



COZEN  

---

O'CONNOR®

500 Attorneys • 22 Offices

[www.cozen.com](http://www.cozen.com)

# International eDiscovery Disputes

*Presented by:*

Thomas M. Jones  
Cozen O'Connor  
17 June 2009  
Paris

Privileged and Confidential Materials. The opinions  
contained herein are the opinions of Cozen O'Connor only.

# I. Data Privacy in the U.S.

---



- The United States is a global outlier regarding concepts of privacy and data security. Its unique approach to data privacy and security can best be understood in a historical context, in contrast to other developed countries.

# I. Data Privacy in the U.S.



- Unlike most other developed countries that take a more expansive view of data privacy and security, the U.S. limits data privacy and security to specific types of personal information such as medical (HIPAA), consumer credit (FACTA), social security information, and financial information. In the U.S., for example, it is generally accepted that employees have no data privacy and security rights: that the employer owns all information created, received or stored for company business. In numerous instances, personal data, including name, address, telephone number and more are routinely gathered into marketing databases, and then sold to the highest bidder to fuel mail and internet marketing and profiling efforts.

## II. Differing Notions of Privacy



- In contrast, the European Union and most other developed countries take a more global approach to data privacy and security, embracing it as a fundamental human right. For example, under the EU Data Protection Act of 1995, Employees have an express right to privacy with respect to any information that identifies them directly or indirectly. The collection of personal information in corporate databases, and its use in marketing and advertising are unthinkable violations of this fundamental right.

## II. Differing Notions of Privacy



- Most data protection schemes extend protection to any information that identifies or could be used to identify an individual—their very definition of personal data. Under this broad definition, even a simple company directory, or an email that identifies a sender or recipient are considered personal data worthy of protection.

## II. Differing Notions of Privacy



- Another major difference between how the U.S. and other countries approach data privacy and security relate to the processing and transfer of personal data. Historically, in the U.S., any concern about invasion of personal privacy has taken a back seat to economic interests.
- The internet, in particular, has been fertile ground for all manner of innovative tracking of user preferences, buying patterns, as well as social networking in service of the sale. In this value system, it is understandable that data privacy and security interests have been eroded.

# III. U.S. Data Privacy and Security—Security Breaches



- The widespread collection and sale of personal information in the United States for commercial marketing purposes and the significant number of security breaches of governmental, corporate and nonprofit data repositories that have resulted in the compromise of sensitive personal information has led to a crisis of confidence in the ability of technology to protect this interest.
- Recent examples include:

# III. U.S. Data Privacy and Security—Security Breaches



- March 6, 2009: Loss of 50,000 consumer personal records from UPS, Idaho National Laboratory
- March 21, 2008: Loss of 1 million customer personal and financial records from a stolen Compass Bank laptop computer;
- March 12, 2008: Loss of 10,000 social security numbers and personal data from a Harvard University database;
- January 29, 2008: Loss of 38,000 social security numbers and other personal information from a hard drive stolen from Georgetown University;
- January 17, 2008: Loss of 650,000 credit card numbers and Social Security numbers of GE Money customers from a missing backup from an Iron Mountain facility.

## IV. Common Characteristics of the EU Directive and Similar Acts



- The EU Data Protection Directive and similar data privacy schemes impose strict limitations on the processing and transfer of personal data, in an effort to avoid these kinds of breaches. Neither processing nor transfer can occur under these Acts without specific regulatory authorization.

## IV. Common Characteristics of the EU Directive and Similar Acts



- The EU Directive and similar Acts define the act of “processing” as “any operation or set of operations,” whether manual or automated, including but not limited to “collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction:” *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.*

## IV. Common Characteristics of the EU Directive and Similar Acts



- By comparison, in the U.S., “processing” is generally understood as only technical actions applied to data, such as conversion from one format to another, de-duplication, high-level filtering, indexing and statistical sampling. These deep semantic differences are the cause of a “failure to communicate” on how to harmonize the legitimate interests of data privacy and for cross-border discovery.
- As noted above, in the United States, personal data would ordinarily be viewed as something very unique to a person, and data with a high degree of sensitivity, such as their medical records, their social security number, their personal address and telephone number, and their banking records. This, under the EU Directive and similar legislation, is given the status of “personal sensitive data”; and is afforded even greater protection.

## V. The Problem of Cross-Border Discovery Conflicts



- Currently, many organizations and individuals find themselves between a rock and a hard place with respect to data privacy and security demands on the one hand, and the need to conduct cross-border discovery on the other.
- In the U.S., organizations risk sanctions for failure to comply with sweeping discovery requests permitted by the U.S. court rules, because relevant data generally includes at least some personal data.

## V. The Problem of Cross-Border Discovery Conflicts



- Outside the U.S., organizations risk sanctions under Data Protection regulations and blocking statutes. In a recent 2008 case, *In Re Christopher X*, the French Supreme Court affirmed a conviction and €10,000 fine for a French attorney for violating the French Blocking Statute. The French Blocking Statute prohibits the collection of information in France for the purpose of a judicial or administrative proceeding outside of France. Other countries have similar blocking statutes.

## V. The Problem of Cross-Border Discovery Conflicts

---



- In this case, the French Advocat was simply acting on behalf of U.S. co-counsel in a matter filed in the United States. The specific act that was found improper was that of approaching, in Paris, a former director of one of the litigants to determine whether he had knowledge relevant to the litigation in the United States.

## VI. The Work of The Sedona Conference® and the Article 29 Working Party



- Since 2004, The Sedona Conference® & International Working Group on Electronic Information Management, Discovery and Disclosure (WG6) has worked to educate clients, courts and counsel regarding the practical implications of data privacy and security in the cross-border context. These issues are examined in greater detail in *The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy & e-Discovery—Public Comment Version (2008)*, available at [www.thesedonaconference.org](http://www.thesedonaconference.org).

## VI. The Work of The Sedona Conference® and the Article 29 Working Party



- The Sedona Framework document was relied upon by the Article 29 Working Party in publication of its recent *Working Document 1/2009 on Pre-Trial Discovery for Cross-Border Civil Litigation (WP 158)*, [www.ec.europa.eu/justice/home/fsj/privacy](http://www.ec.europa.eu/justice/home/fsj/privacy). The Article 29 Working Party refers is the group established under Article 29 of the EU Directive to apply its principles to specific factual situations.

## VII. Traps for the Unwary and Tips to Avoid Them



- Both U.S. and non-U.S. data privacy and security professionals need to know how to navigate the competing currents of data privacy and security and cross-border discovery in the context of litigation and regulatory investigations. Here are several practice pointers to help avoid injury between the “rock and the hard place” of data privacy and security and cross-border discovery:

## VII. Traps for the Unwary and Tips to Avoid Them

---



- Engage local counsel in the particular jurisdictions for guidance as to local laws, both procedural and substantive, because they vary from country to country.
- Explore whether your organization is eligible for certification under the U.S. Department of Commerce Safe Harbor provision, if so, consider doing so.

## VII. Traps for the Unwary and Tips to Avoid Them

---



- Understand the developing U.S., data privacy and security landscape. Many organizations have been caught off guard with respect to emerging U.S. requirements, such as mandatory destruction of stale consumer credit information under FACTA; and many more have not yet taken steps to comply with the new Red Flag Rules that go into effect in May 2009.

## VII. Traps for the Unwary and Tips to Avoid Them

---



- Consider the use of “in-country” culling of information for cross-border discovery purposes so as to limit the amount of relevant personal data that needs to be transferred to the bare minimum.
- Consider the use of a “Data Privacy & Security Regulated” category for information that is collected outside the U.S.

## VII. Traps for the Unwary and Tips to Avoid Them

---



- Include provisions in case management orders and protective orders that help protect the privacy and security of personal data that is processed or transferred in the context of cross-border litigation and regulatory activity.
- Consider the data privacy implications of moving IT data centers from non-U.S. locations to U.S. locations.

## VII. Traps for the Unwary and Tips to Avoid Them

---



- Include data privacy and security standards in the development of new systems and applications that contain personal or personal sensitive data, as defined by countries in which your organization does business.

## VII. Traps for the Unwary and Tips to Avoid Them

---



- Participate in the efforts of groups such as The Sedona Conference®, the International Association of Privacy Professionals, the International Chamber of Commerce, the Defense Research Institute, the American Bar Association and others in finding common ground between U.S. and non-U.S. data privacy and security requirements.

## VII. Traps for the Unwary and Tips to Avoid Them

---



- Help educate the bench and bar as to the increasing scope of data privacy and security statutes and regulations.
- Establish a process, with the help of your Chief Security Officer, to develop and update policies, procedures, practices and processes to ensure compliance going forward.

- ## Trends



- A global trend appears to be emerging regarding data privacy and security. On the one hand, the U.S. is experiencing a piecemeal proliferation of specific data privacy and security regulations, in partial response to significant data privacy and security breaches, and increases in frequency of identify theft. Outside the U.S., the EU and other regions are becoming more aware of the practical costs imposed by broad-based data privacy and protection regulations that create a dangerous “Catch 22” for multinational businesses.

- ## Trends



- The author predicts that this convergence trend will continue, and that, in time, the U.S. will embrace a more global, rather than sectoral, approach to data privacy and security. The administrative and societal costs of not doing so are simply too high. Similarly, the author predicts that the data privacy and security schemes in place in the EU and other countries will be softened somewhat, particularly in light of the global economic crisis, so as to more fairly balance economic interests with those of personal privacy.



# ***EU Article 29 Data Protection Working Party Document on Pre-Trial Discovery for Cross-Border Civil Litigation***

# I. Executive Summary



- On February 11, 2009, the Article 29 Data Protection Working Party issued a “Working Document” on the issue of pre-trial discovery for cross-border civil litigation (WP 158). The significance of this document is that it expressly acknowledges, for the first time, the tensions between data privacy concerns of EU Member States and the legitimate need to conduct discovery for cross-border litigation. The Article 29 Working Party acknowledges the assistance of The Sedona Conference® International Working Group on Electronic Information Management, Discovery and Disclosure (WG6) in this effort, through its 2008 public comment draft *Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery* (available free at [www.thesedonaconference.org](http://www.thesedonaconference.org)).

# I. Executive Summary



- Although the Working Document provides some suggestions for mitigating this tension, it is not a final opinion, but only “an initial consideration of the issue of the transfer of personal data for use in cross-border civil litigation” (WP 158, p. 14). In the words of the Article 29 Working Party, it is “an invitation to public consultation with interested parties, courts in other jurisdictions and others to enter a dialogue with the Working Party,” rather than a fully developed set of principles and guidelines. *Id.* This Working Document limits its discussion to 1) Preemptive document preservation in anticipation of proceedings before U.S. courts or in response to requests for litigation hold, known as “freezing;” and 2) Pre-trial discovery requests in U.S. civil litigation. It does not address the issues of 3) Document production in U.S. criminal and regulatory investigations; and 4) Criminal offences in the U.S. relating to data destruction (WP 158, p. 3).

# I. Executive Summary

---



- The Working Party acknowledges that resolving even the first two issues is beyond the scope of an Opinion of the Working Party, and that they can only be resolved on a governmental basis by agreements such as the Hague Convention. Nevertheless, in the meantime, it provides the following suggestions and guidelines for clients, counsel and courts:

# I. Executive Summary

---



- Encourage the use of protective orders by foreign courts (including the U.S.) to limit discovery and/or protect the privacy of personal information that is processed or transferred to the U.S. for litigation;
- Encourage initial recourse to the Hague Convention, where possible, as a mechanism for cross-border discovery;
- Strictly scrutinize and limit the retention of personal information simply because it might be relevant to future, reasonably foreseeable litigation;

# I. Executive Summary



- Provide data subjects with a real opportunity to give clear and unambiguous consent to use of their personal data for this purpose, with a real opportunity to withdraw consent without retaliation of any kind;
- Where personal data is processed, provide data subjects with notice of the identity of any recipients, the purposes of the processing, the categories of data concerned and the existence of their rights, even where the data is being collected from a third party, and delaying such notification only so long as is needed to avoid a substantial risk or jeopardy an ongoing; criminal or civil investigation of wrongdoing;
- Check whether there is a legal basis for compelling the host country to comply with an order of a court in another jurisdiction seeking discovery;

# I. Executive Summary

---



- Include adequate safeguards against the unauthorized retransmission, onward transfer or modification of the personal data to be processed and transferred;
- Take appropriate steps in the host country to filter, redact, render anonymous data or employ pseudonym with respect to data, so as to limit the discovery of personal data to the smallest amount that is objectively relevant to the issues being litigated;
- Use of an independent, trusted third party expert in the Member State to make relevance determinations as to any personal data to be transferred;

# I. Executive Summary

---



- Involve the data protection officers at the earliest stage to help counsel the parties and to educate foreign courts, and to request U.S. courts for relevant protective orders to comply with EU and national data protection rules;
- Take reasonable steps to preserve the integrity and security of the personal data in handling by external service providers such as law firms, litigation support service vendors and experts;

# I. Executive Summary



- Requiring external service providers to collect, filter, review and otherwise process personal data only for the specific purposes for which it was collected, abide by strict confidentiality obligations, communicate with only specified persons about the data, comply with retention restrictions, and periodically be verified as compliant with these obligations by the data controller;
- Retain custody of the personal data for only as long as the specific action is pending; and
- Consider the use of Safe Harbor or Binding Corporate Rules for a single transfer or all relevant information relating to a matter, except for future, reasonably anticipated litigation.

## II. Background



- Article 29 of Directive 95/46/EC establishes the Working Party on the Protection of Individuals with regard to the Processing of Personal Data (“Working Party”) and charges the Working Party with, among other things, making “recommendations on all matters relating to the protection of persons with regard to the processing of personal data in the Community.” Working Document 158 is intended to give guidance to data controllers who are subject to EU law (*i.e.*, those individuals within a company who may be in a position to direct the processing and/or transfer of personal data) in dealing with requests in the context of cross-border civil litigation and regulatory investigations.

## II. Background



- The Working Party acknowledges that there are two schemes under which personal data may be obtained for use in non-EU litigation—the Hague Convention on the “Taking of Evidence Abroad in Civil and Commercial Matters and the EU Directive 95/46. The Working Party encourages parties to utilize the Hague Evidence Convention as an initial method of obtaining data, but also acknowledges that some Member States, such as France, Germany, Spain, and the Netherlands, signed the Hague Evidence Convention with reservations that preclude the discovery of any information if the information is to be used in foreign legal proceedings (with limited exceptions).

## II. Background

---



- Recognizing the limitations of using the Hague Evidence Convention, the Working Party provides guidance for data controllers who are increasingly faced with demands to process and provide data for U.S. legal matters. While the Working Party is attempting to balance the competing interests of parties who need information to make or defend a legal claim and individuals whose personal data should be protected from disclosure.

- ## Guidance for Data Controllers



- Data controllers are counseled to carefully assess whether there are proper conditions for processing personal data at each stage of the pre-trial process: retention, disclosure, onward transfer, and secondary use. While acknowledging that Working Document 158 does not carry the force of law, the Working Party appears to be trying to assist data controllers with navigating the treacherous, and often uncharted, waters of EU data processing for use in U.S. civil litigation.

- ## Guidance for Data Controllers



- A. 

### Data Processing

- The Working Party recognizes that data controllers must have one of three relevant grounds for processing personal data related to civil litigation: the unambiguous consent of the Data Subject; the need to process data as a means of complying with a legal obligation; or the need to process data as a means of complying with a legitimate interest of the data controller or a third party to whom data has been disclosed. While the Working Party notes that U.S. pre-trial discovery may not constitute a “legal obligation,” some Member States may have imposed a statutory obligation to comply with a court order from another jurisdiction.

- ## Guidance for Data Controllers



- The Working Party highlights that data controllers have an obligation to take appropriate steps to limit the disclosure of personal data to that which is objectively relevant to the issues in the litigation. Data controllers may satisfy this obligation by restricting disclosure to data that has been redacted, “anonymised or at least pseudonymised.” Further, data controllers should provide for in-country filtering of personal data in order to eliminate irrelevant data from transfer out of the source country.

- ## Guidance for Data Controllers



- The Working Party encourages data controllers to approach U.S. Courts to explain their heightened data privacy obligations and to seek appropriate protective orders.

- ## Guidance for Data Controllers



- B. 

### Notice to Data Subjects

- In order to comply with the requirements of Directive 95/46, data controllers must give the data subject notice of the possibility of personal data being processed for litigation. Further, if the data subject's personal data is actually processed, the subject must receive notice of the identity of any party that has received the subject's personal data, the purpose of the data processing, the categories of personal data that have been processed, and a notice of the data subject's right to review and rectify the personal data. Article 14 of Directive 95/46 provides a data subject with the right to object to any processing of the subjects personal data. If the data subject's objection is justified, then the data controller must remove the abject to data from further processing.

- ## Guidance for Data Controllers



- C. 

### Data Security

- Once data processing guidelines have been observed and proper notice to data subjects has been delivered, data controllers must take “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.” The principles of Directive 95/46 that apply to data controllers regarding data security also apply to other parties that may handle personal data—law firms, processing vendors, experts, and even the court personnel in the receiving jurisdiction.

## IV. Conclusion



- WP 158 is clearly a “work in process.” While it identifies a number of issues that arise between competing data privacy and cross-border discovery interests, it admittedly falls short of a solution or a clear way forward. Instead, it provides some basic, yet helpful guidance, but more importantly is a call to dialogue among affected parties and countries.

## IV. Conclusion

---



- The good news is that WP 158 demonstrates unequivocally that the European Union really understands the constraints imposed by civil discovery systems such as those in the United States. And it signals a positive willingness of the European Union to take a leadership role in helping find a way forward that respects both interests.

## IV. Conclusion



- Where this dialogue takes us is uncertain, but it, along; with *The Sedona Conference® Framework for Analysis of Cross-Border Discovery Conflicts: A Practical Guide to Navigating the Competing Currents of International Data Privacy and e-Discovery (2008)* and the work of the DRI, IAPP, AMEA, ICC and others builds a solid foundation for using dialogue to explore and develop a common vocabulary essential to finding a way forward.



COZEN  

---

O'CONNOR®

500 Attorneys • 22 Offices

[www.cozen.com](http://www.cozen.com)

Thank you.

*Presented by:*

**Thomas M. Jones**  
Seattle Office  
1201 Third Avenue  
Suite 5200  
Seattle, WA 98101

Privileged and Confidential Materials. The opinions contained herein are the opinions of Cozen O'Connor only.