The Sedona Conference Journal

Volume 10 2009

E-Discovery, Privacy, and the Transfer of Data Across Borders: Proposed Solutions for Cutting the Gordian Knot

Moze Cowper & Amor Esteban

Recommended Citation: Moze Cowper & Amor Esteban, *E-Discovery, Privacy, and the Transfer of Data Across Borders: Proposed Solutions for Cutting the Gordian Knot*, 10 SEDONA CONF. J. 263 (2009).

E-DISCOVERY, PRIVACY, AND THE TRANSFER OF DATA ACROSS BORDERS: PROPOSED SOLUTIONS FOR CUTTING THE GORDIAN KNOT

Moze Cowper, Amgen Inc., Thousand Oaks, CA
Amor Esteban, Shook, Hardy and Bacon, LLP, San Francisco, CA

Summary

Globalization has "shifted into warp speed."[2] Individuals and businesses now collaborate and compete at a breakneck pace and information has become the new global currency. The ease with which electronic information is now created, moved, and stored, however, places profound stress on the existing international discovery system. This paper calls for the recognition of a practical solution to the issue of litigation discovery and cross-border data transfer between the United States, the European Union, and elsewhere. Finally, this paper also calls for a re-writing of the Hague Evidence Convention. It is time for a modern, global and effective solution.

Introduction

Here is the scenario. You are an in-house counsel or a retained litigator that represents a large company in the United States. The client, though, like so many companies, now does business all over the world. It has offices in Europe, Asia, Latin America, and Australia. The employees at this company are technologically sophisticated. They demand smart phones and unified messaging. They want their voicemails delivered to their email inbox and hand-held devices. They "twitter" and belong to social networking sites. They work on virtual teams and many employees have not seen the inside of an actual office for years. In short, this hypothetical company is a lot like every fast-moving, quick thinking, and globalized company in the world: hungry for information and armed with the financial capital to make things happen.

Now imagine the following: this company, your client, gets sued in the United States. The lawsuit is filed in federal court and not long after the lawsuit is filed your adversary requests a meaningful meet-and-confer under Rule 26(f) of the Federal Rules of Civil Procedure. They want to talk e-discovery. They want to talk location of servers, back-up tapes, hold order systems, unified and instant messaging, and global retention and record preservation policies. They are interested in the data created by your employees who sit in cafes in Paris, while sending messages to customers in Dubai, and using a shared database that sits on a server in Singapore. Put simply, they know what they want, you know they will likely request it under the broad U.S. Federal Rules of Civil Procedure, and you also know it is going to cost you millions of dollars to preserve, collect, process, and review it.

---

1 Moze Cowper is Senior Counsel at Amgen Inc. Amor Esteban is a partner with Shook, Hardy and Bacon, L.L.P. Both Messrs. Esteban and Cowper are members of The Sedona Conference's Working Party 6 on International Electronic Information Management, Discovery, and Disclosure. This paper is presented at "The Sedona Conference® International Programme on Cross-Border eDiscovery & Data Privacy Conflicts," Barcelona, Spain, June 2009. Moze and Amor would like to extend a special thank you to William Burtis, associate, Shook, Hardy and Bacon for his helpful research and counsel as well as Dan Regard of Intelligent Discovery Solutions.

2 *See* Thomas Friedman's *The World is Flat: A Brief History of the Twenty-First Century* (2005).

As a sophisticated litigator and practitioner, you know that there are data privacy laws and "blocking statutes" that prevent you from simply collecting the electronic data of the company's employees located in Europe, Asia, Latin America, and Australia. As a result of these restrictions, the normal rules of collection, processing, and review that apply in the United States do not apply here. Further, as in all litigation, time is not on your side. You need to access this data quickly, assess the strengths and weaknesses of your case, and determine if there is any truth to the allegations brought by your adversary. In order to do this, though, you are going to have to make sense of EU data privacy laws, country specific data privacy laws, and blocking statutes that may subject you to civil or criminal penalties if violated. In short, you need a practical solution to a complicated problem that, until recently, did not really exist on such a large scale.

In the past, practitioners faced with conducting discovery abroad usually turned to The Hague Evidence Convention,[3] the Restatement on Foreign Relations,[4] or the Restatement on Conflict of Laws.[5] The problem is that these tomes and principles were not drafted with an eye towards our new globalized world. While they contain important ideas and wisdom on the underlying considerations involving taking discovery from abroad, none of these treaties or guides offers a practical, workable, and quickly deployable solution.

On February 11, 2009, the Article 29 Working Party published a paper entitled: "Working Document 1/2009 on pre-trial discovery for cross border civil litigation"[6] (hereinafter referred to as WP 158). Acknowledging the horns of the dilemma that threaten to gore so many EU corporations and EU affiliates of US corporations, the Working Party in WP 158 proposes guidance to aid those multinationals caught between US cross-border discovery obligations and EU data protection and privacy laws.

Those hoping for absolution through the Working Party's efforts, however, will be disappointed. Its guidance, the Working Party explained, was made in recognition ". . . that the parties involved in litigation have a legitimate interest in accessing information that is necessary to make or defend a claim, but this must be balanced with the rights of the individual whose personal data is being sought." While understanding the seemingly inconsistent obligations that arise when cross-border discovery requires access to or disclosure of protected personal data, the Working Party is also mindful of the limitations on its own authority. As stated by the Working Party:

> Although this paper sets out guidelines it is to be noted that resolving the issues of pre-trial discovery is beyond the scope of an Opinion by the Working Party and that these matters can only be resolved on a governmental basis, perhaps with the introduction of further global agreements along the lines of the Hague Convention.

In short, the Working Party, while wanting to help, is not in the business of giving corporations a "free pass" to ignore EU privacy obligations only because US discovery laws are in conflict. On the other hand, through its guidance, the Working Party does demonstrate that, in appropriate circumstances, and with appropriate measures in place to safeguard personal data, a certain level of harmonization is achievable.

The question of how data controllers reach this place of peaceful coexistence is the focus of this paper and, while not perfect, a possible solution is suggested. This paper will also propose

---

3 The Convention on the Taking of Evidence Abroad in Civil or Commercial Matters (otherwise known as the "Hague Evidence Convention") is a multilateral treaty that was signed by the U.S. in 1970. The Hague Evidence Convention offers optional procedures in the form of minimum standards with which contracting states agree to comply in order to facilitate the taking of evidence abroad. It "does not modify the law of any contracting state [including the Federal Rules of Civil Procedure], require any contracting state to use its procedures either in requesting evidence or in responding to requests, nor compel any contracting state to change its own evidence gathering procedures." *Société Nationale Industrielle Aérospatiale v. U.S. District Court for the Southern District of Iowa*, 482 U.S. 522, 534 (1987). Under the Convention parties may seek a Letter of Request or Letter Rogatory be sent from the Convention authorities to a foreign court to compel production of evidence. However, this procedure may be "unduly time consuming and expensive, as well as less certain to produce needed evidence than direct use of the Federal Rules." *Id.* at 542.

4 The Restatement (First and Second) of Foreign Relations was originally drafted in 1962 and later revised in 1965. The Restatement (Third) of Foreign Relations was published in 1986.

5 The Restatement (First) Conflict of Laws was originally drafted in 1934 and was later revised in 1971.

6 Working Paper, Working Document 1/2009 on Pre-Trial Discovery for Cross-Border Civil Litigation, 00339/09/EN, WP 158 (Feb. 11, 2009) [hereinafter WP 158] (this is a working document and initial consideration for public comment). The paper can be found at: http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp158_en.pdf.

the idea of a single document – a Certificate of Compliance for the Transfer of Personal Data Across Borders – that will attempt to memorialize the protections contemplated by European Union data privacy experts and governments when data is collected and processed in the European Union for purposes of responding to discovery requests or governmental investigations in the United States. In the meantime, the authors echo the Working Party's admonition that a more perfect solution lies in "further global agreements" by the governments on both sides of the Atlantic. This paper concludes with a suggested strategy that may help lead towards that sort of international stipulation between nations.

The Recent Article 29 Working Party Paper

Our analysis of WP 158 starts with the candid admission that our interpretation may not accurately reflect the intent of the Working Party. We think it unlikely, however, that the Working Party would acknowledge the heightened pressure on multinational corporations to comply with seemingly inconsistent laws, introduce their writing with the stated purpose of providing "guidance," but then fail to provide a viable path out of the labyrinth. In our view, the Working Party has come to the conclusion that a balance is attainable between the individual's privacy rights in the European Union and the multinational's need to prosecute a legal claim or defend itself against a cause of action in the United States. This balance, we think, is attainable by taking reasonable precautions to safeguard personal data along the lines described by the Working Party.

Permissible Processing

To begin with, the Working Party clearly identifies the act of preserving personal data for litigation purposes as constituting "processing" under the Directive but recognizes that, under appropriate conditions, this processing may be legitimized.[7] Article 7 of the Directive sets out the limited circumstances under which personal data may be processed and, for each ground stated, its scope and procedural requisites. Three of the various circumstances described in Article 7 appear to permit processing for US discovery purposes but, as the Working Party points out, two of these are illusory.

Consent of the data subject, for example, will permit a data controller to process the data subject's personal data pursuant to Article 7(a). The Working Party discourages "consent" as a valid means of legitimizing the processing of data, however, because it is difficult to obtain truly voluntary consent under the strictures of Article 2(h) and because the data subject retains the right to withdraw consent at any time, which is antithetical to the US discovery process.[8]

A second possible but equally unattainable form of legitimizing the processing of personal data is under Article 7(c), which permits processing if "necessary for compliance with a legal obligation to which the controller is subject." The Working Party notes, however, that this channel is available only where the legal obligation arises from application of the law of a Member State.[9] In other words, as has been previously found by the Working Party, the "legal obligation" that is the condition precedent of Article 7(c) does not include within its definition a US law or court order, except when that law or order is enforced through an EU judicial authority pursuant to the Hague Convention.[10] Further, a multinational subject to a US preservation obligation typically does not have the year or more it will take to get relief through the Hague. Article 7(c), consequentially, is of little use to the multinational, especially for preservation purposes, when "processing" in the form of a litigation hold is immediately required upon learning of litigation or recognizing that litigation is reasonably likely.

---

7 *Id.* at p. 8.
8 *Id.* at p. 9 ("relying on consent may . . . prove to be a 'false good solution', simple at first glance but in reality complex and cumbersome.") (quoting from Working Document on Common Interpretation of Article 26 (1) of Directive 95/46/EC of 24 October 1995, at p. 11, 2093/05/EN, WP 114 (Nov. 25, 2005) [hereinafter WP 114].
9 *Id.* at p. 9.
10 Working Party, Opinion 1/2006 on the Application of EU Data Protection rules to Internal Whistle-blowing Schemes in the Fields of Accounting, Internal Accounting Controls, Auditing Matters, Fight Against Bribery, Banking; and Financial Crime, at 9, 00195/06/EN, WP 117 (Feb. 1, 2006) [hereinafter WP 117] (citing Privacy Directive Article 6.); Working Party, Opinion 10/2006 on the Processing of Personal Data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT), at 21, 01935/06/EN, WP 128 (Nov. 22, 2006) [hereinafter WP 128].

The last of the three exceptions under Article 7 raised by the Working Party holds the most promise and seems to be the recommended course of action. Article 7(f) recognizes as lawful the processing of personal data if "necessary for the purposes of legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject."

It is helpful here that the Working Party has previously recognized that a US legal requirement constitutes a "legitimate interest" for purposes of Article 7(f).[11] The Working Party in WP 158 reiterates that earlier position, this time specifically recognizing that a US discovery order may be sufficient to permit processing pursuant to Article 7(f), albeit within certain limitations:

> Compliance with the requirements of the litigation process may be found to be necessary for the purposes of a legitimate interest pursued by the controller or by the third party to whom the data are disclosed under Article 7(f).

But that does not end the inquiry. For processing to be lawful under Article 7(f), the "legitimate interests" of the controller or third party must not be 'overridden by the interests for fundamental rights and freedoms of the data subject.'[12] This balancing test, according to the Working Party, requires consideration of proportionality, relevancy to the litigation and the consequences to the data subject.[13] Moreover, if the balancing test tips in favor of the data controller, adequate safeguards need to be put in place.

Proportionality

In order to use the "legitimate interests" grounds of Article 7(f) as the means for processing personal data in response to US discovery, the data controller must comply further with Article 6 of the Directive, which requires that the personal data must be:

> (a) processed fairly and lawfully;
>
> (b) collected for specified, explicit and legitimate purposes and not furthered processed in a way incompatible with those purposes;
>
> (c) adequate, relevant and not excessive in relation to the purposes for which they are collected;
>
> (d) accurate; and,
>
> (e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected for which they are further processed.

The Working Party envisions a process where the proportionality of Article 6 may be satisfied by the data controller through its active management of the process; steering a course towards harmonization by employing such measures as petitioning the US court for appropriate limitations on the discovery of personal data through protective orders; engaging third party neutrals in the European Union to "filter" or narrow the scope of what will be further processed and possibly disclosed; and, involving data protection officials early, presumably to liaise with affected data subjects and confirm personal rights are honored.[14]

---

11 *See* WP 128, note 10, p. 18. (Where an entity was subject to both US and EU jurisdictions, "[i]t cannot be denied that SWIFT has a legitimate interest in complying with subpoenas under U.S. law.").
12 WP 158, note 6, p. 9 (quoting from the Directive, Article 7(f)).
13 *Id.* at p. 10.
14 *Id.* at pp. 10-11.

Adequate Safeguards

When the "legitimate interests" of the data controller, viewed through the prism of proportionality, favor processing of personal data, the Directive requires that certain safety measures are in place for the protection of the data subject. The "adequate safeguards" that justify processing of personal data are described by the Working Party in various parts of the Opinion and include:

> (1) maintaining shorter retention periods relative to personal data to reduce the number of personal data records that may exist at the time a litigation hold is issued;
>
> (2) achieving transparency pursuant to Articles 10 and 11 of the Directive, meaning:
>
> > (a) giving data holders advance, general notice of the possibility of their personal data being processed for litigation;[15] and,
> >
> > (b) identifying to the data subject any recipients of their data, the purposes of the processing, the categories of data concerned and the existence of the data subject's rights in those cases where personal data is actually processed for litigation purposes;[16]
>
> (3) providing notice that the data subjects have the right to object to processing pursuant to Article 14 of the Directive;[17] meaning the data controller must additionally provide information concerning:
>
> > (a) the right to object at any time on compelling legitimate grounds to the processing of data related to the data subject;[18]
> >
> > (b) the existence, purpose and functioning of its data processing;[19]
> >
> > (c) the recipients of the personal data;[20] and,
> >
> > (d) the right to access, rectification and erasure of the personal data pursuant to Article 12;[21]
> >
> > (The Working Party further advises that the appropriate data protection authorities should be notified of the proposed processing activities);[22]
>
> (4) considering the use of culling to separate the relevant from the irrelevant so that "a much more limited set of personal data may be disclosed as a second step";[23]
>
> (5) considering whether culling may be conducted by a trusted third party in the European Union to reduce the number of personal records to be processed;[24]
>
> (6) considering whether personal data should be anonymised or at least pseudoanonymised to protect the data subjects identity,[25]

15 *Id.* at p. 11.
16 *Id.*
17 *Id.* at p. 10.
18 *Id.* at p. 18.
19 *Id.*
20 *Id.*
21 *Id.* at p. 12 (recognizing the friction between a data subject's right to modify data and the US discovery obligation to preserve, the Working Party suggests that the burden is on the party receiving the data to petition the US court for the appropriate protective order).
22 WP 128, note 10, at p. 19.
23 WP 158, note 6, p. 10.
24 *Id.*
25 *Id.*

(7) recognizing that sensitive personal data should be managed under Article 8, which may require, for example, the express consent of the data subject to process sensitive personal data, as well compliance with any specific Member State requirements;[26]

(8) recognizing that special categories of data, such as doctor/patient confidential materials, should be managed in exclusive ways, according to the applicable special obligations that apply in those circumstances;[27] and,

(9) ensuring that ". . . all reasonable technical and organizational precautions to preserve the security of the data to protect it from accidental or unlawful destruction or accidental loss and unauthorized disclosure or access" have been taken by the data controller, and, in this regard, the Working Party conveyed that:

> (a) these requirements are to be imposed on law firms, litigation services, experts, court services and others involved with the litigation and having access to the personal data;
>
> (b) the data controller would remain responsible for the resulting processes; and,
>
> (c) notwithstanding the data controller's ultimate responsibility, third party recipients should be bounded by the principles of the Directive, process the data only for the specific purposes for which it was collected, comply with the retention periods and maintain the data's confidentiality.[28]

Transfer to Third Countries

As we think the above analysis demonstrates, the Working Party has helped multinationals to identify a mechanism by which personal data that is truly relevant and necessary for US litigation may be processed by the data controller pursuant to Article 7(f) when adequate safeguards are in place. The final question is whether the same data may be lawfully transferred to the United States to fulfill the data holder's legal obligations in discovery. The Working Party clearly answered this question in the affirmative. What is less clear by its guidance is which of the several procedural mechanisms are available to justify the transfer, or under what circumstances each transfer protocol may be used lawfully to transfer personal data.

The Working Party, for example, states its preference of the use of Binding Corporate Rules (BCRs) or Safe Harbor where a significant amount of data is to be transferred.[29] Neither of these, however, are traditionally viewed as valid transfer options when dealing with the fulfillment of US discovery obligations. BCRs are designed for use with regard to the transfer of personal data *within the same corporate group* at a multinational level.[30] Moreover, BCRs require approval by the national data protection authority having jurisdiction over the personal data in question, a condition that is not likely to exist in most cases when litigation arises. More to the point, the Working Party has made it clear in prior writings that BCRs cannot be used to justify onward transfers to third parties that are not part of the BCR corporate group.[31]

Reference to use of Safe Harbor as a transfer mechanism for US discovery purposes seems equally misplaced. Safe Harbor is a procedure designed to create the presumption of adequate data protection standards by signatory corporations and permits transfer amongst those corporations that are Safe Harbor recognized. Onward transfer to non-qualified third persons for discovery purposes is prohibited.[32]

---

26 *Id.*
27 *Id.*
28 WP 158, note 6, p. 12.
29 *Id* at p.13.
30 Working Party, Working Document: Transfers of Personal Data to Third Countries: Applying Article 26 (2) of The EU Data Protection Directive to Binding Corporate Rules for International Data Transfers, at 6, 11639/02/EN, WP 74 (June 3, 2003) [hereinafter WP 74].
31 *Id.* at p. 10-11 ("Transfers of personal data to companies outside the corporate groups would remain possible but not on the basis of arrangements put in place by legally enforceable corporate rules but on the basis of any other legitimate grounds under Article 26 of the Directive . . . ").
32 *U.S. Department of Commerce, Safe Harbor Privacy Principles* (July 21, 2000) (can be found at www.export.gov/safeharbor/SH_Privacy.asp).

Presumably in recognition of these limitations, the Working Party refers to the Hague Convention and "urges that this approach should be considered first as a method of providing for the transfer of information for litigation purposes."[33] Proceeding under the Hague Convention, however, also has significant limitations, some of which the Working Party recognizes.[34]

Perhaps in recognition of these limitations concerning BCRs, Safe Harbor, and the Hague Convention, the Working Party cautiously acknowledges that "[w]here the transfer of personal data for litigation purposes is likely to be a single transfer of all relevant information, then there would be a possible ground for processing under Article 26(1)(d) of the Directive where it is necessary or legally required for the establishment, exercise or defence of legal claims."[35]

Article 26(1) of the Directive identifies the exceptions to the rule of Article 25 that precludes onward transfer of personal data to countries not providing an adequate level of data protection.[36] Article 26(1)(d) permits such a transfer to a third country if "the transfer is necessary . . . for the establishment, exercise or defence of legal claims."

The implication in WP 158 that discovery obligations imposed by US litigation justifies a transfer under Article 26 (1)(d) "for the establishment, exercise or defense of legal claims" is supported by a similar conclusion reached by the Working Party in its prior writing, in which it demonstrated the reach of this exception by referring hypothetically to the permitted transfer of personal data by an EU subsidiary to its US parent in defense of a claim brought by an employee of the parent in a US court.[37]

It is also worth noting that in a prior writing the Working Party noted that ". . . this exception [Article 26(1)(d)] can only be applied if the rules governing criminal or civil proceedings applicable to this type of international situation have been complied with, notably as they derive from the provisions of the Hague Conventions of 18 March 1970 ("Taking of Evidence" Convention) and of 25 October 1980 ("Access to Justice" Convention).[38] While not clear, it is presumed that the Working Party does not mean by this reference that application must first be made to proceed under the Hague Convention but rather that all the same safeguards must be "complied with." A contrary interpretation would be inconsistent with the Working Party's current position that "urges," but does not require, use of the Hague Convention when that procedure is potentially available.

An Imperfect Solution

In WP 158, the Working Party has plotted a course through the maze that stands before those multinational corporations caught between US discovery and EU data privacy laws. The Working Party's philosophy appears to be that, although not easily traveled, at least one route can be safely negotiated largely by demonstrating respect for, and thereby achieving compliance with, the spirit and the letter of both sets of rules.

Two years ago, a number of data privacy and legal commentators called for a sort of hybrid approach to the above problem by suggesting a standardized set of "legal processes protocols."[39] The proposed solution closely resembles the model suggested by the Article 29 Working Party. In an article published in *Privacy & Security Law*, Crosley *et al.* argued that "U.S. discovery processes are not necessarily antithetical to European values" and that the "debate has vastly overstated these differences." More importantly, though, the authors offered a practical way forward; they maintained that "the key to a long term-solution to this issue is to achieve an understanding that the processing of EU personal data in compliance with U.S. discovery rules should be treated as legitimate when conducted within a framework of stringent legal process data protection controls."

33 WP 158, note 6, p. 14.
34 *Id.* at p. 13 (". . . not all Member States . . . have signed . . . and even if a State has signed it may be with reservations.").
35 WP 158, note 6, p. 13.
36 WP 114, note 8, p. 6.
37 *Id.* at p. 15.
38 *Id.*
39 *See* "A Path to Resolving European Data Protection Concerns with U.S. Discovery," Crosley, Raul, McNicholas, and Dwyer in *Privacy & Security Law*, Vol. 6, No. 41, (October 15, 2007).

Crosley *et al.*, further suggested that "[a] scheme of legal process protocols could well form the basis to initiate a dialogue with EU authorities . . ." and that these "protocols" could contain: 1) "extensive advance notice" and disclosure to employees (and any other data subjects); 2) a comprehensive "EU Data Protective Order" and/or "an EU Model Contract for data transfers incident to discovery;" 3) the use of a special Protective Order; and 4) the use of a Special Discovery Master. The authors contemplated that this protocol would provide "clear and complete" disclosure to the EU employees of multinationals that describe "the data processing method, identify prospective data recipients, and inform data subjects of their rights under applicable U.S. law and EU data protection laws . . . as well as the means for enforcing those rights." The authors argued that "such disclosures may most easily take the form of a special section of, or addendum to, the company's privacy policy . . . ."

The authors then suggested that "a special protective order, issued by the U.S. Court, specifically to address EU data protection concerns about the processing of personal data during litigation" would also help effectuate the proportionality principle – or the idea that the data to be transferred be "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed." Such a protective order could restrict the scope of the disclosures ordinarily allowed under U.S. discovery rules, possibly by allowing processing of EU documents containing personal data only when they are demonstrated to be directly relevant to the issues presented, as opposed to being merely "reasonably calculated to lead to the discovery of admissible evidence."[40] Finally, and in order to ensure "transparency both to data subjects and EU data protection authorities" the protective order could contain, they suggested, the appointment of a "special discovery master to monitor compliance with EU data protection requirements."

In the end, the mechanisms for data transfer mentioned above are all systemic. At their core, they are all compliance regimes that take time and infrastructure to implement. The hybrid approach proposed by Crosley *et al.* is creative but also seems to rely on approval by some greater authority and this seems a bit unwieldy. What we need is an easily deployed and self-authenticating approach: a single document that captures the spirit of compliance with data privacy but does not require layers of bureaucracy to implement. What we need is a new approach.

A New Approach: A Proposed Certificate of Compliance for the Transfer of Data Across Borders

While the suggested approach by Crosley *et. al.* makes sense and certainly is better than the current state of affairs, the solution may be made even more pragmatic and simple to effectuate. For example, requiring a special master to oversee any transfer of personal data out of the EU will be cumbersome and unwieldy – whether in the context of litigation or even for an informal investigation. What would a multinational corporation do, for example, when faced with a U.S. government investigation involving the transfer of data from employees located in one of their offices in Europe but where no formal legal proceeding had been filed in the U.S.? Should the company or counsel hire a retired judge, as they might in the case of arbitration, and have that individual oversee the process? This would take time, resources, and would require educating someone on EU privacy and the local laws of the countries from where the data was being exported. In short, it would be unduly burdensome and, in the end, perhaps unworkable.

Adherence to any data privacy law, whether in the EU or in any other part of the world, is about compliance. Different countries have different views on what is public and private information. These ideas are fundamental. And as such, they are a function of national identity and the human experience as it has developed in that part of the world. Companies, however, now operate in every part of the world. And in order to conduct business in different parts of the planet, the individuals who run those companies need to be mindful, respectful, and *comply* with the laws and norms of the places in which they operate.

40 *See* U.S. Federal Rule of Civil Procedure 26.

What if a multinational company and its counsel could create a single document that addressed data privacy laws in the European Union (or elsewhere) but did not require them to simultaneously create an entire compliance program dedicated to the transfer of data out of the EU? The document, much like the Model Contract suggested by Crosley *et al*. above, would address the various requirements of the 95/46 Directive as well as the ideas set forth in WP 158, drafted by the Article 29 Working Party. It would also simplify the process for a company and its counsel so that compliance would be more likely because it would be self-authenticating.

Such a document – or a Certificate of Compliance for Transfer of Personal Data Across Borders (hereinafter "Certificate of Compliance") – would accompany the data (like a modern day bill of lading that accompanies physical cargo) from one jurisdiction to another. Further, this document would be filed with the local DPA as evidence that the company and counsel that seek to transfer that data are aware of the data privacy laws of the country where the data resides, understand their obligations under those laws, and will *comply* with the data privacy restrictions of the country in which they operate.

The Certificate of Compliance would contain the following provisions: 1) a statement concerning the purpose for which the data is being collected and confirm that the data will not be used for any other purpose (this would include a brief description of the litigation, investigation, or matter in the U.S. as well as the recipient of the data); 2) a statement as to how and when the data will be collected (this would include time, date, by whom and with what technical tool the data will be collected); 3) that all reasonable measures are being taken in order to limit what data is being collected (for example, that search terms will be run against the data in order to narrow the data set to only the most relevant information and confirming that the non-responsive data will not be processed along with the responsive data); 4) an identification of the types of data that will be collected (e.g., email, Word documents, PowerPoint, etc.).

The Certificate of Compliance should also: 5) confirm that this data is subject to a protective order and include a copy of the protective order as an attachment to the Certificate of Compliance (the protective order should specifically mention the EU privacy law that governs the transfer of data and confirm compliance with same, limit the number of individuals who will have access to the EU-transferred data, and provide consequences if the data privacy law is not complied with); 6) set forth the resources available to the employee should they have questions about their privacy rights (at a minimum, this would mean identifying the appropriate DPA in the applicable country and a means to contact the DPA office); 7) confirm that all reasonable steps will be taken in order to protect the data from accidental or unlawful destruction; 8) confirm that a copy of the Certificate of Compliance has been filed with the proper DPA; and 9) identify and include the signature of the person responsible for overseeing the collection, processing, review, and production of the data (most likely the attorney overseeing the matter or the company's privacy officer).

A Certificate of Compliance can, and should be, this straightforward and simple. As Crosley *et al*. have suggested, the current debate between complying with data privacy laws while still being able to conduct discovery under the U.S. federal rules has been "vastly overstated." Companies that operate in the United States but with offices located abroad want to do the right thing. Until now, however, there has not been a workable solution to this conflict of legal obligations. Furthermore, the Article 29 Working Party "sees the need for reconciling the requirements of the US litigation rules and the EU data protection provisions. [And] [i]t acknowledges that the Directive does not prevent transfers for litigation purposes . . . ."[41]

A Certificate of Compliance is the first step. It is practical, easily deployed, and attempts to address the data privacy concerns raised by both the Directive and the recent paper by the Article 29 Working Party. What companies and their counsel really need, though, is a long term solution to a problem that will only continue to expand. The Hague Evidence Convention has the four walls and

41 *See* the Article 29 Working Party paper: "Working Document 1/2009 on pre-trial discovery for cross border Civil litigation," at http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2009/wp158_en.pdf.

the beginning of a solid foundation upon which to build a meaningful multi-lateral treaty for collecting electronic evidence from abroad. But the treaty needs a renovation. It needs to read like a modern document that understands how information moves, is stored, and can be collected with the click of a button. The next part of this paper is a look at the current Hague Evidence Convention, its use or non-use, and makes some suggestions of what a new treaty should look like.[42]

A Long Term Solution: Rethinking the Hague Evidence Convention

In terms of its usefulness to conduct e-discovery across borders, the Hague Evidence Convention is in dire need of help. The treaty suffers from a number of failings, some self-imposed, some imposed by interpreting bodies. First, and in light of the U.S. Supreme Court's decision in *Aérospatiale*, the treaty has essentially become "discretionary" for U.S. and foreign litigants in U.S. courts.[43] Second, Article 23 of the treaty specifically permits a contracting State to "declare that it will not execute Letters of Request issued for the purpose of obtaining pre-trial discovery of documents as known in Common Law countries."[44] Third, the Convention does not take into consideration the data privacy laws of many countries. Fourth, the Convention does not offer a solution to the issue of "blocking" statutes. Finally, requests for e-discovery under the Convention are "rare"[45] and the Convention offers no real guidance for conducting e-discovery abroad.

In 1970, the United States signed on to the Hague Convention on the Taking of Evidence Abroad in Civil and Commercial Matters. Pursuing discovery through this treaty, it seemed, would establish a formalized process for conducting discovery abroad. But that was not to be. In *Aérospatiale*, a French aircraft manufacturer, defending a plane crash case in Iowa, argued that the Convention was the sole means of gathering evidence within the territories of the contracting countries, including France and the United States.[46]

After determining that the Convention was not a preemptive replacement for the Federal Rules, the Supreme Court considered two possibilities: first, that international comity required "a first resort" to use of the Convention procedures; or second, that the Convention contains alternative procedures which American courts have the option of employing.[47] With a narrow 5-4 split, the Court rejected a rule requiring "first resort to Convention procedures" and instead held that in each case trial courts determine whether to apply Convention procedures or the Federal Rules after considering three things: "(1) the particular facts, (2) sovereign interests, and (3) the likelihood that resort to [Convention] procedures will prove effective."[48]

In May 2008, the Permanent Bureau of the Hague Conference on Private International Law issued a questionnaire to Member States and State Parties in preparation for the Special Commission Convention which was held in February 2009. The goal of the questionnaire and the convention were to define key issues facing the Hague Evidence Convention as well as "assist the Permanent Bureau in drafting parts of a possible new edition of the Practical Handbook on the Operation of the Evidence Convention and/or a possible Guide to Good Practice" in relation to specific issues arising from the operation of the Convention.[49]

The Permanent Bureau drew a number of interesting conclusions from the responses to the questionnaire. Among them, the Bureau found that "the statistics provided by responding States do

42 As the Article 29 Working Party acknowledged in the 11 February 2009 white paper: "Although this paper sets out guidelines it is to be noted that resolving the issue of pre-trial discovery is beyond the scope of an Opinion by the Working Party and that these matters can only be resolved on a governmental basis, perhaps with the introduction of further global agreements along the lines of the Hague Convention."

43 In *Société Nationale Industrielle Aérospatiale v. United States District Court*, 482 US 522 (1987), the Supreme Court determined that the Hague Convention did not displace the Federal Rules in relation to foreign-based discovery; rather, it was a permissive supplement. *See also* "The Mandatory/Non-Mandatory Character of the Evidence Convention" issued by the Permanent Bureau of the Hague Conference on Private International Law, 10 December 2008.

44 *See* Article 23 of the Hague Evidence Convention.

45 *See* "Summary of Responses to the Questionnaire of May 2008 Relating to the Evidence Convention, with Analytical Comments," drawn up by the Permanent Bureau, February 2009 at http://www.hcch.net/index_en.php?act=text.display&tid=48.

46 *Id.* at 524-525, 529.

47 *Id.* at 529, 533.

48 *Id.* at 538, 544.

49 *See* p. 4 of "Summary of Responses to the Questionnaire of May 2008 Relating to the Evidence Convention, with Analytical Comments," (hereinafter "Summary Report") drawn up by the Permanent Bureau, February 2009 at http://www.hcch.net/index_en.php?act=text.display&tid=48.

not permit many firm conclusions to be drawn, however it is possible to say with some confidence that the Convention appears to be widely used, with, at very least, over 1500 uses of Chapter I, and 2500 uses of Chapter II, in 2007."[50] The Bureau also found that the "high use of the Convention is reflected in a high level of overall satisfaction with the Convention."[51] Finally, the Bureau made a number of important recommendations regarding the timeliness of responding to Letters of Request (4 months if the request was for oral evidence and 6 months for "all other requests.").

The report also included a number of observations on e-discovery and blocking statutes. It found that "requests for e-discovery are rare, but are becoming a reality."[52] The report noted that "some such requests have been successfully executed . . . [but] very few data are available on the practical difficulties that can arise in respect of such requests."[53] The report then concluded that "requests for discovery relating to electronically stored information are likely to increase . . .[and that] such requests should be treated in the same manner as requests for hard copy documents." As for blocking statutes, the report noted that "blocking statutes are reasonably common, but far from universal. [W]here they do exist, such Statutes are rarely used."[54]

Unfortunately, what the report did not include are practical solutions to the issue of conducting e-discovery across borders. In light of a recent French Supreme Court decision,[55] it also likely underestimates the likelihood that States will begin to enforce their blocking statutes where they are made aware that protected information is being disclosed pursuant to a foreign court proceeding. What, then, should the Bureau have recommended in terms of conducting e-discovery abroad? What should it have recommended in terms of blocking statutes?

A new Hague Evidence Convention needs to do more than just "recognize" e-discovery, blocking statutes, and data privacy concerns around the globe. While the details of a new international treaty is too ambitious for this paper and outside of its intended scope, we applaud the Working Party's recognition that a more perfect solution to the cross-border discovery conundrum lies in "further global agreements" between the EU, US and other sovereignties. We believe that any real long term solution mandates immediate steps in that direction.

We think, as well, that to begin to construct a workable multinational accord, a concerted analysis is needed to determine the shortcomings of today's Hague Convention. We believe that by studying what has not worked, and the frustrations experienced by multinationals trying to comply with seemingly inconsistent laws, the best resolution can be obtained, and a new Hague Evidence Convention can rise like a phoenix from the ashes.

We therefore suggest that the contours of any new treaty or modifications to the Hague Convention begin with at least the following considerations:

1. The process for application to the international tribunal to aid in cross-border discovery or transfer of data must be simple, expeditious, reliable and repeatable;

2. The determinations made by the international tribunal must be prompt, capable of enforcement and willingly enforced by the signatory countries;

3. *Aérospatiale* must be abandoned or at least set aside in those cases where application is made to the international tribunal for enforcement of discovery orders;

50 Interestingly, of the 1500 requests under Chapter I, 477 of those requests were for oral testimony, 215 of the Requests for documentary evidence, 77 requests for bank records, and 55 requests were for written interrogatories. In short, the majority of the requests did not involve e-discovery. *See* p. 16 of the Summary Report.

51 See page 6 of the report. Interestingly, when one looked at the actual responses of the Member states a slightly different story also emerged. For example, in responding to the question: How do you rate the Convention? India responded: "Excellent. Prima-facie the objects of the Convention appear to be excellent. However since no request have been received for execution under the Convention, no specific comments can be provided at this stage." For a full copy of the Member State responses go to: http://hcch.e-vision.nl/upload/wop/2008synopsis20.pdf.

52 See page 51 of the Summary report.

53 *Id.*

54 See p. 26 of the Summary Report.

55 Cour de Cassation Chambre Criminelle [Cass. Crim.], Paris, Dec. 12, 2007, Juris-Data no. 2007-332254 (France's Supreme Court upheld criminal conviction and fine against French attorney for conducting a private investigation on behalf of US litigants, finding that information sought was of an economic, financial, or commercial nature and was aimed at collecting evidence for use in a foreign judicial procedure).

4. Blocking statutes must be abandoned or at least set aside in those cases where application is made to the international tribunal for enforcement of discovery orders;

5. The laws of each signatory country must be respected but compromise also must be expected so that fairness and reasonableness should always prevail; and,

6. When the scope of discovery in one country encroaches on the rights of individuals of the another country, those courts involved and the international tribunal should resort to a tiered approach that prioritizes discovery on a sliding scale basis. This means, for example, that discovery that is least objectionable and mostly of a business nature should be made available first and based on broad concepts of relevancy and materiality. Discovery that infringes on individual rights should require a higher burden of persuasion and would be permitted pursuant to a more narrow scope as to what is relevant and material. Discovery that seeks highly sensitive information of a private or delicate nature should not be permitted absent a showing of 'good cause,' meaning that the information is necessary, is not otherwise available from other sources and that the request is not intended to embarrass or harass.

Conclusion

These six concepts are familiar to courts in almost every country. As Crosley, *et al*. determined, we are not all that much different. Basic concepts of 'search for the truth' and 'respect for individual rights' are the cornerstones of the judiciaries of both the European Union and the United States. The differences, and therefore the friction, arise more because of a fear of the unknown. By developing an international framework that is speedy, reliable and one that fairly resolves cross-border discovery issues, consistent with data privacy rights, these biases, we are confident, will cease to exist.

Epilogue by The Sedona Conference®

On June 10-11, 2009 The Sedona Conference® held its International Programme on Cross-Border eDiscovery, eDisclosure & Data Privacy Conflicts in Barcelona, Spain. The preceding paper was presented at that conference and subject to dialogue by the almost 100 conference participants and faculty from The Sedona Conference®, the European Commission, various EU member state Data Protection Authorities, the US and UK judiciary, the US State Department, and the US National Archives and Records Administration, as well as lawyers and others from more than 10 countries.

The conference began with a keynote address by Dr. Alexander Dix, the Commissioner for Data Protection and Freedom of Information, Berlin, Germany, and Chair of the Article 29 Working Party Subgroup on Cross-Border Discovery. That was followed by a series of discussions regarding the recent Article 29 Working Party Document 158 on pre-trial discovery for cross border civil litigation, and the recently-published Sedona Conference® Framework for Analysis of Cross-Border Discovery Disputes (available free for download and personal use at www.thesedonaconference.org).

Day One of the conference continued with discussion of similar issues found within arbitration and ADR, including the sufficiency of ADR procedures to satisfy the privacy of data concerns and exceptions found in the EU Data Privacy Directive Article 29. There was also discussion of the four current data-transfer paradigms (the Hague Evidence Convention, the US Safe Harbor Program, Binding Corporate Rules, and Model Contracts) and the imminent Mutual Legal Assistance Treaty (MLAT), their applications and their limitations.

Day Two of the conference focused on practical solutions, with the preceding paper providing the background and stimulus for the dialogue. Thus, the participants reviewed and discussed the concept of a "certificate of compliance" with nine content and procedural elements that would address personal privacy, risk awareness, and data protection around specific collections of information.

After the conference, The Sedona Conference® held a short meeting of its International Working Group on Electronic Information Management, Discovery and Disclosure (WG6). At that meeting, it was agreed that WG6 would provide a formal response to the Article 29 Working Party Document 158, and, using the preceding article as a starting point, prepare a sequel to its Framework for Analysis paper focusing on practical solutions for accomplishing cross-border data transfers in civil litigation consistent with the EU Data Privacy Directive, and other statutes and rules governing pre-trial discovery and data transfers across borders.