system, show a particular distaste for the American discovery process. 'As of 1986, some 15 states had adopted legislation expressly designed to counter United States efforts to secure production of documents situated outside the United States.'[7] These have taken a number of forms, from providing mechanisms for its citizens to

[5] *Deb Radcliff, 'Computer Forensics Faces Private Eye Competition' Baselinemag, January 2, 2008, p 1 http://www.baselinemag.com. ('In April [2007], the state attorney general opined that even if you never set foot in South Carolina, if you're collecting evidence to be used in court here, you still need a South Carolina [PI] license', says Steve Abrams, a licensed independent PI and computer forensic examiner based in Sullivans Island, S.C. 'Licensing authorities in New York, Pennsylvania, Texas and Oregon have opined the same way.')*

[6] *Charles McClellan, America, 'Land of (Extraterritorial) Discovery: Section 1782 Discovery for Foreign Litigants', 17 Transnational Law & Contemporary Problems 809, 822 (2008) (quoting Hans Smit, 'American Assistance to Litigation in Foreign Aid and International Tribunals: Section 1782 Title 28 of the U.S.C. Revisited', 25 Syracuse Journal of International Law and Commerce, 1, 10 n.46 (1998)).*

[7] *Restatement (Third) Foreign Relations Law § 442, Reporters' Note 1 (1987).*

refuse requests, to prohibiting its citizens from cooperating altogether in the case of France.[8] The process generally acceptable to most countries is through the Hague Convention on the Taking of Evidence Abroad in Civil or Commercial Matters.[9] That treaty calls for letters of request to be issued by the court having jurisdiction over the matter and sent to the relevant authority in the country where evidence is being sought. While this process has assisted litigants who previously had no recourse when seeking discovery of witnesses or documents located in a foreign country, the US Supreme Court noted in the seminal case of *Societe Nationale Industrielle Aerospatiale v. District Court*[10] that the use of the treaty is not mandatory in foreign discovery matters and that it does not override the Federal Rules of Civil Procedure.[11] In this case, the Supreme Court took a pragmatic view in suggesting that the treaty was merely in place to protect the rights of foreign litigants and that where both parties are amenable to the discovery request, there is no need to involve foreign authorities in the matter. Justice Blackmun's dissent clearly alludes to this perception and argues that with the civil law system, in particular, the process by which evidence is collected, normally by a judge rather than the litigants, is as much a part of the analysis as the willingness of parties to comply with the request. He notes judges are often entrusted with the role of balancing the rights of the parties as well as the rights of the public as a whole, including affected third parties, when deciding whether to transfer that evidence to a foreign court.[12]

Considering the view of the majority and similar holdings in other courts that effectively suggest that the treaty's procedures should be the last resort rather than the first, it would be safe to conclude that remote discovery would probably be a matter requiring little, if any, consultation with foreign authorities as far as US courts are concerned. In effect, what little related case law on this subject tends to bear this out. For example, in 2002, Vasily Gorshkov was convicted of stealing credit card numbers by a Seattle-based federal court. The evidence in the case was gathered by FBI agents who lured Gorshkov and his accomplice into the United States from Russia, where through an undercover ruse, they asked the two men to type their username and password into a computer the FBI was monitoring. The account credentials were for a computer located in Russia. The agents then used the credentials to gain access to that computer and download the evidence implicating the two in multiple cases of fraud. Because the FBI used its own computer, told the defendants they wanted to watch them, and obtained a search warrant before viewing the downloaded file, the Federal District Court Judge ruled that the evidence was admissible and that the FBI had done nothing wrong. He further asserted that the fact that the agents' action violated the law of the Russian Federation was not relevant because the law of the Russian Federation did not apply.[13] It transpires that the Russian authorities did not agree, and filed a criminal complaint against the agents, while the agents received the Director's Award for Excellence as a result of the successful sting operation.[14]

While such a flagrant flaunting of another nation's laws may result in the exclusion of evidence in civil matters, courts have nonetheless shown that US interests, particularly those of the litigants, come first. In response to blocking statutes, courts have adopted a five factor test for considering whether a party should be compelled to produce information that resides in another jurisdiction, particularly in cases where the party needs to travel to that country to retrieve it or request employees in the foreign country to facilitate its delivery even when the foreign nation specifically forbids it. The factors include: (1) the importance to the litigation of the information requested; (2) the degree of specificity of request; (3) whether the information originated in the United States; (4) the availability of alternative means of securing the information; (5) the extent to which failure to comply would undermine the interests of the United States or compliance with the request would undermine the interests of a foreign sovereign nation.[15] However, case law suggests if the

[8] *James Chalmers, ' The Hague Evidence Convention and Discovery Inter Parties: Trial Court Decisions Post Aerospatiale' , 8 Tulane Journal of International and Comparative Law 189, 213 (2000) (noting that '[i]t is difficult to take the French ' blocking statute' at face value given that, taken literally, it appears to prevent French nationals doing business abroad from taking court action in foreign tribunals. Instead, it appears that the statute was intended to assist French nationals involved in litigation abroad by providing them with a reason for refusing to disclose information.')*

[9] *Opened for signature, 18 March 1970, 23 U.S.T. 2555, T.I.A.S. 7444, 847 U.N.T.S. 231.*

[10] *482 U.S. 522 (1987)*

[11] *482 U.S. 522 (1987) at 544 (declining to hold to hold, as a blanket matter, that comity requires resort to Hague Evidence Convention procedures without prior scrutiny in each case of the particular facts, sovereign interests, and likelihood that resort to those procedures will prove effective).*

[12] *482 U.S. 522 (1987) at 548 (Blackmun, J, dissenting) (' In my view, the Convention provides effective discovery procedures that largely eliminate the conflicts between United States and foreign law on evidence-gathering. I therefore would apply a general presumption that, in most cases, courts should resort first to the Convention.').*

[13] *Mike Brunker, Judge OKs FBI hack of Russian computers, ZDNet, 31 May 2001, http://news.zdnet.com/2100-9595_22-115961.html.*

[14] *Lawyer to challenge FBI in Russian sting, Reuters, 25 August 2002, http://news.cnet.com/Lawyer-to-challenge-FBI-in-Russian-sting/2100-1002_3-955251.html.*

discovery request could be satisfied without leaving the United States or requesting the aid of someone in a foreign country through a means such as remote discovery, courts are not likely to even consider treaty requirements or blocking statutes when deciding whether to grant the request to compel.[16]

While the court's inclination to ignore the wishes of a foreign government in both civil and criminal cases is certainly the most expedient means of resolving a discovery dispute when that foreign government's assistance is not needed, it is nonetheless troubling. Disregard for international comity can arise in other forums that are not directly of interest to the court or the litigants but could have a chilling effect on future cross border litigation and even the transfer of data across borders outside litigation. For example, under provisions of the EU Data Protection Directive[17] and its subsequent enforcement of member nations, the default position is that the United States does not have sufficient data protection laws for the protection of personal data to permit the transfer of such data. However, under the Safe Harbor provisions negotiated with the US Department of Commerce,[18] an organization can voluntary submit to such provisions that the Department of Commerce will then enforce as a condition of receiving personal data on EU citizens. However, the Safe Harbor provisions are problematic within the context of discovery, because the provisions only apply to data transferred to another country but within the same organization. Because the purpose of discovery is to disclose data to another party, the Safe Harbor provisions do not provide adequate protection. Additionally, while consent of the subject of the data is usually sufficient to exempt the application of privacy laws, where the consent is by an employee, EU authorities typically view such consent as coerced and therefore not allowed.[19] As an alternative, the EU Data Protection Directive does allow for transfers outside the Safe Harbor protection where 'the transfer is necessary . . . for the establishment, exercise or defense of legal claims.'[20] However, such transfers must be ordered by a European judicial authority pursuant to a letter of request, such as provided for under the Hague Convention.[21] Based on recent precedent, litigants are not likely to make such a request if the information can readily be obtained by simply obtaining access to a remote computer.

As a result, the situation is difficult. As technology advances to the point that multinational corporations can easily resort to these self-help measures without risking sanctions or even awareness by foreign governments that this is going on, the pattern will continue, with the criteria for compliance being US privacy laws that Europeans, in particular, find inadequate. However, it may take one significant and public privacy breach to convince European governments that the Safe Harbor provisions are relatively weak within the US legal system and may be rescinded, making cross company communications problematic across borders. Other implications could be outright refusal to allow US persons direct remote access to the personal data of EU citizens residing on systems within an EU country. Ultimately, distributed storage and cloud computing may either make that discussion moot, or laws could effectively limit the use of such technology across national borders. Given the undesirable consequences that could result from direct regulation of such technology for the regulating country, it is to be hoped that a more efficient solution that preserves international comity and the rights of each country's citizens while satisfying the demands of the US discovery system will come about. The models described above could work, but no one currently has the incentive to implement them.

Gib Sorebo is an information security consultant and assists organizations in managing their information security and privacy risks, and compliance obligations. He speaks on various topics, including information security liability, electronic discovery, and security breach laws. He holds a Juris Doctor from Catholic University.

gibsorebo@hotmail.com

[15] *Restatement (Third) of Foreign Relations § 442(1)(c) (1987)*

[16] *Article 29 Data Protection Working Party, Working Document 1/2009 on pre-trial discovery for cross border civil litigation at 5, 00339/09/EN, WP 158 (Feb. 11, 2009) (noting 'that if the company is subject to US law and possesses, controls, or has custody or even has authorized access to the information from the US territory (via a computer) wherever the data is "physically" located, US law applies without the need to respect any international convention such as the Hague Convention.').*

[17] *EU Data Protection Directive at 31–50.*

[18] *U.S. Department of Commerce, Safe Harbor Privacy Principles (July 21, 2000), http://www.export.gov/safeharbor/SH_Privacy.asp.*

[19] *Carla L. Reyes, 'The US Discovery-EU Privacy Directive Conflict: Constructing a Three-Tiered Compliance Strategy', 19 Duke Journal of Comparative and International Law 357, 374-78 (2009) (discussing limitations of Safe Harbor provisions and consent); but see Stanley W. Crosley, Alan Charles Raul, Edward R. McNicholas and Julie M. Dwyer, 'A Path to Resolving European Data Protection Concerns With U.S. Discovery', 6 Privacy & Security Law Report 1, 5 (Oct. 15, 2007) (suggesting that consent, particularly when obtained in advance of the litigation, may be sufficient).*

[20] *EU Data Protection Directive, art. 26(1)(d).*

[21] *Carla L. Reyes, The US Discovery-EU Privacy Directive Conflict: Constructing a Three-Tiered Compliance Strategy, note 17, at 365-66.*

