

## Chapter 1

# What is Electronic Evidence?

*By Nick Akerman and Angeline Chen*

- § 1:1 Introduction
  - § 1:2 1970 Amendment to Rule 34
  - § 1:3 The *Zubulake* decisions
  - § 1:4 The Sedona Conference
  - § 1:5 December 2006 Amendments to the Federal Rules of Civil Procedure
  - § 1:6 September 2008 addition of Rule 502 to the Federal Rules of Evidence
  - § 1:7 Impacts on in-house counsel
  - § 1:8 Business and records management processes
  - § 1:9 Attorney-client and work product privileges
  - § 1:10 International implications
  - § 1:11 Privacy and other confidentiality obligations
  - § 1:12 Corporate governance
  - § 1:13 Conclusion
- Appendix 1A. Sedona
- Appendix 1B. Federal Rules of Civil Procedure

**KeyCite®:** Cases and other legal materials listed in KeyCite Scope can be researched through the KeyCite service on Westlaw®. Use KeyCite to check citations for form, parallel references, prior and later history, and comprehensive citator information, including citations to other decisions and secondary materials.

### § 1:1 Introduction

Now, more than ever, in-house corporate counsel are critical to the success of the company's litigation. In-house corporate counsel remain the focal points to partner with outside counsel on trial strategy, points of law, and company personnel knowledgeable about facts on a particular litigation. Today, they must also serve as: (1) outside counsel's point of contact for the company's information systems (including networks, intranets, computers, personal digital assistants, and portable storage devices)—what potential evidence resides on those information systems, how information is maintained on those systems (as well as how those

systems are maintained), and the identity of the custodians of that data; and (2) the internal lead or facilitator to the corporation's information technology departments and personnel, in whom the technical expertise and knowledge about those information systems and computers reside. In today's business world, information systems are where much, if not all, of the evidence needed to understand, prove, or defend a case resides. Gone is the era when in-house corporate counsel and law firms would simply need to send teams of attorneys and paralegals to company files and warehouses to scour boxes of documents to search for the one piece of paper that would prove its case. Instead, substantial portions of the discovery process have become almost entirely computerized.

The same information that was contained on paper and filed in boxes is now also stored as bits and bytes of data on computers and network systems. The ubiquitousness of electronic mail, the ease of computer usage, relatively inexpensive storage, and the inconvenience threshold of individual discipline in appropriately deleting or managing electronically stored information has also resulted in the creation of vast oceans of electronically stored data that far exceeds the paper boundaries of yesterday. In today's brave new world, in addition to the company files and warehouses, in-house counsel is required to enlist (or become) savvy information technology individuals, teamed with attorneys and paralegals, to scour company servers, workstations, computers, and backup tapes to sift through gigabytes, terabytes, and eventually petabytes of ones and zeros for the relevant data that the new rules require be preserved and managed. Today, the data is downloaded to a central database and the same paralegals and attorneys search with a couple clicks of the mouse for relevant evidence using keywords. Gone is the era where identifying the issues for the review team was sufficient—at a minimum, paralegals and associates must be familiar with de-duplication, maintaining an electronic chain of custody, appropriately identifying key words, and crafting thoughtful Boolean searches that can withstand downstream challenges from the opposing party.

Electronically stored information (ESI) is essentially anything that can be stored in electronic form on a computer or other media device. A computer is broadly defined by federal statute to mean "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunc-

tion with any such device.”<sup>1</sup> This includes all desktop and laptop computers, personal digital assistants, iPods, floppy disks, CDs, DVDs, USB flash drives, backup tapes, voice mail, servers, and access control systems. In addition, the Fed. R. Civ. P., as amended on December 1, 2006, now also define ESI subject to discovery as also expressly encompassing sound and video recordings, voice mails, and the like.

ESI differs from regular paper documents in a number of significant respects. First, the volume of electronic documents, particularly e-mail, can be massive and duplicative. Companies can receive millions of e-mails per day that can be dispersed over multiple computers between the sender and recipients, servers, portable handheld devices, and backup tapes. Second, electronic documents contain what is known as metadata that records such information as prior drafts of the document, its author and time and date stamps showing when the document was created, last accessed, and last saved, as well as other attributes. Third, electronic documents contain dynamic content that is subject to change. Simply opening and closing a document on the computer can change its last accessed date and other metadata associated with that document. Fourth, data, unlike paper documents, even when destroyed, can often be extracted from the computer’s hard drive using special forensic software. Fifth, electronic data is not always easily accessible and determining the reasonability of that accessibility can be dependent upon the technology and information systems involved. ESI that exists only on a backup tape, for example, may take a long time to locate and access and in some instances may require the use of equipment that is obsolete. Preservation and eventual recovery of such information, however, may be required if the information itself cannot otherwise be obtained. Finally, the “content” of ESI—unlike hard copy documents—can be rendered incomprehensible if separated from the system on which it was either created or managed (e.g., legacy or specialized and proprietary systems).

The move from paper to encompass a wider spectrum of computer-based discovery has not been an easy transition for lawyers, whether in-house or outside, or their respective clients. There have been a number of bumps along the way exemplified by a series of well-known court decisions sanctioning parties for not properly complying with their electronic discovery obligations. In certain instances, these transgressions may have been caused by “the lack of expertise on the part of parties and their lawyers

---

[Section 1:1]

<sup>1</sup>18 U.S.C.A. § 1030(e)(1).

in computer technology and data processing,”<sup>2</sup> but in other instances, courts have found that such conduct bordered on fraud or reckless indifference. In *In re Telxon Corp. Securities Litigation*, the magistrate judge recommended that a default judgment be entered against Pricewaterhouse-Coopers, LLP, for failing to comply with its electronic discovery obligations and made the following findings of reckless indifference or fraud with respect to its electronic discovery obligations:

PwC failed at the start of discovery to check thoroughly its local servers and its archives for relevant documents, failed to compare the various versions of relevant documents on those databases, failed to produce documents as they were kept in the ordinary course of business, and failed to reproduce thoroughly and accurately all documents and their attachments. Prior to litigation PwC had permitted destruction of documents despite committing to their preservation. Despite these failures, PwC time and time again told the court and the parties that it had made a complete disclosure of all relevant documents and attachments and that it had produced them in the order in which they were stored by PwC. The only conclusion the court can reach is that PwC and/or its counsel engaged in deliberate fraud or was so recklessly indifferent to their responsibilities as a party to the litigation that they failed to take the most basic steps to fulfill those responsibilities.<sup>3</sup>

It is precisely this type of opinion that keeps corporate counsel up at night. The amendments to the FRCP in December 2006 addressing electronic discovery have further contributed to this concern. This chapter will review the historical context in which these amendments were promulgated and provide an overview of the amended rules.

### § 1:2 1970 Amendment to Rule 34

While electronic discovery is a hot issue for corporate counsel today, it did not start with the amendments to the Federal Rules of Civil Procedure (FRCP) in December 2006. In 1970, nearly 40 years ago, Rule 34 of the FRCP was amended to expand the definition of a document to include “data compilations from which information can be obtained, translated if necessary, by the respondent through detection devices into reasonably usable form.” While 1970 was in the dark ages of the computer era, the Advisory Committee Notes stated that the purpose of this change in the definition of documents was “to accord with changing technology.” The Advisory Committee further explained that this amendment

---

<sup>2</sup>*Bills v. Kennecott Corp.*, 108 F.R.D. 459, 462, 40 Fair Empl. Prac. Cas. (BNA) 1182, 42 Empl. Prac. Dec. (CCH) P 36732 (D. Utah 1985).

<sup>3</sup>*In re Telxon Corp. Securities Litigation*, 2004 WL 3192729, at \*33 (N.D. Ohio 2004).

makes clear that Rule 34 applies to electronic data compilations from which information can be obtained only with the use of detection devices, and that when the data can as a practical matter be made usable by the discovering party only through respondent's devices, respondent may be required to use his devices to translate the data into usable form. In many instances this means that respondent will have to supply a printout of computer data.

The Advisory Committee further recognized that the burden in producing electronic discovery "placed on the respondent will vary from case to case, and the courts have ample power under Rule 26(c) to protect respondent against undue burden or expense, either by restricting discovery or requiring that the discovering party pay costs" and that "if the discovering party needs to check the electronic source itself, the court may protect respondent with respect to preservation of his records, confidentiality of nondiscoverable matters, and costs."

Initially, electronic discovery involved relatively simple document requests that mirrored the simple ways computers were used at the time. For example, in *Adams v. Dan Rivers Mill, Inc.*,<sup>1</sup> the plaintiffs in a race discrimination case "sought the defendant's current computerized master payroll file and all computer print-outs for W-2 forms of the defendant's employees" to prepare statistics upon which discriminatory practices could be determined. The court rejected the defendant's request to limit the production to a computer printout and held that "[b]ecause of the accuracy and inexpensiveness of producing the requested documents in the case at bar, the court sees no reason why the defendant should not be required to produce the computer cards or tapes and the W-2 print-outs to the plaintiffs."<sup>2</sup>

*Bills v. Kennecott Corp.*<sup>3</sup> addressed the issue of which party bears the cost of producing the employee data in an age discrimination case. The defendant sought to shift the approximated \$5,400 cost of producing the computer printout to the requesting plaintiff. The court recognized that the Advisory Committee statement to Rule 34 provides "no guidance as to how properly to determine whether the burden or expense is 'undue' where

---

[Section 1:2]

<sup>1</sup>Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 221, 4 Fair Empl. Prac. Cas. (BNA) 523, 4 Empl. Prac. Dec. (CCH) P 7754, 15 Fed. R. Serv. 2d 1275 (W.D. Va. 1972).

<sup>2</sup>Adams v. Dan River Mills, Inc., 54 F.R.D. 220, 222, 4 Fair Empl. Prac. Cas. (BNA) 523, 4 Empl. Prac. Dec. (CCH) P 7754, 15 Fed. R. Serv. 2d 1275 (W.D. Va. 1972).

<sup>3</sup>Bills v. Kennecott Corp., 108 F.R.D. 459, 462-64, 40 Fair Empl. Prac. Cas. (BNA) 1182, 42 Empl. Prac. Dec. (CCH) P 36732 (D. Utah 1985).

discovery of computer stored information is concerned.”<sup>4</sup> The court declined to shift the cost of production to the requesting plaintiffs finding that “(1) the amount of money involved is not excessive or inordinate; (2) the relative expense and burden in obtaining the data would be substantially greater to the requesting party as compared with the responding party; (3) the amount of money required to obtain the data as set forth by defendant would be a substantial burden to plaintiffs; (4) the responding party is benefited in its case to some degree by producing the data in question.”<sup>5</sup>

---

<sup>4</sup>Bills v. Kennecott Corp., 108 F.R.D. 459, 462-64, 40 Fair Empl. Prac. Cas. (BNA) 1182, 42 Empl. Prac. Dec. (CCH) P 36732 (D. Utah 1985).

<sup>5</sup>Bills v. Kennecott Corp., 108 F.R.D. 459, 464, 40 Fair Empl. Prac. Cas. (BNA) 1182, 42 Empl. Prac. Dec. (CCH) P 36732 (D. Utah 1985).