VORYS
EMPLOYMENT LAW BULLETIN

August 2007
Volume 4, Issue 2

Court Issues New Default Standard For E-Discovery

In connection with the recent revisions to the Federal Rules of Civil Procedure relating to discovery of electronically stored information ("ESI"), on June 6, 2007, the United States District Court for the Northern District of Ohio issued a new default standard for electronic discovery. This new order places very specific duties upon the parties with regard to E-discovery. The parties in a case are always free to agree upon a different process, but until and unless such agreement is reached, the parties will be obligated to follow this new default standard. While this new default standard presently only applies to cases filed in the Northern District of Ohio, other courts may already have or may soon impose similar standards.

In This Issue:

Disclosures of ESI systems and custodians -- The new standard requires that, at the outset of each case, each party must provide to the opposing party a list of the most likely custodians of relevant ESI and a description each relevant electronic system.

ESI Retention -- The new standard also requires that within the first 30 days of discovery, the parties are to work toward an agreement outlining the steps each party will take to segregate and preserve the integrity of all relevant ESI. The Order requires that each party identify a retention coordinator who, within 7 days of identifying the relevant document custodians, will be responsible for taking steps to ensure that relevant e-mail and other ESI is not destroyed or altered. Counsel will then be required certify to the court that these steps have been taken.

The E-Discovery Coordinator -- The new standard further requires that each party designate an E-discovery coordinator, who may be an employee of the party, a third-party consultant, or in-house or outside counsel and who must be:

- Sufficiently familiar with the party's electronic systems to explain and answer questions regarding these systems.
- Knowledgeable about the technical aspects of E-discovery, including document storage, organization, and format issues.
- Prepared to participate in E-discovery dispute resolutions.

The complete text of the new standard can be found at http://www.ohnd.uscourts.gov/Clerk_s_Office/Local_Rules/AppendixK.pdf.

In light of the new Federal Rules, employers, both within and outside of the Northern District of Ohio, should consider taking steps now to prepare summaries of likely relevant electronic systems, to ensure that effective procedures are in place to activate "litigation hold" procedures to prevent improper destruction of relevant ESI, and to develop persons capable of serving as the E-discovery coordinator in future litigation. If you wish to discuss any of these issues further, please contact your Vorys attorney.

By: Douglas R. Matthews • Phone: 614.464.5460 • E-mail: drmatthews@vssp.com

Monitoring Workplace E-mails in European Union

In the Unites States, private businesses monitor employees' use of e-mail for a variety of purposes including ensuring worker productivity, preventing disclosure of confidential or sensitive information and preventing viruses or malicious code. Because companies generally own the equipment, software and systems used by employees in the workplace and have policies prohibiting personal use of its business systems, courts have generally concluded that employees have no expectation of privacy in their communications at work. As a result, monitoring usually can be implemented without much restriction.

But what if your company has operations in Europe?

Unlike the United States, individuals in European Union (EU) countries have an expectation of privacy even while at the workplace and using company owned equipment. This expectation of privacy has roots in the complex EU privacy law landscape, which includes general rights of privacy granted to individuals under national constitutions, specific legislation or case law as well as specific data protection and privacy legislation, such as the EU's Data Protection Directive.

Additionally, some EU countries have adopted codes of conduct, workplace privacy principles or other guidance intended to address the obligations or best practices regarding disclosure and use of workers' personal information and their workplace privacy, which, depending on the country, might be used to determine privacy violations by courts or enforcement agencies.

Despite the myriad of authorities in the EU and varying interpretations of law and enforcement by individual countries, the first step in analyzing any proposed e-mail monitoring is answering the following questions:

- Is there a legitimate business purpose for the monitoring?
- Does the planned monitoring or retrieval go no further than is necessary to meet the legitimate business purpose for monitoring?
- Have you selected the least intrusive method to accomplish such monitoring?

If you can answer "Yes" to the foregoing questions, there are still other areas to consider based on the location of your employees:

- **Determine the role of unions, work councils or similar organizations in the countries you operate.** For example, in Italy, employers cannot monitor e-mail content or Internet usage unless the employer has reached an agreement with the local union or has authorization from the local labor office.
- **Determine the country's view on private or personal e-mails**. For example, a recent French case ruled that an employer may monitor and note that an employee is using a computer system for personal reasons (and may take disciplinary action for such use); however, an employer cannot review the contents of a personal e-mail.
- **Have you adequately disclosed the type and extent of monitoring to your employees**. For example, the United Kingdom Information Commission has advised employers to give employees notice of permitted uses of company e-mail, the type and extent of any monitoring and the penalties for breaching company policy.

Because interpretations of law, enforcement and penalties vary greatly across EU countries, it is critical to have legal counsel examine the particularities and sometimes peculiarities of a specific country before monitoring employee e-mails.

Monitoring and retrieving e-mails can be an important and legitimate tool for protecting and growing your business. By understanding and considering the unique privacy law framework in the EU and taking the proper steps, it can continue to be an important part of your business in the EU.

By: Benjamin J. Rickert • Phone: 614.464.6236 • E-mail: bjrickert@vssp.com