

Ungaretti & Harris LLP
E-Discovery Update

Legal Update:

Stengart v. Loving Care Agency, Inc., et al.

Supreme Court of New Jersey (March 30, 2010)

By Susan G. Feibus

Stengart v. Loving Care Agency, Inc., et al., is a case that, at a minimum, should motivate employers to review their electronic communications policies. The Supreme Court of New Jersey held that an employee had a reasonable expectation of privacy when she communicated with her lawyers through a personal, password protected e-mail account – even though she used a company laptop. As a result, the e-mails between the employee and her lawyers were protected by the attorney-client privilege and were not discoverable in litigation.

The issue of whether the e-mails were privileged arose after the employee filed an employment discrimination lawsuit against her former employer. The employer retained a forensic specialist to recover all files stored on the employee's laptop, including the e-mails, which automatically had been saved on the hard drive. In discovery, the company's lawyers disclosed that the e-mails had been retrieved but refused to return them. The employee sought relief in court. The trial court ruled that, in light of the company's written policy on electronic communications, the employee waived the attorney-client privilege by sending e-mails on a company computer. The appellate court reversed and, in a potentially far reaching decision, the Supreme Court affirmed the appellate court.

In finding the e-mails privileged, the *Stengart* court found that the employer's electronic communication policy did not provide the employee adequate notice that the company would save on a hard

drive, or monitor the contents of, e-mails sent from a personal account. More significantly, the *Stengart* court suggested that the e-mails would be privileged even if the company's policy had been clearer:

Because of the important public policy concerns underlying the attorney-client privilege, even a more clearly written company manual – that is, a policy that banned all personal computer use and provided unambiguous notice that an employer could retrieve and read an employee's attorney-client communications, if accessed on a personal, password protected e-mail account using the company's computer system – would not be enforceable.

Moreover, the *Stengart* court concluded that the refusal of the employer's lawyers to return the e-mails to the employee was a breach of New Jersey's Code of Professional Conduct, for which the lawyers were subject to sanctions.

While courts in other jurisdictions, including Illinois, have given employers' electronic communications policies more deference than did the Supreme Court of New Jersey in *Stengart*, this decision highlights important lessons for employers:

- Employers periodically should review their written electronic communications policies to make sure that the language is clear and that the policy is consistent with the evolving law. Generalized statements about an employer's right to monitor electronic communications may be insufficient to extinguish an employee's privacy rights. The same is true of an employer's attempt to prohibit or limit personal use of the employer's computer, which a court may find untenable in this electronic age or create ambiguity regarding what use is permissible. Employers should adopt policies that specifically inform employees that even personal, password protected e-mail accounts can be and are monitored and such e-mails may be stored on the company's hard drive.
- Employers should obtain from each employee a written acknowledgement of receipt of the company's electronic communication policy. The acknowledgment also should state that the employee has read and understands the policy.
- Employers should recognize that even if these practices are followed, not all employee information stored on company computers may be discoverable. Whether an employee had a reasonable expectation of privacy in e-mail sent or received on a company computer likely will be subject to a case-by-case analysis.

Contents

Legal Update: *Stengart v. Loving Care Agency, Inc., et al.*
Supreme Court of New Jersey (March 30, 2010)

By Susan G. Feibus

E-Discovery and Federal Investigations

By Lisa C. Sullivan

Courts Limit the Effect of the Computer Fraud and Abuse
Act in Trade Secret Cases

By Richard H. Tilghman IV

Tech Corner

Discovery Deadlines, Understanding What is Involved

By Heidi Goldwater

E-Discovery and Federal Investigations

By Lisa C. Sullivan

Even for those well-versed in e-discovery issues, responding to a federal agency request may be daunting. Federal agencies often have unique and differing procedures for electronic document productions, and, often, it is desirable to respond quickly. The best preparation is, simply, expecting that the procedures may be nuanced, so that if a federal agency request hits your desk, you are not taken by surprise.

In this article, we compare and contrast the practices of three agencies: the Securities and Exchange Commission (the "SEC"), the Federal Trade Commission's Bureau of Competition (the "FTC"), and the Antitrust Division of the Department of Justice (the "DOJ").¹ The differing practices of these three agencies make an interesting study.

Of course, in a particular investigation, an agency will provide specific instructions that may differ from the practices we discuss. However, in the experience of Ungaretti & Harris attorneys who have represented clients before these agencies, staff typically follows these recommended e-discovery practices when they issue subpoenas, civil investigative demands, second requests, and the like. We have also found that the agencies are willing to discuss, and sometimes agree to, modifications when circumstances warrant.

Media for Submitting Responsive Documents

All three agencies will accept production of electronic documents on CDs, DVDs, or hard drives, but that is where the similarities end. While the DOJ states a preference for production on hard drive, the other two do not state a preference. The FTC will additionally accept production on flash drives, a media not mentioned by the SEC or DOJ. The FTC has detailed specifications for each type of media; for example, CDs must be "CD-R CD-ROM optical disks formatted to ISO 9660 specifications."

With respect to allowing agency access to hosted productions, the SEC has not articulated a policy. Both the FTC and DOJ warn that such access may be impossible due to technical issues and security protocols, but both are open to discussing such access. The FTC requires that a database have specific capabilities, such as text and field data searches, custom coding fields, and printing.

Production of Scanned Documents

The three agencies have slightly differing requirements for how scanned documents should be formatted. The SEC requests an image file, a delimited text file, OCR, and an opticon cross-reference. The FTC prefers TIF images with OCR text, with four specified fields. The DOJ indicates its wants image files with searchable OCR text.

Production of E-mails

Similarly, the agencies have differing requirements for production of e-mails. The SEC prefers e-mails be in delimited

text with images and native attachments, but will also accept Microsoft .pst or Lotus Notes .nsf files. The FTC prefers e-mails produced as TIF images with extracted text, and specifies 16 fields of metadata it wants. As for e-mail attachments, the FTC's formatting requirements differ based on whether the attachment is in Excel, Access, or some other program. The DOJ prefers e-mails and instant messages be produced as image files with searchable text, metadata, and bibliographic information.

Production of Other Electronic Documents and Data

For other types of electronic documents, the SEC sets out comparatively simple requirements: an ASCII delimited file containing the media associated with the file, the text extracted from the native file, and a directory path to the native file. The FTC has differing requirements for Excel files (native format with extracted text and metadata), Access and other multimedia files (native format with metadata), and other file types (images with extracted text and metadata). The FTC also outlines 14 fields applicable to metadata. The FTC alternatively may permit data to be submitted in native format with a "built" Concordance database. Like the FTC, the DOJ's requirements differ based on the document type (spreadsheets in native format with searchable text, metadata, and bibliographic information, and possibly only the first five pages imaged; presentations in native format and in slide image format with speaker notes with related searchable text, metadata, and bibliographic information; and other electronic files as image files with related searchable text, metadata, and bibliographic information).

Production of Data Using Proprietary Software or Databases

When production of electronic data involves proprietary programs, the SEC may, as an accommodation, consider web-based production or production on a dedicated computer. The FTC's guidance does not speak to proprietary programs, but in our experience, the FTC will request production if they are necessary to enable the FTC's review and analysis of data. The DOJ indicates it will request a list of databases with descriptions of each, then will discuss the production of databases.

Review software

The agencies vary in the programs they use for loading and reviewing electronic data, and these differences may impact production. The SEC uses Concordance 8.2 and Opticon 3.2, the FTC uses LexisNexis Concordance 2007 v 9.58, and the DOJ uses Summation.

Electronic Bates stamping

In civil litigation, parties are usually free to choose any Bates stamping convention. This is not necessarily the case for federal agencies. The SEC is fairly relaxed, permitting either numeric or alphanumeric conventions. The FTC's requirements are a bit more detailed; the FTC prohibits a space between the prefix and the numeric portion of a Bates number. The DOJ has the most detailed requirements. It prohibits use of a space, slash, backslash, or underscore in a Bates number, but recommends use of a hyphen. The DOJ also suggests that a Bates number use no more than three segments (for company, custodian, and number).

De-Duplication

Most e-discovery vendors have de-duplication capability to reduce the volume of documents and the associated expense, and experienced litigants usually discuss de-duplication at Rule 26(f) conferences. A similar discussion should be expected when dealing with a federal agency. The SEC's Manual is silent on de-duplication. The FTC, however, permits "vertical" de-duplication (eliminating duplication within a particular custodian's files), but requires approval from FTC staff for "horizontal" de-duplication (eliminating duplication across multiple custodians). The DOJ notes that it typically permits vertical de-duplication and has on occasion allowed horizontal de-duplication that preserves and produces information about blind copy recipients. The DOJ has not yet permitted "near-de-duplication," *i.e.*, eliminating all e-mails in a chain except for the final e-mail, but encourages parties who are interested to propose it to staff.

Writings Accompanying Productions

In civil litigation, parties do not typically provide an index of electronic documents. The federal agencies generally want an index of some sort. Together with the responsive documents, a response to the SEC should include a list briefly describing each item produced, and a list of the number of records produced per custodian. The FTC expects a list with comparatively more detail, such as Bates ranges for each custodian, the numbers of records per custodian, and the list of fields in the order in which they are listed on data files. The DOJ requests only an index of documents by custodian and Bates number.

* * * *

Federal agency investigations or subpoenas often come as a surprise, and generally have an accelerated schedule. Anticipating the nuances in electronic production to federal agencies is the best first step in preparing a quick and compliant response.

¹ The SEC's recommended practices for its staff members are set forth in Sections 3.2.6.2 and 3.2.6.2.3 of its Enforcement Manual, available online at <http://www.sec.gov/divisions/enforce/enforcementmanual.pdf>. The Bureau of Competition of the FTC has issued the "Bureau of Competition Production Guide: An eDiscovery Resource," available online at <http://www.ftc.gov/bc/guidance/index.shtml>. The Antitrust Division of the DOJ discusses practices in the article, "E-Discovery Initiatives at the Antitrust Division," available online at http://www.justice.gov/atr/public/electronic_discovery/243194.htm, and the attachments to that article.

Courts Limit the Effect of the Computer Fraud and Abuse Act in Trade Secret Cases

By Richard H. Tilghman IV

In recent years, employers increasingly have attempted to use the Computer Fraud and Abuse Act ("CFAA") against employees who wrongfully download confidential company information from their work computer. But lately, courts have limited the effect of the CFAA against employees who wrongfully access company data.

Section 1030(a)(5) of the CFAA creates civil and criminal penalties for the unauthorized access of a computer if such access causes "damage" or "damage and loss." "Damage" is defined as "impairment to the integrity or availability of data, a program, a system, or information." "Loss" is defined more broadly as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data program, system, or information. . ."¹ In trade secret cases, employers have argued that the CFAA provides a cause of action against employees who access confidential company information without authorization and use that information against the interests of the employer. But recent cases from the Northern District of Illinois have rejected the notion that economic losses from the unauthorized use of confidential information qualify as "damage and loss" under the CFAA.

For example, in *Del Monte Fresh Produce, N.A., Inc. v. Chiquita Brands Int'l*,² shortly before going to work for a competitor, an employee e-mailed herself confidential company data. The court held that merely accessing confidential data and using it to benefit a competitor was not the type of "damage" that the CFAA was designed to protect. In the absence of any deletion of company data or the installation of destructive software, the employee was not liable under the CFAA. Likewise, the court rejected the employer's attempt to recover the costs of hiring a technology consultant to search the employee's laptop, finding that the consultant was hired to assist the employer in the lawsuit, not to conduct a "damage assessment" of the company's computer systems.

Similarly, in *Mintel Int'l Group, Ltd. v. Neergheen*,³ the court rejected a claim for damages under the CFAA where an employee copied and e-mailed confidential company data because the employee did not destroy any data or disable any computer networks or databases. As in *Del Monte*, the court rejected the employer's claim for fees paid to a computer forensics expert because the expert was not conducting a "damage assessment" as that term is used in the CFAA.

These decisions have important implications for employers. First, employers will need to pursue traditional claims—such as breach of employment contract and trade secrets violations—against employees who access, but do not destroy, confidential information. Second, employers should be careful about how they retain information technology consultants to investigate employee misconduct. If such consultants are hired to determine whether an employee's wrongful access of company data damaged the company's systems, the employee may be liable under the CFAA. In contrast, employers are unlikely to recover the costs of hiring a computer forensics expert to assist during litigation.

¹ 18 U.S.C. § 1030(e).

² 616 F. Supp. 2d 805 (N.D. Ill. 2009).

³ No. 08-cv-3939, 2010 WL 145786 (N.D. Ill. Jan. 12, 2010).

Discovery Deadlines, Understanding What is Involved

By Heidi Goldwater

Your company is involved in a case with a fast approaching discovery deadline. What should you do? As soon as you have the request, you should work closely with your outside counsel to determine how much work will be involved in meeting the deadline. They will need to evaluate the data set, determine the best method of review, and set deadlines for production in order to meet the mandated deadlines.

Details of production format need to be discussed with outside counsel and agreed upon by all parties. For example, is the production going to consist of .tif image files or are native files being produced? Another question that typically arises is whether to produce data with or without OCR files. OCR files make the collection searchable. A large document production is not useful without searchable text files.

The Collection Process Time

Simply because you have the data in your possession, does not mean it is ready for production. The review process could take days or weeks depending on the volume. It is best to speak with outside counsel immediately after receiving the discovery request so that an appropriate amount of review time can be allotted prior to the deadline.

Discovery Data Types

There are also different types of data that may be responsive to the discovery request. It is important to make sure that a search of all types of data has occurred.

E-mail – Typically, you receive e-mail as either individual message files or as a message database, such as a Microsoft Outlook .pst file or a Lotus Notes .nsf file. During the mail review process by outside counsel, there may be messages originally collected that will not be produced either because they are not relevant or because of privilege.

User and other network files – These consist of all working files a custodian may store on their PC or a network file share. Each of these needs to be reviewed.

Forensic files – Many cases mandate that forensic images be taken of computers and file servers. This involves working with your outside counsel and forensic vendor and determining what data on the collected drives is to be filtered for searching.

Hardcopy files – These constitute any hardcopy working files your custodians may have. They also need to be reviewed for production.

The Review Process

Once you have collected all this data, there are many different strategies for review. You can discuss these various options with your outside counsel. Many law firms conduct online reviews. The law firm may send your data to a vendor and/or have the data processed for a review using the law firm's internal system, such as Summation or Concordance. Finally, many vendors offer review tools where they can host the data and the law firm's attorneys can log on remotely for the review.

Processing the Data for Production

Once the data has been reviewed and flagged for production, the next step is to have the data processed. This could take several days depending on the volume. Again, your outside counsel will work with you to make certain that the documents are Bates labeled for proper identification and contain any specific brandings such as "CONFIDENTIAL" or "ATTORNEYS EYES ONLY" if a protective order has been entered in the litigation. This is completed electronically.

It is important to remember that discovery requests may be more complex and time consuming than initially expected. Consulting with outside counsel upon receipt of the request and throughout the process will ensure your company meets the court imposed deadlines.

For further information on the E-Discovery and Document Management Group or this update, please contact one of our members:

| | | |
|------------------------|--------------|----------------------|
| Tina B. Solis, Editor | 312.977.4482 | tbsolis@uhlaw.com |
| Kamau A. Coar | 312.977.4343 | kacoar@uhlaw.com |
| Susan G. Feibus | 312.977.4877 | sgfeibus@uhlaw.com |
| Lisa C. Sullivan | 312.977.4465 | lcsullivan@uhlaw.com |
| Emily M. Dierberg | 312.977.4122 | emdierberg@uhlaw.com |
| Nile N. Park | 312.977.4125 | npark@uhlaw.com |
| Richard H. Tilghman IV | 312.977.4881 | rhtilghman@uhlaw.com |
| Heidi Goldwater | 312.977.9215 | hgoldwater@uhlaw.com |

This **E-Discovery Update** has been prepared by Ungaretti & Harris LLP solely for informational purposes and does not constitute legal advice. This information is not intended to create, and receipt of it does not constitute, an attorney-client relationship. Readers should not act upon this information without seeking professional counsel.

© Copyright 2010 UNGARETTI & HARRIS LLP
www.uhlaw.com