Washington Journal of Law, Technology & Arts

Volume 5
Issue 5 *Supplement*

Article 4

4-1-2009

Evaluating *Columbia Pictures Industries v. Bunnell* and the Role of RAM under the Federal Rules of Civil Procedure on E-Discovery

Loren M. Hall

Cite as: Loren M. Hall, *Evaluating Columbia Pictures Industries v. Bunnell and the Role of RAM Under the Federal Rules of Civil Procedure on E-discovery*<, 5 SHIDLER J. L. COM. & TECH. 23 (2009), *available at* <http://lctjournal.washington.edu/vol5/a23Hall.html>

EVALUATING COLUMBIA PICTURES INDUSTRIES V. BUNNELL AND THE ROLE OF RAM UNDER THE FEDERAL RULES OF CIVIL PROCEDURE ON E-DISCOVERY

Loren M. Hall[1]

Abstract

In 2007, the District Court for the Central District of California required the preservation of data stored in random access memory (RAM), which sparked significant commentary about the rapidly expanding realm of electronically-stored discoverable information. This Article addresses the impact of *Columbia Pictures Industries v. Bunnell* in the context of the duty to preserve and produce documents, and the scope of information that can be subject to e-discovery obligations. This Article also describes how the 2006 amendments to the Federal Rules of Civil Procedure provide a necessary limitation—reasonableness—on the costly and unrealistic preservation, and subsequent production, of electronic information. Furthermore, this Article discusses how *Columbia Pictures Industries v. Bunnell*, like several other recent federal court cases involving e-discovery, fits within a broader trend in e-discovery litigation that recognizes new forms of electronic information with the same limits of reasonableness. It closes by reviewing the important reminders given by *Columbia Pictures Industries v. Bunnell*, including future trends and the need for data retention policies.

Table of Contents

Introduction
Brief History of E-discovery and the 2006 Amendments to the Federal Rules of Civil Procedure
Duties and Procedures: The Background of *Columbia Pictures Industries v. Bunnell*
    The Duty to Preserve
    Defining the Scope of Discoverability
Where *Columbia Pictures Industries v. Bunnell* Fits Within the Amended Federal Rules' Realm of Reasonability
Going with the Flow: Broadening the Scope of Discoverable Evidence
    The Importance of a Sound Litigation Hold Procedures and Data Destruction Policies
Conclusion
Practice Pointers

INTRODUCTION

<1>Technology has changed the way information is stored and communicated. Today, the type of information subject to electronic discovery (e-discovery) under the Federal Rules of Civil Procedure varies greatly in terms of volume, range, and how such information may be deleted.[2] Managing electronic information in anticipation of

litigation, evaluating the costs of production during litigation, and protecting privileged material are all factors that make e-discovery potentially time-consuming and difficult.[3]

<2>As the law of e-discovery continues to evolve, a pertinent question remains as to the scope of a party's duty to preserve discoverable electronically-stored information. The case of *Columbia Pictures Industries v. Bunnell* brought that question to the forefront of the legal community.[4] In *Bunnell*, a federal magistrate ordered a defendant to preserve and produce server logs that contained data stored in random access memory (RAM);[5] the decision was upheld by the district court.[6] The conclusion that data stored in RAM was discoverable garnered the attention of legal press, which noted that the decision could make preservation of data "extraordinarily burdensome,"[7] cause "e-discovery anarchy,"[8] or potentially "open up a landslide of new discovery obligations."[9]

<3>Nevertheless, the *Bunnell* decision is unique in its treatment of data stored in RAM, and does not greatly change the nature of e-discovery or indicate a trend toward unmanageable duties of preservation in civil litigation. This Article discusses the *Bunnell* decision within the context of the 2006 amendments to the Federal Rules of Civil Procedure and the duties of preservation and production. After analyzing *Bunnell* alongside other developments in e-discovery case law, this Article demonstrates that *Bunnell* falls within the existing e-discovery framework. Though novel, *Bunnell* is dependent upon its facts, and fits within a broader trend in e-discovery that recognizes new forms of electronic information while still limiting the expansion of preservation and production by what is "reasonable."

BRIEF HISTORY OF E-DISCOVERY AND THE 2006 AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE

<4>Both Congress and the courts have recognized the need to amend the rules of discovery to account for changes in technology affecting the storage of information. Since the amendment of the Federal Rules of Civil Procedure to include electronic data within the definition of "documents,"[10] courts have interpreted these rules to protect producing parties from undue burden and expense. However, the courts have also continued to expand the scope of the type of information that must be preserved.[11] Moreover, the courts have also addressed the challenges in e-discovery in several landmark cases by developing new tests for determining accessibility and allocating costs.[12]

<5>Facing these developments, the federal judiciary's Civil Rules Advisory Committee amended the Federal Rules of Civil Procedure to better accommodate the information age. The Supreme Court approved the amended rules on April 12, 2006,[13] and changed the federal civil discovery rules in several significant ways. For instance, the types of electronic data related to core litigation issues had outgrown their categorization as a type of "document," and as such, the committee recognized "electronically stored information" as being apart from other "documents."[14] Other changes included the following: (1) a requirement that the parties meet early in litigation to discuss and plan for electronic discovery;[15] (2) new rules addressing the production of information that is not reasonably accessible;[16] (3) review of privileged content;[17] (4) adequate forms of production;[18] and (5) appropriate sanctions for discovery violations.[19]

<6>Decided after these new rules became effective, the *Bunnell* decision reflects the technological developments that brought about the changes in the rules. Within the new rules framework, *Bunnell* involves three key issues: the duty to preserve documents, the obligation to produce such documents, and the scope of information that can be subject to e-discovery obligations.

<7>*Columbia Pictures Industries v. Bunnell* is a case that involves technology, which provides a rich setting to address issues regarding e-discovery rules. Defendant Bunnell operated TorrentSpy, a Web site featuring a search engine that allowed users to search, locate, and download dot-torrent files.[20] The search engine, along with the appropriate software and network of users, facilitated the copying and distribution of music, film, and other files sought by the users.[21] The plaintiffs alleged that these files were unauthorized copies of copyrighted material,[22] and that TorrentSpy knowingly enabled and profited from the sharing of copyrighted films and television programs.[23]

<8>Columbia Pictures filed a motion seeking an order that Bunnell preserve and produce a number of records that would give information on the users who had accessed the site, including the types of files searched for, shared, and the dates of the relevant transactions.[24] Due to the nature of TorrentSpy's online business model, the requested data was temporarily stored in its systems' RAM; the data would be archived in server data logs only if necessary.[25] Because federal courts had never before ordered data stored in RAM to be preserved and produced, the court faced a novel issue in e-discovery: whether information stored in RAM constituted discoverable electronically-stored information, and whether preservation and production of such stored information was required by law. In spite of facing an original legal scenario, the resulting court order fit well within developed case law on the duty to preserve electronic evidence and the limits on its production during discovery.

The Duty to Preserve

<9>In general, if information is relevant to a dispute, parties have a duty to preserve evidence once litigation is reasonably anticipated.[26] In response to this obligation, companies often initiate a "litigation hold" preventing the destruction of potentially discoverable material.[27] In tangible document terms, this means that the party must stop shredding hard copy files. In cases of e-discovery, this can become an affirmative duty to enable or enhance the party's existing preservation policies or controls, which are often implemented through networked technology systems.

<10>Failure to perform this affirmative duty where necessary may be considered "spoliation," or the destruction of evidence during pending or reasonably foreseeable litigation.[28] In cases of spoliation, a party may request that the court impose sanctions on the other party if it believes that the non-moving party is breaching its duty to preserve relevant evidence.[29] Sanctions can range from fines to termination of the lawsuit with prejudice, depending on the severity of the spoliation.[30]

<11>To prevent onerous and expensive affirmative burdens of preservation for businesses during their ordinary day-to-day operations, the new rules also include a "safe harbor" provision in Federal Rule of Civil Procedure 37(f). The rule relevantly states that, "[a]bsent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of the routine, good-faith operation of an electronic information system."[31] Thus, the provision prohibits courts from penalizing organizations for the routine destruction of electronic information prior to the onset of litigation. In *Bunnell,* for example, the federal magistrate judge refused to grant the plaintiffs' motion for sanctions, citing Rule 37(f) and the lack of precedent directly on point that could support a finding that destruction of RAM data information was done in bad faith and in violation of TorrentSpy's preservation obligations.[32]

<12>Despite this application of the safe harbor in *Bunnell,* parties should avoid relying too heavily upon its protection. The provision will not protect improper destruction of records once litigation is reasonably

anticipated.[33] Also, the provision is relatively untested and its full effect on e-discovery remains contested.[34] Moreover, its protection may be limited to the use of systems that, in regular operation, delete, overwrite, or alter certain types of relevant data, such as RAM.[35] Nevertheless, the addition of Rule 37(f) does limit the duty of preservation by recognizing the lawfulness of routine electronic data destruction. This indicates that although more types of data may be called into court, the rules provide reasonable limits on what needs to be preserved and produced.

Defining the Scope of Discoverability

<13>Even if electronic evidence is properly preserved prior to litigation, a court may elect not to require its production. The Rules provide courts with numerous factors to consider when deciding if electronic data must be produced for the opposing party during discovery. These factors include the relevance of the data to the issues litigated,[36] and whether the data is so important as to outweigh the costs or burdens associated with its inaccessibility.[37]

<14>The test of relevancy, like that for all potentially discoverable material, is rooted in the rules of evidence.[38] If this test is met, Federal Rule of Civil Procedure 26(b) additionally provides that it can be subject to a production request: "[p]arties may obtain discovery regarding any nonprivileged matter that is relevant to any party's claim or defense . . . ."[39] However, the test for what constitutes "reasonably accessible," and which party should bear the costs of producing inaccessible evidence is not articulated in the rules themselves. As such, courts have imposed their own parameters.

<15>For example, in *Zubulake v. UBS Warburg*,[40] the District Court for the Southern District of New York classified data as being either "relatively accessible" or "relatively inaccessible," depending on how it is stored. Each category also has its own sub-categories. Relatively accessible data is data that is kept in an accessible format, which includes active, online, or hard drive data. In addition, accessible data also involves data that is retained as near-line data, which includes information on optical disks or an offline storage archive. By contrast, relatively inaccessible data includes backup tapes and erased, fragmented, or damaged data.[41] The *Zubulake* Court used these categories of accessibility and other factors to decide whether the costs of production may be shifted from the producing party to the requesting party.[42]

<16>The 2006 amendments utilize the *Zubulake* decision's language on accessibility to limit the scope of discoverable information. Indeed, the rules now create a similar categorized system. Information that is deemed not reasonably accessible by the responding party must only be produced if the requesting party can demonstrate "good cause" and reasonableness; "good cause" is based upon relevancy and a determination that the material is not overly duplicative of other reasonably accessible data.[43]

<17>For example, in *Ameriwood Industries, Inc. v. Liberman*,[44] the plaintiff employer alleged that former employee defendant had sabotaged the plaintiffs' business.[45] In response, the defendant claimed that any of the defendant's lost sales were due to poor business management, and requested production of hundreds of thousands of electronic documents to prove this alleged fact. Facing that request, the plaintiff asserted that the documents requested were not reasonably accessible. After consideration, the federal district court concluded that there was not "good cause" to justify a request because the request was not specifically tailored to produce relevant documents.[46]

<18>*Ameriwood Industries, Inc. v. Liberman*, among others, also demonstrates that simply because data fits

within the duty of preservation (i.e., it is electronically stored information that is reasonably related to the litigation), does not mean that its production will be required during discovery. Rather, the policy interests of accessing more types of information due to technological advancement, is balanced by the goal of preventing disproportionate burdens on litigants.[47] *Columbia Pictures v. Bunnell* arose in this unique balancing context.

WHERE COLUMBIA PICTURES INDUSTRIES V. BUNNELL FITS WITHIN THE AMENDED FEDERAL RULES' REALM OF REASONABILITY

<19>In *Columbia Pictures v. Bunnell*, the magistrate judge first addressed whether the data stored in RAM fit within the scope of discovery at all. In other words, whether data stored in RAM constituted relevant evidence that could be discoverable if it qualified as "electronically stored information."[48] The magistrate judge determined that, without question, this data passes the relevancy test because it would identify the instances and culprits of copyright violations.[49] The parties disagreed, however, as to whether RAM fit within the scope of "electronically stored information" and, therefore, could be required to be produced during discovery.[50]

<20>As the court noted, RAM had previously been recognized as a type of storage that could be the basis for *liability*.[51] Although the Ninth Circuit Court of Appeals did not address the discoverability of RAM information in *MAI Systems Corporation v. Peak Computers*, the court of appeals reasoned that because the defendant was able to use software loaded in its computer systems' RAM, such use was considered "copying" the software and, therefore, a violation of the license agreement between the plaintiff and defendant.[52] Since information copied in RAM could be the basis of legal liability, the magistrate court in *Bunnell* reasoned it should also qualify as electronically stored information for the purposes of discovery.[53] Although RAM may be more temporary than other forms of computer memory, the *Bunnell* Court concluded that RAM should also be included as a type of storage appropriate for production during discovery.[54]

<21>In addition to RAM, TorrentSpy and its affiliates also had Web server logs at their disposal.[55] Through the use of its server logs, TorrentSpy could have permanently stored the discoverable data that had been temporarily stored in RAM.[56] It is this "fixing" of the RAM to a more permanent medium that helped bring the information contained in the RAM within the range of being electronically stored information, and subjected it to production.[57]

<22>It is worth noting that requiring the discovery of the server logs themselves was not novel because such logs had already been found discoverable when under control of third parties in *Arista Records LLC v. Does 1-20*.[58] *Arista Records*, like *Bunnell*, involved alleged copyright infringement by Internet users and a motion by the plaintiffs to compel the production of user information on Web server logs.[59] Furthermore, at least one court has previously found that where reports or documents have been destroyed, but could have been recreated through data still in electronic storage, such data is also discoverable.[60]

<23>If TorrentSpy had not been capable of "fixing" the relevant data, the court probably would not have required its preservation or production. Indeed, the court proceeded to distinguish *Bunnell*'s facts from those in *Convolve, Inc. v. Compaq Computer Corp.*, where the District Court for the Southern District of New York held that the loss of certain computer data obtained during routine tuning and re-calibrating of devices was not spoliation.[61] The measurement data at issue in *Convolve, Inc.*, much like RAM, was not permanent unless recorded separately.[62] However, unlike *Bunnell*, the defendant in *Convolve, Inc*. did not have an equivalent server-log system with the capability to permanently store the data.[63]

<24>In weighing these competing forms of data and accessibility, the magistrate court also considered the potential burden placed on the defendants to maintain the data in its Web server logs, and produce it for the plaintiffs. Finding that the cost weighed in favor of the plaintiffs requests, the court held that RAM constituted "electronically stored information" and that it would be reasonable for the defendant to produce RAM during discovery.[64] As such, the defendant was required to produce the records upon a showing of good cause and by court order; however, the court initially declined to order sanctions for not archiving the records in the server logs prior to the order because the defendant could not be faulted for not preserving the data prior to the court order.[65]

<25>Nevertheless, following further discovery by the parties, the district court found that the defendants, in fact, willfully committed spoliation of evidence when it deleted and modified its user forums postings, directory headings, user Internet Provider (IP) addresses, and identities and addresses of its Web site moderators.[66] Concluding that the defendants "engaged in widespread and systematic efforts to destroy evidence and have provided false testimony under oath in an effort to hide evidence of such destruction," the court granted the plaintiffs' motion for sanctions terminating the lawsuit in their favor.[67]

<26>Thus, *Bunnell* demonstrates that courts will consider whether the burden of production outweighs the likelihood of revealing relevant evidence.[68] Had Bunnell convinced the court that the burden of preserving and producing the records was prohibitively high, the court may have limited the production order or required the plaintiff to share in the costs of its production. Regardless, federal courts have established that the costs of preservation and production should not exceed the amount in controversy,[69] and that cost shifting between parties is necessary where justified.[70]

<27>Finally, the court's ruling also highlights the dangers of failing to retain relevant and reasonably accessible data, or destroying such evidence following the commencement of litigation. Although *Bunnell* may be novel in its focus on RAM, after closer scrutiny, the case falls well within the recognized boundaries of the realm of reasonability. Indeed, *Bunnell* fits comfortably within the framework of expanding e-discovery obligations based on the amended rules and recent case law.

GOING WITH THE FLOW: BROADENING THE SCOPE OF DISCOVERABLE EVIDENCE

<28>Historically, the bulk of initial e-discovery issues involved e-mail and other business records on back-up tapes. However, recent case law indicates continued expansion of the type of data and medium of data storage involved in discovery. As demonstrated by court-ordered preservation and production of server logs in *Bunnell*, the development of technology has led to a broader definition of what constitutes "electronically stored information." This expansion includes both standard data, as well as "metadata."[71] Indeed, in recent years, courts have continued to find that metadata "is subject to the duty of preservation and is discoverable,[72] and may require its production through load files or a native format.[73] Metadata's valuable role in authenticating documents and in proving how, when, and where electronic information was created indicates its value to litigation and likely continued use.[74]

<29>In addition, and as was previously noted, data kept on server logs is also discoverable.[75] Files kept in online Web browser cache folders also have been subject to discovery requests when relevant for proving what Web sites were visited by defendants.[76] Even Web server logs containing user information similar to those used by the defendant in *Bunnell* have previously been subject to discovery.[77] Nevertheless, all of these developments are tempered by the requirement of relevancy and standards of reasonable accessibility.

<30>More specifically, the changes made in the 2006 amendments discussed above confirm the significance of reasonable measures in producing electronically stored information. In addition to the two-category model of reasonable accessible and inaccessible data, courts may consider a number of factors before requiring a party to produce data that the party has identified as inaccessible.[78] Although the Rules Committee crafted the amendments to allow for changes in discoverable information,[79] the Rules Committee also made it clear that the standards of reasonability would remain the same. It remains clear that if a requesting party believes that reasonably foreseeable evidence was intentionally destroyed after litigation, a court may sanction the responding party only if there is some proof that the evidence was relevant.[80] However, even before the addition of the "safe harbor" amendment, courts did not penalize defendants for destroying data when acting consistently with their routine destruction policy.[81]

<31>Finally, discovery requests that appear to be "fishing expeditions" continue to be frowned upon by the courts, as they likely do not satisfy the "good cause" requirement for ordering production of burdensome requests.[82] Similarly, courts have established that the duty to preserve generally entails suspending the use of a routine document destruction policy rather than implementing new methods of recording and storing data.[83] Although the scope of discoverable information will continue to broaden as the courts' understanding of electronically stored information expands, e-discovery obligations continue to be tempered by standards of reasonability.

The Importance of a Sound Litigation Hold Procedures and Data Destruction Policies

<32>Providing another valuable lesson for attorneys and their business clients, the court order in *Bunnell* reinforces the importance of reasonable preservation and destruction policies, and a strict adherence to those policies by employees. TorrentSpy and its affiliates had the means to record its user data in its server logs, and were ordered by the court to start preserving this data for production during discovery.[84] TorrentSpy was not penalized for failing to use the logging method prior to litigation, but rather because of a finding of subsequent and intentional spoliation of the evidence that had been ordered preserved.[85]

<33>Furthermore, *Bunnell* provides a reminder of the importance and limitations of the Federal Rules' "safe harbor" provision. As discussed above, the "safe harbor" clause of the 2006 amendments protects the good-faith destruction of primarily temporary electronic information (like that stored in RAM) when done in adherence with an existing destruction policy prior to litigation.[86] Information officers at organizations are just now beginning to appreciate the value of adhering to these policies,[87] and studies show that many executives are now recognizing the need to better understand their company's approach to preservation and destruction.[88] Several Web sites and organizations offer advice on developing policies appropriate to different business models and guidelines for sticking to these policies.[89] Information officers and attorneys alike, however, should take notice that the safe harbor does not protect against destruction of evidence once the duty of preservation has been activated.

CONCLUSION

<34>As technology continues to develop new modes of communication and new ways to create and store information, civil litigation will certainly reflect these changes by making more types of stored information subject to discovery. However, this expansion will still be restrained by the Federal Rules' standards of reasonability. Although *Columbia Pictures Industries v. Bunnell* indicates that a familiar medium of computer memory may now play a greater role in litigation, it should not be construed as requiring new and expensive policies for

preservation and destruction of data. Organizations acting in good faith and with reasonable methods of preservation can continue to do so without fear, at least where there is no anticipation of pending litigation. By developing and sticking to sound data retention policies—and by having effective and fully implemented litigation hold procedures—companies will continue to survive the requirements of e-discovery.

PRACTICE POINTERS

- Evaluate the potential discovery liabilities unique to different business models and the electronic information generated by such business, similar to those unique challenges highlighted by TorrentSpy in *Columbia Pictures Industries v. Bunnell*.
- Develop comprehensive data destruction/preservation policies and educate employees on how these policies are put on hold when litigation becomes reasonably foreseeable.
- Preserve reasonably foreseeable evidence that may be found to be relevant by a court, when litigation has commenced or is reasonably anticipated to begin.
- Reasonably foreseeable evidence may include traditional forms of electronic information such as e-mails and back-ups, but may also include cached files, visit logs and meta-data necessary to authenticate other types of discoverable evidence.
- Review and become familiar with the Federal Rules of Civil Procedure and the various types of data that are now subject to discovery.
- When filing discovery requests, specifically target certain types of discoverable electronic information to ensure disclosure and more efficacious administration of discovery issues by the courts.
- Educate companies and their employees about changes in the law with regard to novel types of electronically discoverable evidence.

<< Top

Footnotes

1. Loren M. Hall, University of Washington School of Law, J.D. program Class of 2009. Thank you to Professor Jane K. Winn of the University of Washington School of Law, and Helen Bergman Moure, Partner of K&L Gates, for their feedback and guidance in developing this Article.
2. Barbara J. Rothstein, Ronald J. Hedges & Elizabeth C. Wiggins, Fed. Judicial Ctr., Managing Discovery of Electronic Information: A Pocket Guide for Judges 2-4 (2007), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf.
3. *See generally* Kenneth J. Withers, *Electronically Stored Information: The December 2006 Amendments to the Federal Rules of Civil Procedure*, 4 Nw. J. Tech. & Intell. Prop. 171 (2006).
4. Columbia Pictures Indus. v. Bunnell (*Bunnell*), No. CV 06-1093FMCSCX, 2007 WL 2080419 (C.D. Cal. May 29, 2007), *motion for rev. denied*, 245 F.R.D. 443, 447-48 (C.D. Cal. Aug. 24, 2007).
5. *Bunnell*, 2007 WL 2080419, at *14. "RAM is a type of computer memory that can be accessed randomly; that is, any byte of memory can be accessed without touching the preceding bytes. RAM is the most common type of memory found in computers and other devices, such as printer . . . . In

common usage, the term RAM is synonymous with main memory, the memory available to programs. For example, a computer with 8M RAM has approximately 8 million bytes of memory that programs can use." Webopedia.com, RAM, http://www.webopedia.com/TERM/R/RAM.html (last visited Feb. 9, 2010).

6. *Bunnell*, 245 F.R.D. at 448. The case concluded in December 2007, when the district court found that the defendant had committed spoliation of evidence and granted the plaintiffs' motion for terminating sanctions. *See* Columbia Pictures, Inc. v. Bunnell, No. 2:06-cv-01093, 2007 WL 4877701 (C.D. Cal. Dec. 13, 2007) (order granting plaintiffs' motion for terminating sanctions).

7. Alan Cohen, *When Rams Talk*, LAW FIRM INC., Sept. 1, 2007, (Magazine) *available at* 2007 WLNR 28023941.

8. Sharon Caffrey, *California Court Orders Preservation of RAM Data*, MONDAQ BUS. BRIEFING, July 3, 2007, *available at* http://www.mondaq.com/unitedstates/article.asp?articleid=49710.

9. Correy E Stephenson, *The Discoverability of RAM Data*, MINNESOTA LAWYER, Aug. 27, 2007 (quoting Corynne McSherry, staff attorney at the Electronic Frontier Foundation in San Francisco, California), *available at* http://www.minnlawyer.com/article.cfm?recid=75604.

10. *See Proposed Amendments to the Federal Rules of Civil Procedure Relating to Discovery*, 48 F.R.D. 487, 527 (1970).

11. Daniel B. Garrie et al., *Electronic Discovery and the Challenge Posed by the Sarbanes-Oxley Act*, 2005 UCLA J. L. & TECH. 2, 3 (2005).

12. *See, e.g.*, Rowe Entm't, Inc. v. William Morris Agency, Inc., 205 F.R.D. 421, 423 (S.D.N.Y. 2002) (developing several factors to balance in determination of which party should bear discovery costs); Zubulake v. UBS Warburg LLC (*Zubulake I*), 217 F.R.D. 309 (S.D.N.Y. 2003) (adapting *Rowe* factors to establish 7-part test for determining which party to bear costs of discovery).

13. *See generally* George L. Paul & Bruce H. Nearon, THE DISCOVERY REVOLUTION: E-DISCOVERY AMENDMENTS TO THE FEDERAL RULES OF CIVIL PROCEDURE (2006).

14. FED. R. CIV. P. 26(b), 33, 34.

15. FED. R. CIV. P. 26(f).

16. FED. R. CIV. P. 26(b)(2).

17. FED. R. CIV. P. 26(b)(5).

18. FED. R. CIV. P. 34(b).

19. *See generally* Lee H. Rosenthal, *A Few Thoughts on Electronic Discovery After December 1, 2006*, 116 YALE L.J. POCKET PART 167 (2006), *available at* http://www.yalelawjournal.org/content/view/82/23/.

20. *Bunnell*, 2007 WL 2080419, at *2. Dot-torrent files are electronic files that utilize the BitTorrent communications protocol to transfer files over peer to peer (p2p) networks. *See generally* Wikipedia.com, BitTorrent (protocol), http://en.wikipedia.org/wiki/BitTorrent_%28protocol%29 (last visited on Feb. 9, 2010).

21. *Bunnell*, 2007 WL 2080419, at *2.

22. *Id.* at *1.

23. *Id.*

24. *Id.*

25. *Id.* at *3. In general, RAM stores data related to programs or processes running on the computer, but does so in a volatile state—meaning that any data stored in RAM will be lost when the computer or device is turned off. Wikipedia.com, RAM, http://en.wikipedia.org/wiki/RAM (last visited Feb. 9, 2010). RAM on computers and other electronic devices stores information only as long as needed to run whatever process that is currently in use by the system, and then allows this data to be rewritten by the next program run on the computer. *Id.* It is this volatile nature of RAM that prompted commentators to question its conclusion as discoverable material. *See, e.g.*, Cohen, *supra* note 7.

26. AAB Joint Venture v. United States, 75 Fed. Cl. 432, 44 (Fed. Cl. 2007); Silvestri v. Gen. Motors Corp., 271 F.3d 583, 590 (4th Cir. 2001).

27. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 217-18 (S.D.N.Y. 2003).

28. *See, e.g.*, Mosaid Techs., Inc. v. Samsung Elecs. Co. Ltd., 348 F. Supp. 2d 337, 339 (D.N.J. 2004); Cache La Poudre Feeds, LLC v. Land O'Lakes, Inc. (*Cache*), 244 F.R.D. 614, 620 (D. Colo. 2007).

29. *Cache*, 244 F.R.D. at 620.

30. *See, e.g.*, Leon v. IDX Sys. Corp., 464 F.3d 951, 959-62 (9th Cir. 2006) (holding that plaintiff's intentional destruction of relevant email records warranted terminating sanctions and substantial fine, and that lesser sanctions would have been futile). *See generally* Shira A. Scheindlin & Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 MICH. TELECOMM. & TECH. L. REV. 71 (2004).

31. FED. R. CIV. P. 37(f).

32. *Bunnell*, 2007 WL 2080419, at *14.

33. Oklahoma *ex rel*. Edmondson v. Tyson Foods, Inc., No. 05-CV-329-GKF-SAJ, 2007 WL 1498973, at *6 (N.D. Okla. May 17, 2007) ("The Court further advises the parties that they should be very cautious in relying upon any 'safe harbor' doctrine as described in new Rule 37(f).").

34. *See* Daniel Renwick Hodgman, Comment, *A Port in the Storm? The Problematic and Shallow Safe Harbor for Electronic Discovery*, 101 NW. U. L. REV. 259, 281 (2007).

35. *See* COMM. ON RULES OF PRACTICE & PROCEDURE, JUDICIAL CONFERENCE OF THE U.S., SUMMARY OF THE REPORT OF THE JUDICIAL CONFERENCE COMMITTEE ON RULES OF PRACTICE AND PROCEDURE 163 (2005), *available at* http://www.uscourts.gov/rules/Reports/ST09-2005.pdf.

36. FED. R. CIV. P. 26(b)(1).

37. FED. R. CIV. P. 26(b)(2)(B).

38. FED. R. EVID. 401. The Rule states that relevant evidence is "evidence having any tendency to make the existence of any fact that is of consequence to the determination of the action more probable or less probable than it would be without the evidence." *Id.*

39. FED. R. CIV. P. 26(b)(1).

40. *Zubulake I*, 217 F.R.D. at 314.
41. *Id.* at 318-20.
42. For a full discussion of the cost-shifting analysis, *see* Mafé Rajul, Comment, *E-Discovery–Can the Producing Party Expect Cost-Shifting?: The New Trend and What Can Be Done to Reduce Production Costs*, 2 SHIDLER J. L. COM. & TECH. 3 (2005), *available at* http://www.lctjournal.washington.edu/Vol2/a003Rajul.html.
43. FED R. CIV. P. 26(b)(2) ("On motion to compel discovery or for a protective order, the party from whom discovery is sought must show that the information is not reasonably accessible because of undue burden or cost. If that showing is made, the court may nonetheless order discovery from such sources if the requesting party shows good cause, considering the limitations of Rule 26(b)(2)(C). The court may specify conditions for the discovery.").
44. *Ameriwood Indus., Inc. v. Liberman*, No. 4:06CV524-DJS, 2007 WL 496716 (E.D. Mo. Feb. 13, 2007).
45. *Id*. at *1.
46. *Id.* at *3.
47. *See* Hodgman, *supra* note 34, at 265.
48. *Bunnell*, 2007 WL 2080419, at *4.
49. *Id.*
50. *Id.* at *4-5.
51. *Id.* at *5 (citing MAI Sys. Corp. v. Peak Computer, 991 F.2d 511 (9th Cir. 1993)).
52. *MAI Sys. Corp.*, 991 F.2d at 518.
53. *Bunnell*, 2007 WL 2080419, at *5.
54. *Id*.
55. *Id.* at *7.
56. *Id.* at *7-8.
57. *Id.* at *5-6.
58. Arista Records LLC v. Does 1-20, No. 05-CV-2144-WDM-PAC, 2005 WL 3776346, at *1-2 (D. Colo. Nov. 7, 2005).
59. *Id.*
60. Burkybile v. Mitsubishi Motors Corp., No. 04 C 4932, 2006 WL 3191541, at *4 (N.D. Ill. Oct. 17, 2006).
61. Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 177 (S.D.N.Y 2004).
62. *Id*. at 177.
63. *Id*. at 168.

64. *Bunnell*, 2007 WL 2080419, at *12.

65. *Id.* at *14.

66. *Bunnell*, 245 F.R.D. at 443.

67. *Id.* at 446.

68. McPeek v. Ashcroft, 202 F.R.D. 31, 34 (D.D.C. 2001) ("[E]conomic considerations have to be pertinent if the court is to remain faithful to its responsibility to prevent 'undue burden or expense'. . . . If the likelihood of finding something was the only criterion, there is a risk that someone will have to spend hundreds of thousands of dollars to produce a single e-mail. That is an awfully expensive needle to justify searching a haystack.").

69. J.C. Assocs. v. Fidelity & Guaranty Ins. Co., No. 01-2437, 2006 WL 1445173, at *2 (D.D.C. May 25, 2006).

70. Mia Mazza et. al, *In Pursuit of FRCP 1: Creative Approaches to Cutting and Shifting the Costs of Discovery of Electronically Stored Information*, 13 RICH. J.L. & TECH. 11 (2007). *See Zubulake I*, 217 F.R.D. at 309; Zubulake v. UBS Warburg LLC (*Zubulake II*), 230 F.R.D. 290 (S.D.N.Y. 2003); Zubulake v. UBS Warburg LLC (*Zubulake III*), 216 F.R.D. 280 (S.D.N.Y. 2003); *Zubulake IV*, 220 F.R.D. at 212; Zubulake v. UBS Warburg LLC (*Zubulake V*), 229 F.R.D. 422 (S.D.N.Y. 2004); Zubulake v. UBS Warburg LLC (*Zubulake VI*), 382 F. Supp. 2d 536 (S.D.N.Y. 2005).

71. Metadata is literally "data about data" that gives details about electronic documents.

72. *See, e.g., In re* Telxon Corp. Sec. Litig., No. 5:98CV2876, 1:01CV1078, 2004 WL 3192729, at *34-35 (N.D. Ohio July 16, 2004); Williams v. Sprint/United Mgmt. Co., 230 F.R.D. 640, 650 (D. Kan. 2005).

73. *See, e.g.,* Hagenbuch v. 3B6 Sistemi Elettronici Industriali S.R.L., No. 04 C 3109, 2006 WL 665005 (N.D. Ill. Mar. 8, 2006).

74. *See generally* Philip J. Favro, *A New Frontier in Electronic Discovery: Preserving and Obtaining Metadata*, 13 B.U. J. SCI. & TECH. L. 1 (2007).

75. Creative Sci. Sys., Inc. v. Forex Cap. Mkts., LLC, No. C 04-03746 JF, 2006 WL 870973, at *1 (N.D. Cal. Apr. 4, 2006) (finding spoliation for party's reconfiguration of servers containing record of software installation since court had issued an order to preserve "all electronic evidence or evidence stored on computers regardless of the medium on which it is stored").

76. Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 645-46 (E.D. Pa. 2007) (finding spoliation of evidence when the defendant law firm automatically destroyed cache files because the defendant did not purposefully destroy the files and would not reasonably know that the files were relevant to the suit for public displays of copyrighted images).

77. Arista Records LLC v. Does 1-20, No. 05-CV-2144-WDM-PAC, 2005 WL 3776346, at *1 (D. Colo. Nov. 7, 2005) (granting plaintiff's request for discovery of defendant's identities from their Internet Service Provider because plaintiff showed good cause that such subscriber activity logs would soon be destroyed if the court did not order preservation).

78. FED. R. CIV. P. 26(b)(2)(C) advisory committee's note ("Considerations may include: (i) the specificity of the discovery request; (ii) the quantity of information available from other and more easily accessed sources; (iii) the failure to produce relevant information that seems likely to have existed

but is no longer available on more easily accessed sources; (iv) the likelihood of finding relevant, responsive information that cannot be obtained from other, more easily accessed sources; (v) predictions as to the importance and usefulness of the further information; (vi) the importance of the issues at stake in the litigation; and (vii) the parties' resources.").

79. FED. R. CIV. P. 34 advisory committee's note.

80. Crandall v. City & County of Denver, Colorado, No. 05-cv-00242-MSK-MEH, 2006 WL 2683754, at *2-3 (D. Colo. Sept. 19, 2006) (ruling that plaintiff had the burden to show that the destroyed e-mails contained relevant evidence where defendant's e-mail destruction policy continued after the toxic tort litigation commenced).

81. *See, e.g.*, Frye v. St. Thomas Health Servs., No. 03C1466, 2005 WL 5417507 (Tenn. Cir. Ct. May 31, 2005) (denying motion for sanctions for spoliation of evidence where defendant found to have complied with its own preservation policy).

82. Balfour Beatty Rail, Inc. v. Vaccarello, No. 3:06-cv-551-J-20MCR, 2007 WL 169628, at *3 (M.D. Fla. Jan. 18, 2007) (plaintiff's request to search defendant's hard drives without specific mention of what they would search for constituted a "fishing expedition.").

83. Doe v. Norwalk Cmty. Coll., No. 3:04-CV-1976, 2007 WL 2066497, at *2-4 (D. Conn. July 16, 2007) (citing *Zubulake I*, 220 F.R.D. at 218).

84. *Bunnell*, 2007 WL 2080419, at *13.

85. *Bunnell*, 245 F.R.D. at 446.

86. FED. R. CIV. P. 37(f).

87. Cory Levine, *Deliberating on E-discovery and the Changes to the FRCP*, FINANCETECH, Feb. 13, 2007, http://www.financetech.com/focus/regulatorycompliance/showArticle.jhtml;jsessionid=4QSDVL1ZKKYRYQSNDLPSKH0CJUNN2JVN?articleID=197005766 ("'Variation will kill you in an operation like ours, and we only operate one way. We endeavor to be repeatable every time the same way so there's very little variation,' said John Ritter, VP of information security for Bank of America (Charlotte, N.C.) at a recent legal-technology conference in New York. 'You have to think about what is your process going to be, and how are you going to follow that practice every single time or as close to every single time as you can.'").

88. Robert McMillan, *Ready to Produce IMs in Court?*, IDG NEWS SERVICE, Jan. 4, 2007, http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9007162&source=rss_topic54.

89. *See, e.g.*, K&L Gates, Electronic Discovery Law, http://www.ediscoverylaw.com/ (last visited Feb. 9, 2010) (online database and blog discussing legal issues and best practices relating to e-discovery); Discovery Resources, http://www.discoveryresources.org/ (last visited Feb. 9, 2010) (archive of e-discovery news and editorial articles).