E-Discovery: The New Information Management Battleground

Latest Developments in the Law and Best Practices

Introduction

The following case summaries illustrate some of the technical challenges presented by the new electronic discovery rules, and how to address them. The cases highlight how technology, along with policy review and familiarity with the changes in the Federal Rules of Civil Procedure, can meet those challenges.

1. Inability to effectively search records raises ire of court

3M Co. v. Kanbar, 2007 U.S. Dist. LEXIS 78374 (N.D. Cal. Oct. 10, 2007)

1.1 Overview

During a deposition, a defense witness mentioned an email message that the defense had not produced during discovery. This raised doubts as to whether the defendant had produced all information responsive to the case, as it had previously certified. Although the court did not order another search, it did require the defendant to certify again that all responsive documents had been found, and to describe the actions it had taken to insure its search was complete. The court emphasized that, given the defense's failures during discovery, they had better be very sure that all documents had in fact been produced before they signed the new certification.

February 2008

P.O. BOX 1045 • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM

1.2 Case Study

In this case, the defendants did not have an effective records management system. They had little or no idea where or how responsive information was stored in their own systems. The defense was forced to rely upon manual searches by employees to try to find email messages and documents in order to respond to the plaintiff's discovery request. Despite the fact that the employees had already searched for responsive materials three times, they did not find everything, which led to an embarrassing revelation at a deposition. The court's displeasure was evidenced by its requirement that the defendants personally certify that all reasonable efforts had been made to find responsive materials. Given the defendants' reliance on manual searches, this was assuredly an unnerving prospect for those executives. If another responsive email were to turn up, it would mean violation of two certifications (including the original certification), plus a court order, exposing the defendants to the possibility of severe penalties.

1.3 Recommendations

A comprehensive records management solution would have permitted the attorneys to conduct the keyword searches the defense in this case could not. Employees could have set aside responsive materials in a special "legal hold" area. Beyond that, however, attorneys would have had the ability to search beyond these "legal hold" documents to other areas of the archive. Training is also an important part of the solution. Employees must be trained to recognize when they have information relevant to a case. Training is also critical to an overall records management system, so that employees will categorize company information in the correct category, as well as knowing when to discard material not relevant to litigation or other company business.

2. Preplanning can prevent "searching for a needle in a haystack"

MGP Ingredients, Inc. v. Mars, Inc., 2007 U.S. Dist. LEXIS 76853 (D. Kan. Oct. 15, 2007)

2.1 Overview

Plaintiff found itself in a dilemma when defendants produced over 48,000 documents in .TIFF format (i.e. image files) which were stored as maintained by the producer's custodians. Plaintiff complained that it was, "faced with a 48,000 page haystack and no guidance where to look for a few needles." The court had no sympathy for the plaintiff. It held that the defendant was under no obligation to organize or label its documents, produce an index, or match up the documents to particular requests. The court observed that the problem could have been prevented if the parties had conferred and come to an agreement on how the documents were to be produced.

2.2 Case Study

The problem for the plaintiff was that the order of the documents produced by the defendants had no meaning to the plaintiff. Another problem is that TIFF files are not searchable on their own. In many cases (apparently here, although not discussed by the court), they must be processed through optical character recognition software in order for the files to be searchable.

The plaintiff was tripped up by a big "OR" in the Federal Rules. Rule 34 states that documents can either be produced as they are stored in the ordinary course of business, OR they can be

organized and labeled to correspond with the categories in the request. The defendants chose the former option, and the court found that they were not required to do any more than that. The plaintiff was stuck with a haystack of its own making.

2.3 Recommendations

This case offers a cautionary note for the corporate IT department which is acting as the technical resource for its legal counsel. Merely asking for electronic data is not enough. Consideration should be given to the format in which that data will be produced. The court itself stated that the plaintiff could have avoided the situation by discussing the format of production with the defendants beforehand. They could have requested that the defendants produce the material in accordance with the order of the search request, and, failing that, could have asked the court to enter an order mandating the form of production. In addition, the plaintiff could have asked for production in a different format than TIFF—production in the documents' native format, for example. In addition to searchability, plaintiffs could get "metadata," additional information about the documents such as file creation dates, last accessed dates, or sometimes even previous document drafts! As the defendants included hard copy documents within their electronic production, plaintiff could have asked that the production format of those documents be in searchable PDF format. In that way, even if defendants made mistakes in classifying their documents, plaintiffs would have had the ability to search through them to find meaningful documents.

3. Defendant's casual attitude towards discovery leads court to appoint an outside vendor to conduct it

Wingnut Films, Ltd. v. Katja Motion Pictures Corp., 2007 U.S. Dist. LEXIS 72953 (C.D. Cal. Sep. 18, 2007)

3.1 Overview

Defendant conducted a minimal search for electronic documents—clicking through a few folders on two servers, and only three of eleven employees requested even searched for responsive e-mails. Furthermore, defendant took no steps to stop its automatic deletion policies, continuing to purge emails every thirty days and reuse email backup tapes every week, even after receiving electronic discovery requests.

3.2 Case Study

Not only did defendant fail to undertake any meaningful searches of its electronic systems, counsel several times certified that all responsive documents had been produced. These certifications were made after the court had entered orders requiring defendant to respond to plaintiff's discovery requests. It was only after document custodians had been deposed that the truth about defendant's discovery failures came to light. As a result, the court appointed a third party discovery vendor to conduct independent searches of defendant's network and email servers, as well as the hard drives of key employees. Defendant was required to pay all costs and expenses of the vendor, as well as plaintiff's attorney's fees and costs.

3.3 Recommendations

The case illustrates an extreme example of the consequences of failure to take discovery obligations seriously. A party can lose control of the discovery process if it fails to take what a court would consider adequate steps to respond to discovery requests. These steps include extensive discussions between counsel and the IT department so counsel can understand where all potentially responsive electronic documents are located. A comprehensive strategy for responding to the requests should be formulated. The party should also make sure that recycling of backup tapes of systems containing data is suspended. Good faith searches of electronic systems for responsive material are both time-consuming and expensive. It is better to incur the time and expense up-front, rather than paying someone else to do it, with little control over the results.

4. Plaintiff required to bear cost of recombining emails with attachments

PSEG Power New York v. Alberici Constructors, Inc., 2007 U.S. Dist. LEXIS 66767 (N.D.N.Y. Sep. 7, 2007)

4.1 Overview

The controversy centered around 3000 emails which had been separated from their attachments due to incompatibility between the discovery vendor's software and the producer's email system. The defendant, who requested the data, asserted that the plaintiff should pay to recombine the emails with the attachments, as it demonstrated the impracticality of recombining the emails manually. The court agreed.

4.2 Case Study

Defendant had established that the emails, along with their attachments, were relevant to its case. One of the court's key findings was that emails are stored with their attachments in the ordinary course of business; thus, once attachments become separated from the emails, they are no longer stored as kept in the ordinary course of business. Thus, plaintiff's production did not meet the requirements of Rule 34. Although the original source files were still available (Outlook PST files), plaintiff refused to provide them to defendant, as they contained other confidential information.

4.3 Recommendations

The case highlights the need for good quality control. The original disk provided by the plaintiff to the defendant contained no email attachments at all, which a quick review of the disk would have revealed. The plaintiff should have undertaken some test production runs, which would have disclosed the problem at an earlier stage. A company seeking to comply with a discovery request for email in electronic format should carefully investigate the exporting capabilities of its email system. Several tools are available which are designed to pull data from email systems for the specific purpose of complying with electronic discovery requests.

5. Non-party to suit required to produce subpoenaed data in electronic format

Auto Club Family Ins. Co. v. Ahner, 2007 U.S. Dist. LEXIS 63809 (E.D. La. Aug. 29, 2007)

5.1 Overview

Courts are usually reluctant to impose any penalties upon third parties who are dragged into cases. However, in this case, the third party was required to produce its hard copy production again in electronic format. Although it had produced data in hard copy format, the defendant had asked for it electronically. There were indications that the hard copies did not contain all of the material relevant to the case, such as working papers or rough drafts. The third party had provided no evidence that producing the requested material again in electronic format would be unduly burdensome to them.

5.2 Case Study

The third party had failed to provide evidence that the requested data was not reasonably accessible because of undue burden or cost. It also failed to provide any specific facts to justify why the defendant should not have access to the data it requested in electronic format. Since under the new federal rules, electronic data stands in equal footing with paper documents, producing the data in hard copy format is not a valid objection when the party asks for it electronically.

5.3 Recommendations

The electronic discovery amendments to the Federal Rules of Civil Procedure have created a new paradigm for electronic data. It is now more difficult to justify not producing electronic data. Since such data is now on the same footing with paper documents, when parties ask for electronic data, the burden now shifts to the producing party to establish that it is too difficult or costly to produce. Mere statements that producing the data electronically is too expensive will not suffice, since many programs have data exporting capability built in. An example of "inaccessibility" would be data files from an old application which no longer works (perhaps it runs on old hardware the company no longer possesses). Even that's not the end of the story, since vendors exist to convert legacy data to modern applications. The party which doesn't want to produce data electronically may have a difficult road ahead of it.

6. No recovery for hacker's access to bank customers' confidential information

Pisciotta v. Old National Bancorp, 499 F.3d 629 (7th Cir. 2007)

6.1 Overview

Plaintiffs sought damages for harm suffered as a result of a security breach in which a hacker gained access to the personal information of tens of thousands of bank customers. They sought

compensation for the cost of credit monitoring services they had already paid for and would pay for in the future. The appellate court affirmed the dismissal of their claim in the district court, as plaintiffs could not establish any concrete harm, such as money electronically stolen from their bank accounts. Plaintiffs could not recover for anticipated harm.

6.2 Case Study

Plaintiffs were part of a class action against a bank which solicited its customers' confidential information over the Internet, but failed to adequately protect that information from outside intruders. However, the plaintiffs were unable to establish that any financial loss had occurred as a result of that breach, nor could they establish that any identity theft had likewise occurred. Their request for compensation for credit monitoring services was not viable as it requested damages for future harm, not harm already suffered. Relevant statutory law only required notification (as was done), and the court noted that no law of any other state supported plaintiffs' claims.

6.3 Recommendations

In the event of a security breach, the IT department should notify legal counsel as soon as possible about the breach. In Indiana (applicable law in this case) and in other states, the corporate victim of the breach is required to notify those affected. Once it does so, it has fulfilled its obligations under the law, as did the defendant in this case. A company's failure to do so could expose it to fines and costs of prosecution, but not private suits (at least in Indiana). A company should not look to this case as a basis for reducing expenditures on IT security, however. The court leaves open the possibility of compensation for plaintiffs who can prove they suffered actual harm from the security breach—that their identity was stolen, or they suffered some actual loss.

7. Summary

The electronic discovery amendments to the Federal Rules of Civil Procedure have spawned an extensive amount of litigation as the courts seek to apply those new rules to specific situations, a challenging task given the quickly-advancing state of technology. For the most part, litigants who have kept up with the developments in the area and have taken steps to incorporate the new reality into their business environment, from both a technology and policy standpoint, have fared well in litigation. On the other hand, the cases are replete with examples of those who have stuck their heads in the sand and conducted business as usual. Companies which fail to acknowledge this new reality run the risk of creating unnecessary hurdles for themselves in litigation. Given the fact that the vast majority of documents being created today are electronic and may never be incorporated into hard copies, this risk is very real.

Some general observations can be made from the cases examined:

- **Failure to invest in new technology can put the company at risk.** The lack of a keyword search capability forced the defendant in *3M* to rely upon manual searches to find its documents, with the result that some got through the cracks, and earned them a warning from the judge. This was undoubtedly the case in *Wingnut* as well, although the lackadaisical attitude of the defendant towards its discovery obligations was a greater contributor to the sanctions levied against it. A modern e-mail archiving solution could have helped to alleviate the central problem in the *PSEG New York* case (separation of e-mails from their attachments).

- **Familiarity with the Federal Rules amendments is essential.** Ignorance of the new amendments resulted in sanctions in *Wingnut* and left the plaintiff in *MGP Ingredients*

with a 48,000 page "haystack". The third party in *Auto Club* was forced to produce again electronically what it had already produced in hard copy format. As time goes on, courts will become increasingly less tolerant of those who refuse to comply with the Rules.

- **Policies must be written or modified to conform to the new paradigm.** The defendant in *Pisciotta* had reviewed important data security legislation and avoided liability for a data intrusion by notifying those affected as required by the statute. Companies must be cognizant of legal developments in the information technology field and be ready to respond accordingly.

What should the company which is faced with a lawsuit do? The realities of the electronic information age require an immediate response.

- **Begin identifying potentially responsive electronic content <u>now.</u>** Who are the key players in the dispute? What types of electronic media are involved? The sooner a comprehensive source map of potentially responsive electronic data is compiled, the better off the company will be. Any medium is fair game, from the obvious (email, word processing documents, spreadsheets) to the not-so-obvious (personal digital assistants, cell phones, instant messaging). The IT department can play a critical role here.

- **Implement a "litigation hold."** As soon as responsive material is identified, steps must be taken to preserve it. Automatic deletion processes which threaten the data must be disabled. Those involved must be warned not to dispose of any responsive material. In some cases (for example, a trade secret misappropriation case involving a laptop computer), special "forensic" handling of the data or device may be advisable. Coordination with the IT department is essential in order to accomplish this. If your company uses backup tapes for archiving purposes (i.e. retrieval of mistakenly deleted data) instead of for disaster recovery purposes only, the backup tapes are targets for discovery requests.

- **Coordinate with litigation counsel.** Early involvement of litigation counsel is crucial. They can advise as to whether you are taking the right steps concerning data preservation. They may also be able to reduce preservation burdens by negotiating with the other side (i.e. agree that backup tapes will not be sought). In any event, in the federal system, scheduling orders, including provisions for disclosure or discovery of electronically stored information, are issued within 120 days after the complaint is served on the defendant. Thus, getting litigation counsel up to speed on the electronic data environment is important.

These actions are just the tip of the iceberg. For example, after the data is identified, it will need to be compiled and reviewed, and some ultimately will be produced to the other side. Many companies hire outside vendors to assist in this effort.

If not faced with an immediate lawsuit, companies can take steps to reduce the risk of error should litigation arise.

- **Identify all sources of electronic data.** Going through a "mapping of sources'" exercise in an orderly fashion while not under the time pressure of litigation will increase the accuracy of the source map, while also giving management an idea of the magnitude of the electronic records management challenge.

- **Develop a retention strategy.** There is no reason for a company to retain information not related to the business, or business information for longer than business or legal considerations require (except if subject to a "litigation hold"). Large volumes of data can unnecessarily increase search and review costs, and the enterprise may be unnecessarily keeping old data which it will never again use.

- **Investigate technological solutions.** Archiving solutions can save money in the long run by centralizing business information. Deduplication technology can reduce costs by allowing retention of only one of many possible duplicate carbon copies or e-mail strings sent to many

company recipients. The process of searching for responsive data is streamlined. Retention policies can be automatically enforced by identifying data for deletion after the retention period has expired (or by automatically deleting such data). Those same policies can be easily (and selectively) suspended in the event of a litigation hold. Finally, central storage of data also facilitates the review and production process once in litigation.

- **Review electronic data policies.** Does the company have effective email, records management, or legal hold policies? Lack of standards for email, for example, could expose the company to liability for a hostile work environment if offensive emails are not prohibited. A properly promulgated legal hold policy can prepare employees for potential legal holds more effectively than a hastily issued one.

Again, these steps are only the beginning. They must be accompanied by high-level management commitment and support, an appropriate infrastructure (both company and technical), and effective training, auditing, enforcement and improvement programs. Addressing the problems, however, will lead to dividends down the road.

8. About Kahn Consulting

Kahn Consulting, Inc. (KCI) is a consulting firm specializing in the legal, compliance, and policy issues of information technology and information lifecycle management. Through a range of services including information and records management program development; electronic records and email policy development; Information Management Compliance audits; product assessments; legal and compliance research; and education and training, KCI helps its clients address today's critical issues in an ever-changing regulatory and technological environment. Based in Chicago, KCI provides its services to Fortune 500 companies and government agencies in North America and around the world. Kahn has advised a wide range of clients, including Time Warner Cable, Ameritech/SBC Communications, the Federal Reserve Banks, International Paper, Dole Foods, Sun Life Financial, Kodak, McDonalds Corp., Hewlett-Packard, United Health Group, Prudential Financial, Motorola, Altria Group, Starbucks, Mutual of Omaha, Merck and Co., Cerner Corporation, Sony Corporation, and the Environmental Protection Agency. More information about KCI, its services and its clients can be found online at: www.KahnConsultingInc.com.

WHERE LAW & TECHNOLOGY MEET

KAHN
CONSULTING INC.

www.KahnConsultingInc.com info@KahnConsultingInc.com 847-266-0722

P.O. BOX 1045 • HIGHLAND PARK IL • 60035
PHONE: 847.266.0722 • FAX: 847.266.0734 • EMAIL: INFO@KAHNCONSULTINGINC.COM