

eDiscovery Update



November 2007

The Amendments to the Federal Rules of Civil Procedure Concerning E-Discovery Impact on Global Business Enterprises

In December 2006, the Federal Rules of Civil Procedure were modified (“Amended Federal Rules”).

Adding several provisions addressing discovery and production requirements for electronically stored information (“ESI”) that directly impacted global companies. The Amended Federal Rules became necessary to assist U.S. litigants and the judiciary in setting parameters around the discovery of ESI, primarily information transmitted via E-mail. In this era of globalization, this article provides a much needed summary of the obligations U.S. companies face associated with retaining and producing ESI that is stored overseas. This article also provides recommended steps global companies can take to begin mitigating the risks associated with ESI.

Part one illustrates how global business enterprises are struggling with managing ESI. Part two addresses the legal requirements for retaining and producing ESI in U.S. litigation. Part three discusses the business implications of U.S. discovery for global enterprises. Part four discusses the impact of various foreign laws, specifically those in the EU, on the production of ESI in U.S. litigation. Part five offers solutions for companies struggling with seemingly conflicting obligations.

Global Companies Struggle With ESI Retention

E-mail usage proliferated in the late 1990s and, by 2002, it was estimated that businesses in North America had

sent over 3.25 trillion E-mails. As technology advanced, that number has grown exponentially. Indeed, in 2007 alone, business E-mails sent worldwide will reach almost 5 exabytes, doubling the amount sent in 2005-06. This phenomenon resulted in companies struggling to retain E-mails in accordance with applicable retention and litigation-related obligations.

Given the proliferation of, and complexity surrounding, E-mail retention, a large number of companies initially took the position that E-mails did not constitute business records due to the electronic medium in which they were transmitted. As a result, they claimed that they did not need to preserve E-mails, regardless of the content of those E-mails. The Amended Federal Rules no longer allow companies operating in the U.S. to assert such a position.

Several companies are still learning this lesson and have suffered as a result of their failure to retain electronic Business Records. The following examples illustrate this point:

- Due to its intentional spoliation of ESI, Oved Construction Services was sanctioned, had a default judgment entered against it, and had to pay its adversary’s attorneys’ fees.
- A Federal Court in New York found Strategic Resources was grossly negligent because it failed to timely produce 25 gigabytes of data, even though no evidence was destroyed.
- Echostar’s practice of routinely disposing of E-mails, regardless of content, was deemed “risky and extraordinary,” and Echostar was sanctioned for failing to preserve E-mails relevant to a former employee’s EEOC claim.

Summary of Legal Requirements for Retaining and Producing ESI

The Amended Federal Rules addressed five principal areas of electronic discovery. They are:

- The defined term ESI replaced the phrase “electronic compilations of data” (Amended Rule 16(b); 26(a)(1)(B));
- A party must identify to the requesting party a description of where potentially relevant evidence exists, including electronic records and electronic repositories (Amended Rule 26(a)(1));
- Parties must meet and confer regarding the production of ESI early in the pretrial phase of the litigation (Amended Rule 26(f));
- A party need only search and produce records from “reasonably accessible” sources (Amended Rule 26(b)(2)); and
- A party that has disposed of ESI in good faith and in accordance with established records retention practices may avoid sanctions under a limited safe harbor provision (Amended Rule 37).

A few points are worth noting about each change. First, whether ESI is “reasonably accessible” will be decided on a case-by-case basis. Courts will not accept blanket assertions that ESI is too costly or burdensome to locate and/or produce. Instead, companies asserting this position must prove the cost of producing the requested ESI is excessive, and they will bear the burden of establishing that such repositories are not utilized for business, legal, or compliance purposes. The Advisory Committee Notes provide that identifying ESI “as not reasonably accessible does not relieve the party of its common law or statutory duties to preserve evidence.” Additionally, a party is not relieved of its duty to produce ESI merely because it chose to preserve the evidence in a format that makes the ultimate production expensive.

Second, the term ESI is intended to broaden the scope of discoverable information. ESI is discoverable as are traditional hard-copy business records. ESI may include word-processed documents, spreadsheets, E-mail, text files, PowerPoint presentations, digital photos and other data created with a computer, or maintained in an electronic storage medium. This list is not exhaustive and the Amended Federal Rules provide a flexible definition of the term ESI to accommodate technology advances. Thus, litigants should operate under the presumption that they should, at a minimum, retain E-mails similar to other hard-copy records. The scope of ESI, and the burdens associated with its production, will depend upon technology, a court’s understanding of it and the need for the information given its potential impact on a case.

Third, pursuant to Amended Rule 26(a)(1), parties must provide to the requesting party a description of where potentially relevant evidence exists, including evidence stored in electronic repositories. This disclosure relates to information that the disclosing party intends to use to support its claims or defenses. Therefore, eDiscovery preparedness is essential to allow a company to gain an understanding of its technology environment, including the identification of repositories of potentially discoverable ESI, including those stored in other countries.

Fourth, parties must perform a reasonable inquiry as to the location of potentially relevant ESI. The mere issuance of a “litigation hold,” without more, will not suffice to satisfy the “reasonable inquiry” requirement of Amended Rule 26(g)(2). Indeed, litigants have an on-going responsibility to take appropriate measures to ensure that they have preserved and produced all available ESI responsive to discovery requests.

Fifth, recognizing the risks in producing servers or vast volumes of ESI, the Amended Federal Rules offer parties the limited opportunity to recover, or “clawback,” privileged communications that were inadvertently produced. Courts will consider five factors when determining whether a clawback is appropriate:

- the precautions taken to prevent the disclosure;
- how long did the litigant wait to rectify the disclosure?;
- the scope and size of the production;
- the extent of the disclosure, and to what extent have those records been used in the case; and
- are there overriding issues of fairness, such as revealing the truth, that weigh against the clawback?

Finally, the safe harbor in Amended Rule 37 provides that, absent exceptional circumstances, a court may not impose sanctions under the rules on a party for failing to provide ESI lost “as a result of the routine, good-faith operation of an electronic information system.” The Amended Federal Rules do not define “good faith” or “routine,” but litigants should not expect broad protection in this provision, given the generally accepted requirement for document preservation once litigation is imminent. Additionally, a company likely will not receive the benefit of the doubt if its records are disposed of without showing that it followed a valid records retention policy.

Implications for Global Enterprises

Can U.S. companies store or transmit ESI overseas and then claim in U.S. litigation that the materials are inaccessible, too costly or burdensome to retrieve, or that those records are not in the company’s control? As illustrated below, probably not, because maintaining records overseas does not necessarily put the records out of the reach of U.S. litigants.

Courts will focus on whether the ESI are accessible by a business operating in the U.S., regardless of whether that data is stored in London, Tokyo, or Sydney. A U.S. parent company is considered to control data generated by its foreign subsidiaries notwithstanding the physical location of the data. A company cannot avoid producing potentially relevant evidence in a U.S. litigation matter where the U.S. company can acquire

the ESI by requesting or causing the records to be sent to it by the foreign parent. Accordingly, the critical factor is the degree of control and access that the U.S. company is able to exercise over the ESI.

Foreign parent corporations (especially those governed by the laws of the EU) will often contend that producing ESI could run afoul of privacy regulations. However, U.S. courts will look at the extent to which that foreign parent and its subsidiary avails themselves to U.S. laws as well as the need for the parties to access the data stored overseas. Where the foreign company has enjoyed the benefit of conducting business in the U.S., and the ESI is important to the litigation, U.S. court may likely reject the argument that producing ESI stored overseas would violate EU privacy laws. Further, companies storing data of their U.S. subsidiaries overseas must also be mindful that if a U.S. company seemingly transferred or purposefully stored its records overseas for the sole purpose of keeping them out of the reach of U.S. litigants, the Court may sanction or otherwise punish the company refusing to produce the requested records.

Records Retention Concerns in the EU

Perhaps the biggest document retention and eDiscovery challenge that U.S. companies operating overseas face is the fundamental difference between how the U.S. government and U.S. companies view employee generated information and how other countries view that same information. In the EU, employee generated personal information is considered private. So if an employee in an EU nation creates and sends a personal E-mail to a friend and saves it to the company’s server, that E-mail is considered private. Furthermore, if that same E-mail contained both business related information and personal information, at least the personal part of the E-mail would be considered private.

Although the EU’s privacy laws are not uniform, the EU’s 1995 Data Protection Directive prohibits the transfer of personal data to non-EU nations that do not meet “adequacy” standards for privacy protection.

These laws may go so far as to affect where the data may be processed in addition to where it may be transferred.

In contrast, U.S. privacy laws do not provide the same protection for “private information” and, therefore, as a general rule, personal data cannot be transferred to the U.S. from the EU without first devising a system addressing privacy considerations. This includes data transmitted to a U.S. office. In light of these risks, U.S. companies should consider implementing privacy principles in accordance with the “Safe Harbor Principles” (not to be confused with the Amended Federal Rules safe harbor provision) developed by the U.S. Department of Commerce and the European Commission. U.S. Companies do not have to implement the Safe Harbor Principles, but if they attempt to, they must comply with the provisions or risks action by the Federal Trade Commission for non-compliance.

Best Practices for Retaining and Producing ESI in U.S. Litigation

Companies should develop and implement an enterprise-wide records retention program that, at a minimum, meets the legal requirements articulated above. Implementing such policies may allow a company to enjoy the beneficial safe harbor aspects of the Amended Federal Rules and possibly the Safe Harbor Provisions of the Department of Commerce and the EU.

Companies should retain and manage E-mails constituting Business Records, or Record E-mails, in accordance with applicable retention obligations. To ease the burden on their servers and eDiscovery response efforts downstream, these companies should also dispose of Transitory E-mails in a systematic and routine manner. Perhaps the best way to accomplish these tasks is to employ an archiving solution that can store Record E-mails for the periods dictated by law and dispose of stale or Transitory E-mails in a systematic and transparent manner.

Implementing such a policy may allow your company to:

- Demonstrate its compliance with applicable retention obligations and minimize the risks associated with premature disposition of Business Records;
- Reduce the volume of data it would need to manage and subsequently review when retrieving E-mails for litigation purposes;
- Document the disposition of Record E-mails that occurs after the expiration of an applicable retention period; and
- Account for ESI used by business units operating in the U.S., thus minimizing the chance that your company will run afoul of foreign privacy laws.

Global companies should also consider taking the following steps to minimize the risks associated with ESI:

- Develop a litigation response team, comprised of outside counsel, corporate counsel, HR personnel, business line managers and IT staff, ready to respond to an intrusive discovery request;
- Develop a litigation hold policy that is clearly articulated to its employees and that is ready for implementation upon notice of a suit;
- Records retention policies should be inventoried, monitored, and audited, and electronic information systems should be evaluated to ensure they are operating in compliance with those policies. Further, efficient application of a litigation hold protocol requires a map of information likely to be subject to litigation. While it may not be necessary to map all potentially relevant information in advance of litigation, a company should begin this process for the information most likely needed for future

ongoing and predictable litigation or high risk records.

A data map of information stored on company repositories should identify where classes of information are created, distributed and stored. This basic understanding is necessary to provide the security, authenticity, and traceability required in litigation. The information included in this effort generally includes a review of the following:

1. Origination of Record Classification

- a. Purpose of the record classification
- b. Method of creation
- c. Original form(s)
- d. Category/Individuals creating records
- e. Location of business units or individuals creating records

2. Distribution

- a. Who received or used the records within that classification
- b. How is this information distributed to recipients
- c. Is this information likely to be distributed beyond intended recipients?
- d. Information systems involved in distribution

3. Storage/Destruction

- a. Where is the information stored (physical and/or electronic)
- b. Backup and Disaster Recover Systems
- c. Method of Destruction

Conclusion

To comply with the Amended Federal Rules, global companies with U.S. operations must have a plan to locate, preserve and produce ESI in the event that litigation is reasonably anticipated or has commenced. Counsel must become familiar with the scope of the company's ESI as well as how it is stored and the

costs to retrieve and produce the ESI. In addition, if the company is multi-national, U.S. counsel must coordinate with its overseas affiliates to ensure that preservation and production of Business Records does not run afoul of privacy laws.

Records Management, Electronic Communications and eDiscovery Group

Given today's legal and technological environment, many companies have reassessed their records management programs to ensure that they meet the company's operational needs as well as complying with applicable legal requirements. Companies also are examining whether their: (1) employees routinely follow existing retention schedules, (2) stale records are properly and lawfully disposed of; and (3) records are being prematurely discarded.

Vedder Price's attorneys have developed unparalleled experience in and knowledge of the laws applicable to records retention, whether in hard copy or electronic form. Its records management team is composed of attorneys dedicated to enabling its clients to develop customized, yet comprehensive, solutions to: (a) minimize litigation risks and costs; (b) increase records management efficiency; and (c) achieve compliance with all applicable governmental regulations and statutes as well as industry best practices.

The firm counsels companies with regard to all aspects of their records management and eDiscovery needs, including:

- Developing and implementing clear records retention policies designed to meet today's legal and business challenges;
- Assisting in the design and implementation of electronic communications policies covering e-mail, instant messages, voice mail and any other electronic messages sent to or received by company-owned BlackBerrys®, personal digital assistants and other similar electronic communications devices;

- Auditing existing records management programs, including identifying potential compliance gaps, and providing practical and proven recommendations for enhancing current policies and procedures;
- Designing comprehensive training programs on records management and compliance issues; and
- Conducting prelitigation assessment of eDiscovery issues and records management and developing comprehensive strategies for aggressively conducting and responding to eDiscovery.

Vedder Price has been at the leading edge in this rapidly evolving field by taking a proactive approach on records management and eDiscovery issues. Its vast experience includes designing and implementing enterprise-wide records retention and electronic communications policies for a Fortune 20 client, as well as counseling a large mutual fund complex and national health care association on various aspects of their records management programs.

VEDDER, PRICE, KAUFMAN & KAMMHOLZ, P.C.

This bulletin is published by the law firm of Vedder, Price, Kaufman & Kammholz, P.C. It is intended to keep our clients and interested parties informed on recent legal developments. It is not a substitute for professional advice.

Vedder Price is a national full-service law firm with over 250 attorneys in Chicago, New York, Washington, D.C. and New Jersey. Please contact your Vedder Price attorney with any questions or if you need any assistance.

Copyright © 2007 Vedder, Price, Kaufman & Kammholz, P.C. Reproduction of this bulletin is permitted only with credit to Vedder, Price, Kaufman & Kammholz, P.C. For purposes of the New York State Bar Rules, this newsletter may be considered ATTORNEY ADVERTISING. For an electronic copy of this bulletin, please contact us at info@vedderprice.com.

Chicago

222 North LaSalle Street
Chicago, Illinois 60601
312-609-7500
Fax: 312-609-5005

New York

1633 Broadway, 47th Floor
New York, New York 10019
212-407-7700
Fax: 212-407-7799

Washington, D.C.

875 15th Street, N.W., Suite 725
Washington, D.C. 20005
202-312-3320
Fax: 202-312-3322

New Jersey

Five Becker Farm Road
Roseland, New Jersey 07068
973-597-1100
Fax: 973-597-9607