

The International Impact of U.S. eDiscovery Obligations – *Managing Risk and Reducing Compliance Costs*

By: Hiren P. Patel, CEO, Aphelion Legal Solutions

The Fourth International Conference on Legal, Security, and Privacy Issues in IT Law

November 4, 2009

Sliema, Malta

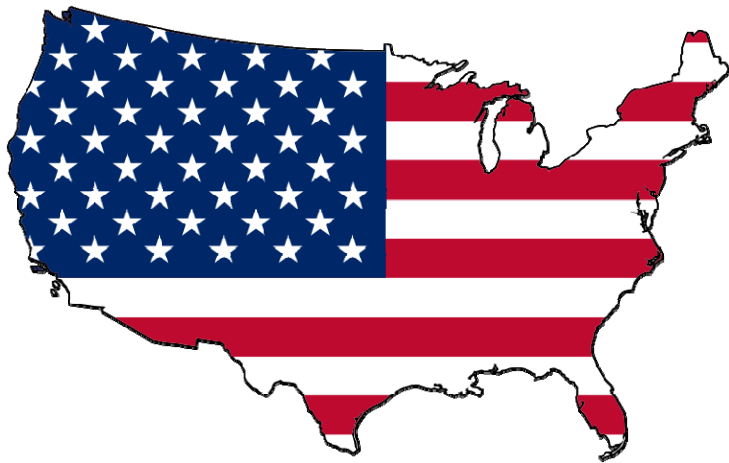
About Aphelion Legal Solutions

- ▶ Aphelion Legal Solutions provides eDiscovery consulting, managed document review, legal staffing, and legal process outsourcing services for businesses around the world.
- ▶ Aphelion's has offices in Houston, TX, Washington, DC, and Chennai, India.
- ▶ Aphelion's Founders and Managers Practiced with Top American Law Firms Prior to Founding Aphelion in 2007.

Overview

- ▶ Introduction; *In re Advocat Christopher X*
- ▶ U.S. eDiscovery Rules
- ▶ Sources of Conflict
- ▶ Judicial Responses to Sources of Conflict
- ▶ Suggested Course of Action for Multinational Businesses with Operating Units in the U.S.

Section I: Introduction



Freedom Fries

v.



French Fries

Garamendi, et. al. v. Altus Finance, et. al.

- ▶ California Insurance Commissioner initiated lawsuit against Altus, a subsidiary of Credit Lyonnais (French government controlled), MAAF Group (consortium of French and Swiss insurers), and others arising from the sale of assets of Executive Family Life Insurance, a failed insurer.
- ▶ Altus / MAAF Group exited the case early through settlement / default.
- ▶ No notable eDiscovery issues.
- ▶ But a French lawyer acting for California was fined 10,000 Euros... and this fine may have a substantial impact on cross-border eDiscovery.

In re Advocat “Christopher X”

- ▶ Christopher X made a phone call to Jean-Claude Y, a former director of MAAF, to obtain information California could use to determine whether to call Jean-Claude Y as a witness.
- ▶ This act constituted a violation of French Penal Law No. 80-538, which prohibits:
 - *requesting, seeking or disclosing ... documents or information ... for the purpose of constituting evidence in view of foreign judicial or administrative proceedings.*
- ▶ The Supreme Court of France upheld the conviction on December 12, 2007. This is the first known case where France’s blocking statute was used to punish an individual for discovery-related actions.
- ▶ And it exemplifies the problems of cross-border eDiscovery affecting multinational business enterprises with significant operations in the U.S.

The “Catch-22” of U.S. eDiscovery

- ▶ There is no predictable framework or set of rules to assist multinational business enterprises in addressing the “Catch-22” of eDiscovery – i.e., what to do when compliance with U.S. discovery rules and court orders requires violating blocking statutes and data privacy laws.
- ▶ Steps in the analysis:
 - Understanding U.S. Discovery Obligations
 - Identifying Possible Conflicting Laws
 - Obtaining Guidance from Court Decisions
- ▶ Certain pro-active measures can limit risk and liability.

Section II: U.S. eDiscovery

CASE IN POINT

by Tom Fishburne

E-DISCOVERY TOWN HALL MEETING

IN CONCLUSION, INCREASING ESI VOLUMES ARE DRIVING UP COST AND RISK AND THE SOLUTION IS THE APPROPRIATE USE OF TECHNOLOGY



© 2009

CASECENTRAL.COM/CASEINPOINT

Overview of U.S. eDiscovery

- ▶ Scope of Discovery: discovery is generally permitted for nonprivileged information if the information sought is “reasonably calculated to lead to the discovery of admissible evidence.” Rule 26(b)(1) of the Federal Rules of Civil Procedure.
- ▶ In federal cases, Rule 26(f) requires an early conference, in part, for the parties to confer on a discovery plan, including “any issues about disclosure or discovery of electronically stored information....”
- ▶ eDiscovery includes identifying, collecting, processing, reviewing, and potentially producing electronically stored information (“ESI”).
- ▶ 2007 revenues for eDiscovery services were almost \$2.8 billion (Socha-Gelbmann 2008 Survey), and Forrester Research expects eDiscovery technology spending to reach \$4.8 billion by 2011.

Overview of U.S. eDiscovery

- ▶ Why is eDiscovery such big business?
 - ESI is voluminous and easily replicable.
 - ESI is difficult to remove, i.e., deletion ≠ destruction.
 - ESI is dynamic. It can be altered in a number of ways, and sometimes even without intent.
 - ESI's metadata contains valuable information.
 - ESI is system-dependent.
 - ESI is portable and mobile.
- ▶ U.S. discovery rules permit broader discovery than most other jurisdictions, and this compounds the effect of ESI.
- ▶ In August 2008, the Radicati Group estimated approximately 55 Billion non-virus or spam emails are sent each day.
- ▶ eDiscovery bridges law and technology and requires a close collaboration between legal counsel and IT professionals.

International Impact of U.S. eDiscovery

- ▶ The obligation to produce extends to ESI within a litigant’s “possession, custody, or control.” Rule 34(a)(1) of the Federal Rules of Civil Procedure.
- ▶ As long as the litigant has a legal right to obtain the information sought on demand, it is deemed to have possession, custody, or control, even if the information is beyond the jurisdiction of the court. *See Buckley v. Vidal*, 50 F.R.D. 271, 274 (S.D.N.Y. 1970).
- ▶ To determine whether a U.S. subsidiary, parent, or affiliate is deemed to “control” information held by a foreign parent, subsidiary, or affiliate, some courts have used a series of factors. *See Stella v. LVMH Perfumes & Cosmetics USA, Inc.*, 2009 U.S. Dist. LEXIS 22948 (Nd. Ill., March 23, 2009). These factors include the following:
 - Adequate ownership share in the subsidiary by the parent.
 - Interlocking management structures.
 - Sufficient control held by the parent over the subsidiary’s directors, officers, and employees.
 - A connection to the transaction at issue.

International Impact of U.S. eDiscovery

- ▶ Other courts have found control on alternative grounds. *See Pitney Bowes, Inc. v. Kern Int'l., Inc.*, 239 F.R.D. 62 (D. Conn. 2006). They include:
 - If the “alter ego” doctrine warrants “piercing the corporate veil.”
 - Whether the subsidiary was an agent of the parent in the transaction related to the litigation.
 - Whether the subsidiary can secure the information sought to meet its own business needs.
 - Whether the subsidiary has access in the ordinary course of business.
 - Whether the subsidiary was a marketer or servicer of the parent’s products.
- ▶ It is not difficult, then, for U.S. courts to subject the documents and ESI of non-U.S. parents, subsidiaries, and affiliates to U.S. discovery rules.

Section III: The Sources of Conflict



Sources of Conflict – Privacy / Data Protection

- ▶ In many non-U.S. jurisdictions, privacy is deemed to be a fundamental right, while in the U.S., privacy rights are subject-matter specific, e.g., HIPAA protects medical information.
 - Enumerated in Article 8 of the European Convention of Human Rights of 1950.
 - Article 1 of the 1995 European Union’s Data Protection Directive protects the “right of privacy with respect to the processing of personal data.”
 - In implementing Article 1, EU Members are permitted to enact statutes with even greater protection (and many have done so).
 - The 1995 Directive restricts prevention of the free flow of data amongst Member States.
 - To process or transfer data, the controller of the data must generally demonstrate necessity or obtain consent. *See* Articles 7 and 26 of the 1995 EU Data Protection Directive.

Sources of Conflict – Privacy / Data Protection

- ▶ Generally, legal requirements from non-EEA (European Economic Area) judicial forums do not meet the necessity exception.
- ▶ Some key definitions:
 - Personal Data = any information relating to an identified or identifiable natural person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity.
 - Processing = any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as 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.
- ▶ *eDiscovery processing work for the purpose of U.S. litigation violates these provisions as soon as any amount of “processing” occurs, even before actual transfer of the data to the U.S.*

Sources of Conflict – Blocking Statutes

- ▶ Blocking statutes are attempts to restrict the transfer of information abroad for the purposes of disclosure.
- ▶ Enacted by most civil law jurisdictions and certain common law jurisdictions (e.g., Canada, Australia).
- ▶ Swiss banking secrecy laws function as a type of blocking statute for certain categories of information. Other states have similar subject matter dependent secrecy laws.
- ▶ The attorney in *In re Advocat Christopher X* was convicted and fined under a French blocking statute.

Section IV: The Judicial Response



Judicial Response to the Sources of Conflict

- ▶ Several recent court decisions illustrate that judges place little weight on foreign restrictions regarding the disclosure of information and generally do not favor arguments based on notions of national sovereignty.
- ▶ *Richmark Corp. v. Timber Falling Consultants*, 959 F.2d 1468 (9th Cir. 1992): PRC's state secrecy law did not excuse compliance with discovery order, even where the PRC law could impose criminal penalties for compliance with U.S. discovery order.
- ▶ *Heidberg v. Grosvenor*, [1993] Q.B. 324, 325 (U.K.): without evidence that any prosecutions under the French blocking statute had ever occurred, it was unreasonable for the litigant to fear prosecution.
- ▶ *Straus v. Credit Lyonnais*, 242 F.R.D. 199 (E.D.N.Y., May 25, 2007): court ordered disclosure, in part, due to a finding of a low likelihood of actual prosecution under the applicable blocking statute.
- ▶ *Enron v. J.P. Morgan Secur. Inc.*, No. 01-16034 (Bankr. S. D. N.Y. July 18, 2007): the French blocking statute did not excuse a party's discovery obligations.

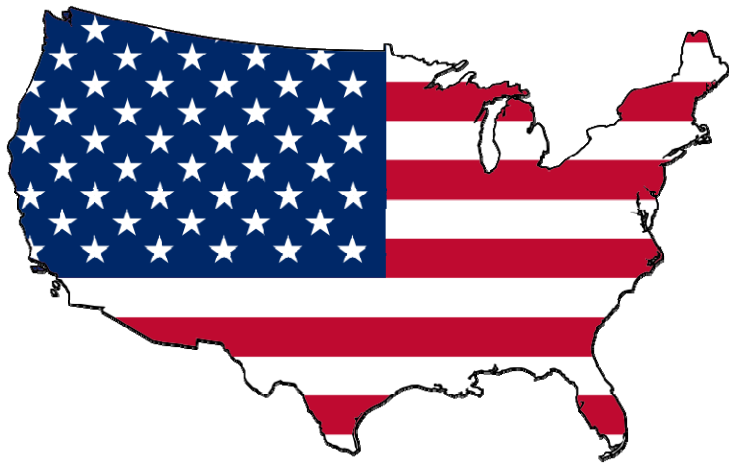
Judicial Response to the Sources of Conflict

- ▶ *Columbia Pictures Indus v. Bunnell*, 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. May 29, 2007): production of server log data located in the Netherlands was ordered even though production would violate Netherlands Personal Data Protection Act.
- ▶ *Reino de Espana v. Am. Bureau of Shipping*, 2007 U.S. Dist. LEXIS 41498 (S.D.N.Y. June 1, 2007): monetary sanctions awarded against Spanish government (plaintiff) for failure to place a litigation hold, and Spanish privacy laws were no excuse.
- ▶ *Linde v. Arab Bank, PLC*, 2009 U.S. Dist. LEXIS 51569 (E.D.N.Y. June 18, 2009): adverse inference instruction ordered due to failure to respond to certain discovery based on foreign bank secrecy laws.
- ▶ *Lynondell-Citgo Refining, LP v. Petroleos de Venezuela, SA*, 2005 WL 1026461 (S.D.N.Y. 2005): adverse instruction ordered due to failure to produce corporate minutes in criminal violation of Venezuelan law.

Will *Christopher X* Alter U.S. Judicial Approach?

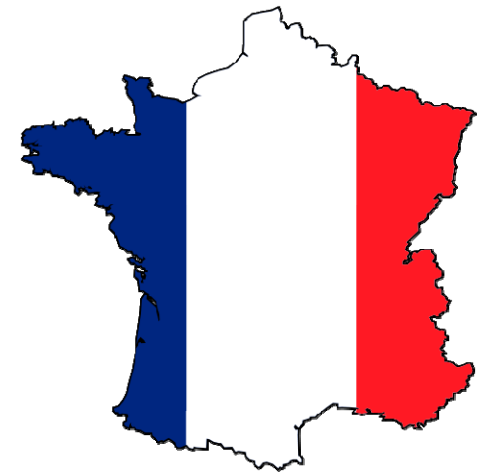
- ▶ The Sedona Conference and numerous commentators suggest that, at the very least, it provides support for an argument that prosecution is now a viable threat.
- ▶ But Magistrate Judge Matsumoto specifically reconsidered the issue in light of *Christopher X*.
 - *Strauss v. Credit Lyonnais, S.A.*, 249 F.R.D. 429 (E.D.N.Y. 2008): Judge Matsumoto considered defendants' motions for protective orders based, in part, on the *Christopher X* decision.
 - Judge Matsumoto distinguished *Christopher X* because: 1) the attorney in that case was not conducting discovery under the Federal Rules; 2) the French court found that the attorney made false statements; and 3) the prosecution was initiated by a complaint from MAAF, which was not likely to happen against Credit Lyonnais.

So Who Wins?



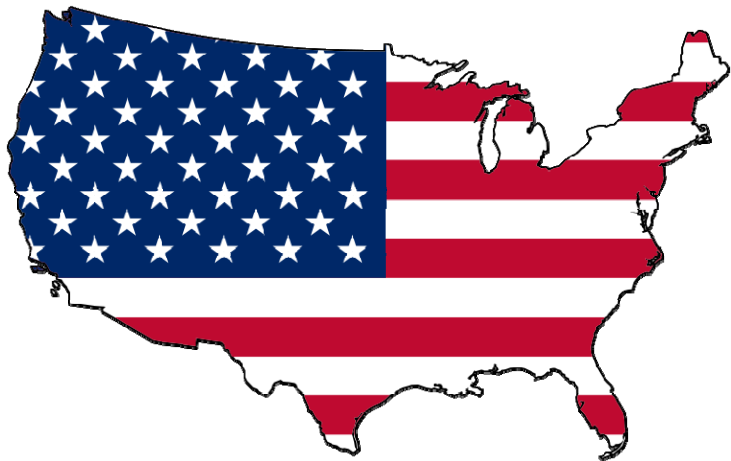
Freedom Fries

v.



French Fries

Still Seems to Be the U.S. Discovery Rules



Freedom Fries

Section V: Suggestions for Multinational Businesses

CASE IN POINT

by Tom Fishburne



© 2009

CASECENTRAL.COM / CASEINPOINT

What Now for Multinational Businesses?

- ▶ Key areas of analysis:
 - Legal –
 - Analyze potential sources of liability.
 - Minimize impact of conflict between discovery and privacy.
 - Understand jurisdiction specific rules for all business units.
 - Structural –
 - Map IT infrastructure and data sources.
 - Determine and remedy problem areas from IT and data map.
 - Ensure close cooperation between legal and IT departments.
 - Practical –
 - Do not assume.
 - Do not procrastinate.
 - Focus on reasonableness.

Best Practices - Legal

- ▶ Analyze potential sources of liability:
 - Different businesses are susceptible to different types of litigation with different levels of discovery.
 - Avoid the “Black Swan” problem – past experience should not be overvalued when assessing sources of liability.
- ▶ Minimize impact of the conflict between discovery and privacy:
 - When practical, obtain consent for data processing and production.
 - U.S. entities and business units should become Safe Harbor Self-Certified.
 - If Safe Harbor is not available, use Model Contractual Clauses as authorized by Article 26(2) of the EU’s Data Privacy Directive.
 - Adopt Binding Corporate Rules to ensure adequacy of data protection, and obtain approval from all relevant data protection authorities.

Best Practices - Legal

- ▶ Understand jurisdiction-specific rules for all business units:
 - Identify the relevant jurisdictions (involves collaboration with IT).
 - Seek opinions from subject matter experts.

Best Practices – Structural

- ▶ Map IT infrastructure and data sources:
 - The human element –
 - Who are the key IT managers for different business units? Is IT management outsourced in whole or in part?
 - How do the business's employees create and use data?
 - What languages are used?
 - The data –
 - What applications are used and for what purposes?
 - What are the formats for structured and unstructured data?
 - How easily can the structured and unstructured data be searched, accounting for format, language, and other factors?
 - The policies –
 - What are the data retention, storage, and backup policies in place?
 - How will data be stored and backed up across the different business units?

Best Practices – Structural

- ▶ Determine and remedy problem areas:
 - Jurisdictional issues –
 - Do the data retention, storage, and backup policies comply with the laws of all applicable jurisdictions?
 - Can the policies be restructured to reduce compliance costs and potential liability?
 - Susceptibility to conflicting laws –
 - Do the data retention, storage, and backup policies trigger conflicting laws from different jurisdictions?
 - Are there feasible options to reduce this susceptibility?
 - The unknown –
 - Are there ways for custodians to create data outside of the policies and otherwise unbeknownst to IT or legal, whether inadvertently or intentionally?
 - Are there effective ways to prevent the creation of unauthorized data?

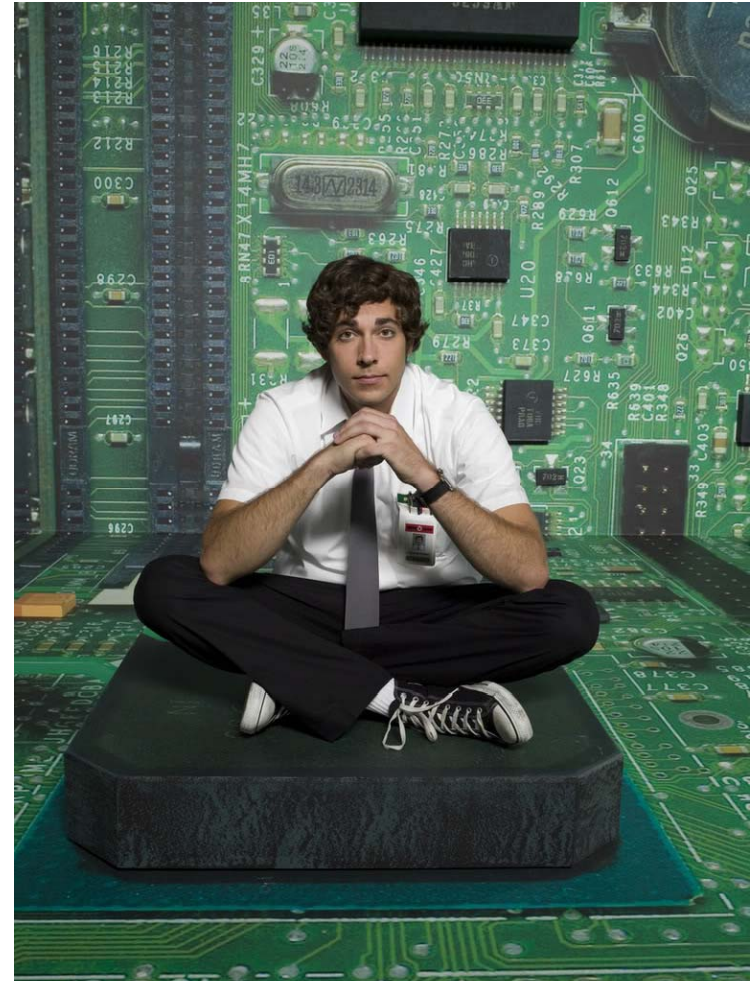
Best Practices – Structural



Should the legal team try to manage eDiscovery alone?

Best Practices – Structural

Or should others be consulted?



Best Practices – Structural

- ▶ Ensure close cooperation between legal and IT:
 - NOTE – for many multinational businesses, IT plays a greater role in ensuring the success of the business than the legal department.
 - Avoid being the unduly meddlesome lawyer who fails to understand and incorporate the needs of the business and of IT into the eDiscovery and legal analysis.
 - Ideally, decisions affecting a business’s eDiscovery liability should be made by a committee including members of the legal department and the IT department.
 - Communication and cooperation extend beyond the business –
 - Outside counsel will make decisions and act on a business’s behalf and must do so based on information obtained from the IT department.
 - Failure to monitor the level of information sharing between outside counsel and IT can result in outside counsel unwittingly committing the organization to costly eDiscovery and to violation of data privacy laws and blocking statutes.

Practical Considerations

- ▶ Do not assume:
 - That outside counsel has already taken into account the implications of cross-border eDiscovery for your organization. This is a new and developing field and many of the very best attorneys are still unfamiliar with the relevant issues.
 - That your eDiscovery vendors have taken into account the implications of cross-border eDiscovery. As processors of data, they are independent businesses that must determine a method to avoid creating liability under data protection and blocking statutes.
 - That particular data only exists in one place. Data is highly portable, and thus, people within an organization can easily trigger the need for cross-border compliance even if IT policies have been designed to minimize this risk.
 - That just because your organization has not faced eDiscovery compliance problems or has not been sanctioned for failure to comply that it will not happen. Sanctions were awarded in 36% of U.S. eDiscovery opinions in 2009.

Practical Considerations

- ▶ Do not procrastinate:
 - Proactive measures limit both cost and risk. Reactive measures can be ineffective and quite costly.
 - Under the Federal Rules, the initial Rule 26(f) conference involves discussion of ESI issues. An analysis of ESI, especially when multiple jurisdictions are involved, will not likely be thorough or complete by the time of the Rule 26(f) conference if the organization waits until a lawsuit is filed.
 - Understanding the ESI issues for a particular litigation, the costs associated, and the cross-border difficulties can be used offensively in requests to opposing parties and to force early settlement.
 - Managing ESI is especially susceptible to the “planning fallacy” – the tendency to underestimate the time necessary for completion.
 - The obstacles that might arise are generally unknown.
 - The amount of time a court case can take to reach a resolution can give the false sense of having enough time.

Practical Considerations

- ▶ Focus on reasonableness:
 - While judicial opinions seem to disfavor arguments premised on foreign national sovereignty and state interests, courts tend to view arguments based on “reasonableness” more favorably.
 - After all, Rule 1 of the Federal Rules of Civil Procedure states that the rules “should be construed and administered to secure the just, speedy, and inexpensive determination of every action and proceeding.”
 - Multinational business enterprises can more effectively petition a court for relaxed production obligations based on Rule 1 and the “reasonableness” jurisprudence when they know their IT structures, the conflicting data privacy and blocking statutes, and their approximate cost exposure to handling ESI.



APHELION
LEGAL SOLUTIONS

*Leveraging Global Legal Talent*SM

Hiren P. Patel, CEO

+1-713-579-9751 (Office)

+1-619-206-8466 (Mobile)

hpatel@aphelionlegal.com