

# **The New Face of Electronic Discovery: Amendments to the Federal Rules of Civil Procedure May Tame Electronic Discovery's Wild West**

By Aaron L. Walter

*This is the original version of the article, which was awarded second place honors in the Third Annual Law Student Writing Contest of the American Bar Association Tort Trial & Insurance Practice Section. Please note a modified version was published in the Advocate.*

## I. Introduction

Electronic discovery refers to the requesting and acquiring of digitally based documents during pre-trial discovery. Since the 1970 amendment to Federal Rule of Civil Procedure 34, courts have uniformly held that computerized data may be subject to discovery rules.<sup>1</sup> Though discovery rules are clearly applicable to electronic discovery, no one can agree on what to call the field. It has been referred to by courts, commentators, and practitioners as “ED” (electronic discovery), “EDD” (electronic data discovery), digital discovery, e-discovery (with or without a hyphen), and as I simply describe it – electronic discovery. While electronic discovery is not a new phenomenon for some practitioners and private discovery firms, it is cutting edge enough that there is not even a standard name for the legal genre.

---

<sup>1</sup> M. Dorvee and Kristen R. Connor, Electronic Discovery in Technology Litigation, 20 No. 11 Computer & Internet Law. 11 (2003) (citing *Bills v. Kennecott Corp.*, 108 F.R.D. 459, 461 (D. Utah 1995)); *Rowe Entm't, Inc. v William Morris Agency, Inc.* (S.D.N.Y. 2002) (“electronic documents are no less subject to disclosure than paper records”).

Recent court decisions reveal the need for standard rules within the federal courts for dealing with electronic discovery. Amendments to the Federal Rules of Civil Procedure to deal with the issue have been proposed and it is expected that there will be vigorous public debate as to the final structure of any amendment or whether the Rules should be amended at all.

Plaintiff's attorneys, led by the American Trial Lawyers Association (ATLA), argue that there is no need for adding special amendments to the Federal Rules of Civil Procedure. They argue that information is information and that Rules governing paper discovery are equally applicable to the electronic variety. Plaintiff's attorneys are likely candidates for placing initial discovery requests for electronic documents. It is understandable that they would not want special rules to develop that might hinder their ability to access these documents or increase the costs of such actions. However, their stance flies in the face of the many fundamental differences between printed and electronic information; between traditional business methods and the modern world of technology.

Many large corporations, insurance providers, and defense attorneys endorse the development of special rules and guidelines pertaining to electronic discovery. Most importantly, they would like safe harbors which would allow for the regular destruction of electronic documents during the normal course of business and a shifting of costs back to the requesting party if recovery were too costly. This would effectively deny many plaintiffs access to potentially pertinent information. Alternatively, it may shift a great financial burden to requesting parties should they want access to certain electronic records.

The better policy is to provide for new rules which acknowledge the fundamental differences between electronic documents and paper documents and provide specific guidelines as to how

they should be handled. This would ensure that the courts are not left to make ad-hoc decisions or adopt competing tests to make important determinations.

The proposed amendments to the Federal Rules of Civil Procedure represent an important realization that electronic discovery is different and that it needs special rules and standards to guide attorneys, parties, and judges through its pitfalls. While some provisions of the amendments are wise and require little change, others may need to be re-thought so that this ball that is rolling towards a very important finish line creates rules that solve problems, and does not create new ones.

## II. Background

### a. Usage of electronic data

To understand why electronic discovery has become such an invaluable part of litigation, it is important to understand the scope of electronic document usage in the United States.

The volume of potential electronic evidence continues to rise each year and e-mail usage is beginning to replace many traditional phone conversations.<sup>2</sup> Use of e-mail in the business setting has grown immensely in the past ten years, and is now a primary form of business communication.<sup>3</sup> Estimates have placed the total number of e-mails sent each day at 31 billion.<sup>4</sup> By 2005 more than 17.5 trillion electronic documents may be created each year.<sup>5</sup>

---

<sup>2</sup> Hon. Shira A. Sheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. Rev. 327, 328 (2000).

<sup>3</sup> Linda M. Watson, *Anticipating Electronic Discovery in Commercial Cases*, 93-May Mich. B. J. 31, 31 (2004) (citing Patricia Nieuwenhuizen, *E-mail: The Smoking Gun of the Future*, *The National Law Journal*, December 11, 2000) (In the year 2000, office workers exchanged an estimated 25 billion e-mail messages per day).

Another study estimates that 93% of actual documents currently generated are in electronic form, and that only 30% of those documents are ever produced in hard copy.<sup>6</sup> Instead of being converted to paper, an estimated 70% of these electronic documents are being created, revised, modified, and stored entirely in electronic form.<sup>7</sup> Documents that do make it to paper are most often printed from a computer, which means the information exists in electronic form as well as paper.<sup>8</sup>

The ability of modern technology to store huge amounts of digital information has created discovery dilemmas. Possibly the most critical issue is that as the volume of evidence a party wishes to discover grows, so grows the costs inherent to its discovery.

While there is of yet no uniform list of the many types of electronic information subject to discovery, numerous types of information can and have been considered.

---

<sup>4</sup> Lynn Jokela, Comment: Electronic Discovery Disputes: Will the Eighth Circuit Courts Move Beyond Ad-Hoc Decision Making?, 30 Wm. Mitchell L. Rev. 1031, 1031 (2004) (citing Wired media (Dec. 27, 2002), available at [http://www.wiredledia.co.uk/news\\_full.asp?IDW297](http://www.wiredledia.co.uk/news_full.asp?IDW297) (last visited Oct. 26, 2004)).

<sup>5</sup> Jokela, *Supra* note 2, at 1031 (citing Ronald Raether, E-Mail Maelstrom, 13 Bus. L. Today 57, 57 (Sept./Oct. 2003)).

<sup>6</sup> Ricahrd E. Best, Why Discover Electronic Data?, available at [http://californiadiscovery.findlaw.com/why\\_electronic\\_discovery.htm](http://californiadiscovery.findlaw.com/why_electronic_discovery.htm) (last visited Oct 26, 2004).

<sup>7</sup> John L. Carroll, Developments in the Law of Electronic Discovery, 27 Am. J. Trial Advoc. 357, 357 (2003). (citing Michael R. Arkfield, The Wired Lawyer: Electronic Discovery Here to Stay, Az. Att'y 8 (July-Aug. 2002)).

<sup>8</sup> Peter Lyman and Hal. R. Varian, Executive Summary, How Much Information, 2003 at <http://www.sims.berkeley.edu/research/projects/how-much-info-2003/execsum.htm> (last visited Oct. 26, 2004)

First among these are user created electronic documents. This category includes documents created by a computer user, including word processing documents like those made in Word® or WordPerfect®, spreadsheets, and presentations.<sup>9</sup>

A second category is e-mail, which unlike interaction via telephone, creates a discoverable record. E-mail is easily distributed to any number of recipients and is stored on both the sender's and the recipient's computers.<sup>10</sup>

The next category is information that is hidden. This is information that is often created and maintained on a computer that was not intentionally created by the user but was automatically created or modified by the computer itself.<sup>11</sup> The most pertinent of these hidden data are meta-data.<sup>12</sup> These contain information in documents that are unavailable when one looks only at the hardcopy of the document.<sup>13</sup> Meta-data provides information like the date, time, and person(s) accessing a document or a network, the edit history of a document, the existence of previous and subsequent e-mails in a chain of e-mails, and hidden comments that can explain changes in documents or authenticate them.<sup>14</sup> Learning this information can help determine the timing of

---

<sup>9</sup> Stephen D. Willinger and Robin M. Wilson, Negotiating the Minefields of Electronic Discovery, 10 Rich. J.L. & Tech. 52, 28 (2004).

<sup>10</sup> Michael Traynor & Lori Ploeger, Hot Topics in Electronic Discovery, 712 Practicing L. Inst. Pat., Copyrights, Trademarks & Literary Prop. 51, 57 (2002).

<sup>11</sup> Willinger, *supra*, note 11 at 28.

<sup>12</sup> Meta-data is defined as "Data about data. Metadata describes how and when and by whom a particular set of data was collected, and how the data is formatted." Available at <http://www.webopedia.com/TERM/m/metadata.html> (last visited Oct. 26, 2004).

<sup>13</sup> Robert Douglas Brownstone, Collaborative Navigation of the Stormy E-Discovery Seas, 10 Rich. J.L. & Tech. 53, 3 (2004).

<sup>14</sup> Best, *supra*, note 8.

certain revisions of a document, identify recipients of the document, and reveal any indications of document tampering.<sup>15</sup>

The Internet has a number of storage mediums of its own, including web sites, intranets, extranets, cache files, browser history files, site log files, bookmarks, and cookies.<sup>16</sup> Cookies are capable of storing information such as passwords and personal preferences.<sup>17</sup>

Compared to their paper counterparts, these electronic documents are much more difficult to eliminate.<sup>18</sup> Paper documents can be shredded into tiny pieces but deleted electronic documents, especially e-mail, are usually continue to be stored on hard drives or other storage devices.<sup>19</sup>

It is a common misunderstanding that once a user deletes a document from their personal computer that it cannot be recovered by them or anyone else.<sup>20</sup> The reality is that when the user deletes a file, only the indexing for the file is removed, leaving the file itself until it is overwritten or a software program is used to cleanse the drive of these files.<sup>21</sup> Since 90% or

---

<sup>15</sup> Brownstone, *supra* note 16 at 3.

<sup>16</sup> Merilee S. Chan, Paper Piles to Computer Files: A Federal Approach to Electronic Records Retention and Management, 44 Santa Clara L. Rev. 805 (2004).

<sup>17</sup> The term “cookie” comes from a virus like program from the 1980s that would require a computer user to type the word cookie to continue using the computer. See C.D. Taveres, Origin of the Cookie Monster, available at <http://www.multicians.org/cookie.html> (last visited Oct. 26, 2004).

<sup>18</sup> Jokela, *supra* note 3.

<sup>19</sup> Alex Salkever, Hot on the E-Trail of Evidence at Enron, <http://www.apfn.org/enron/e-trail.htm> (last visited Oct 26, 2004) (explaining how in the Enron debacle, documents that were shredded by Arthur Anderson employees were recovered in digital form anyway).

<sup>20</sup> Jokela, *supra* note 3.

<sup>21</sup> M. Dorvee and Kristen R. Conner, Electronic Discovery in Technology Litigation, 20 No. 11 Computer & Internet Law. 11, 12 (2003).

more of business documents are created in digital form,<sup>22</sup> it becomes quite likely that even shredded paper documents have digital counterparts waiting to be discovered.<sup>23</sup> Many corporate electronic systems employ a scheduled backup system which duplicates information to backup tape drives, where the documents will likely be retained until the corporate schedule calls for their erasure.<sup>24</sup>

Unlike paper records, electronic documents are often dynamic and cannot simply be secured at the onset of litigation.<sup>25</sup> These records may be continuously modified or even deleted subject to routine destruction policies businesses may have in place.<sup>26</sup> While paper documents subject to discovery are often found in filing cabinets or boxes, electronic documents could exist in any number of environments and mediums.<sup>27</sup> Numerous copies of the very same document can end up in many different places within a company's umbrella.<sup>28</sup>

One major hurdle to developing and following any rules for electronic discovery is that many attorneys and their clients simply do not understand its implications.<sup>29</sup> In a 2000 survey of attorneys, 98% believed the use of technology in discovery would increase.<sup>30</sup> However, 83%

---

<sup>22</sup> Lyman, *supra*, note 8.

<sup>23</sup> Jokela, *supra* note 3.

<sup>24</sup> Chan, *supra* note 19 at 814.

<sup>25</sup> Steven C. Bennett, E-Discovery by Keyword Search, 15 NO. 3 Prac. Litigator 7, 8 (2004).

<sup>26</sup> *Id.*

<sup>27</sup> Best, *supra* note 10.

<sup>28</sup> Dorvee, *supra* note 25 at 12.

<sup>29</sup> Todd L. Krause and Brian D. Coggio, Electronic Discovery: Where We Are and Where We're Headed, 16 No.3 J. Proprietary Rts. 16 (2004) (citing May 2000 survey by PriceWaterhouseCoopers and the American Bar Association's Litigation Section).

<sup>30</sup> *Id.*

said that their clients' IT departments had no established protocol for dealing with electronic discovery requests.<sup>31</sup> 68% of those surveyed said their clients rarely, if ever, took steps to prevent automatic overwriting processes of their electronic data.<sup>32</sup>

More recent surveys have shown progress, but still expose problems. In a 2003 survey, attorneys revealed that 39% of their litigation involved electronic discovery.<sup>33</sup> However, nearly half of those participating answered that they stood somewhere between "not confident" and "neutral" in their confidence in their firm's ability to effectively manage electronic discovery in civil litigation.<sup>34</sup> Less than 14% answered that they were "very confident" in their firm's abilities to manage electronic discovery.<sup>35</sup> In a 2004 edition of the survey, nearly 90% of the attorneys responding said that attorneys in general do not grasp the implications of the size of data sets involved in large electronic discovery projects.<sup>36</sup> Another research study found that only 25% of AmLaw200<sup>37</sup> firms have the requisite knowledge and expertise to professionally handle a complex electronic discovery matter.<sup>38</sup>

---

<sup>31</sup> *Id.*

<sup>32</sup> Krause, *supra* note 41.

<sup>33</sup> Forensics Consulting Solutions, LLC, 2003 eDiscovery in Civil Litigation Survey, available at <http://www.ediscoverysurvey.com/edd1/edd1main.htm> (last visited Nov. 1, 2004).

<sup>34</sup> *Id.*

<sup>35</sup> *Id.*

<sup>36</sup> Forensics Consulting Solutions, LLC, 2004 Litigation Support Survey, available at <http://www.ediscoverysurvey.com/lsm1/lsm1main.htm> (last visited Nov. 1, 2004).

<sup>37</sup> AmLaw 200 is a ranking of America's largest 200 law firms, compiled yearly by American Lawyer Media.

<sup>38</sup> PR Newswire, E-Discovery Execs Name Top EDD Law Firms; 75% of AmLaw 200 Not Qualified to Handle Complex EDD Matters, available at

In some jurisdictions, attorneys may be running out of excuses. As one commentator notes, the State of New Jersey is one of several implementing local rules pertaining to electronic discovery.<sup>39</sup> The New Jersey rules place specific requirements on an attorney to acquaint themselves with records, including electronic, maintained by the client.<sup>40</sup> As noted by the commentator, “it may no longer be sufficient for counsel to plead they are computer challenged.”<sup>41</sup>

Many attorneys who are skilled in the ways of electronic discovery hope to use it to find the “silver bullet” which could win a case or force an opponent’s hand in settlement. Increasingly, e-mails are providing crucial pieces of evidence for litigators.<sup>42</sup> In one case, computer forensics engineers were able to recover an e-mail from one company employee to another discussing the side effects of the drug “Fen-phen.”<sup>43</sup> The rather tasteless e-mail reportedly read “Do I have to look forward to spending my waning years writing checks to fat people worried about a silly lung problem?”<sup>44</sup> The estimated \$3.7 billion settlement reached in this case was among the largest ever against a U.S. company.<sup>45</sup>

---

<http://www.prnewswire.com/cgi-bin/stories.pl?ACCT=109&STORY=/www/story/09-30-2004/0002262333&EDATE=> (last visited Nov. 1, 2004).

<sup>39</sup> Dennis F. Gleason, Will That Be Paper or Digital? A Basic Understanding Electronic Discovery, 226-Feb. N.J. Law 40, 43 (2004).

<sup>40</sup> *Id.*

<sup>41</sup> *Id.*

<sup>42</sup> Jokela, *supra* note 3 at 1033-1034.

<sup>43</sup> Brownstone, *supra* note 18 at 17 (citing Linnen v. A.H. Robins Co., 10 Mass. L. Rep. 189, 1999 Mass. Super. LEXIS 240 (Mass. Super. Ct. June 15,1999)).

<sup>44</sup> *Id.*

<sup>45</sup> CNN, Fen-phen maker agrees to \$3.75 billion settlement, available at

In a similar instance, Chevron Corp. paid \$2.2 million to settle a sexual harassment case brought by employees based on discovered e-mail evidence which included one e-mail titled "25 reasons beer is better than women."<sup>46</sup> Cases such as these encourage other attorneys to utilize electronic discovery to find information which would otherwise have remained hidden.<sup>47</sup> These cases are also an example of how the spontaneity of e-mail can cause persons to be more cavalier with the content of an e-mail than they would with a written or printed memo.<sup>48</sup> Many employees see e-mail as a replacement for a phone call, not for written correspondence.<sup>49</sup> Therefore, e-mail is commonly used rather casually and conversationally. Many e-mail users are under the mistaken belief that their messages will be deleted or remain undiscovered.<sup>50</sup> This all too often leads to a pleasantly surprised requesting party who discovers candid statements that would never have been made on paper.<sup>51</sup>

#### b. Emerging Trends – Discovery of Voicemail and Instant Messages

---

<http://www.cnn.com/HEALTH/diet.fitness/9910/08/fen.phen/> (last visited Oct. 26, 2004).

<sup>46</sup> Brownstone, *supra* note 3 at 17; *See* MSNBC, Porn Problem at Work Persists, available at

<http://msnbc.msn.com/id/5899345/> (adding that 13 percent of companies have faced a lawsuit based on employee e-mail) (last visited Oct. 26, 2004).

<sup>47</sup> Brownstone, *supra* note 3 at 17.

<sup>48</sup> Dorvee, *supra* note 1 at 11.

<sup>49</sup> *Id.*; *See In re Amendments to Rule of Judicial Admin. 2.051 - Pub. Access to Judicial Records*, 651 So. 2d 1185, 1186 (Fla. 1995) (“E-mail transmissions are quickly becoming a substitute for telephonic and printed communications, as well as a substitute for direct oral communications.”)

<sup>50</sup> Watson, *supra* note 4 at 31; *See* Yolanda M. Sanders, Electronic Discovery and Evidence: Safeguarding Against Misuse of Technology in the Workplace, 1 (no. 7) Lab. & Employment Bull., 369, 370 (July 1, 2001).

<sup>51</sup> *Id.*

In recent years, the scope of electronic discovery has expanded from discovery of e-mail and electronic forms of traditional business documents to the more informal realms of digitized voicemail and instant messaging programs.

Twenty years ago voicemail was something of a novelty. Today it is a standard element of business communications.<sup>52</sup> Voicemail, an electronically preserved medium, is open to similar standards of discovery as e-mail.<sup>53</sup> However, elements of these two technologies are not necessarily equivalent. Voicemail is typically deleted after a certain amount of time, either by the user or through automated deletion.<sup>54</sup> Voicemails are typically retained only for a matter of days and deleted voicemails are much more difficult to recover compared to deleted e-mails.<sup>55</sup>

For voicemails that are recovered through discovery there are factors that make the process of reviewing records more difficult.<sup>56</sup> First, while there are different methods to retain e-mail records, including tape backups, files available on business networks, and backups or sent copies still available on the originating computer(s), voicemail messages will generally need to be recovered from the message recipient's account.<sup>57</sup> This means likely recipients must first be identified (they may in fact be unknown). This pool of voicemail recipients could be quite large, which may require a responding party to cast a wide (and thereby expensive) net to preserve

---

<sup>52</sup> Steven C. Bennett, Voicemail: The Latest Front in the E-Discovery Wars, 11/4/2002 N.Y.L.J. S4 (col. 1) (2002).

<sup>53</sup> Dorvee, *supra*, note 1 at 11.

<sup>54</sup> Paul D. Boynton, Voicemail Poised To Become The Next Target Of E-Discovery, Lawyers Weekly USA (July, 2003), available at <http://www.lexisone.com/news/nlibrary/lw070003z.html> (last visited Nov. 1, 2004).

<sup>55</sup> *Id.*

<sup>56</sup> Bennett, *supra* note 77.

<sup>57</sup> *Id.*

these records, and may require an equally wide net on the part of the requesting party to ensure that all relevant voicemail messages are actually obtained.<sup>58</sup>

Unlike with e-mail, no clever methods of searching thousands of voicemail records for specific information exist.<sup>59</sup> While e-mails are text based records, voicemails are sound based records. There are no “TO” or “FROM” lines to review and there is no subject line from which to immediately determine the general nature of the communication. Unless the voicemail messages are transcribed into text form, one must actually listen to every minute of them. Depending on the volume of voicemail requested, this could take hours or hundreds of hours just to determine if any useful information can be gained from them.<sup>60</sup> Completion of either transcription or listening to a large volume of messages may be cost prohibitive due to the current lack of accepted automated voicemail search and transcription technologies.<sup>61</sup>

Despite the costs, the actual sounds of the message may be critical in understanding what was being conveyed.<sup>62</sup> A transcript cannot capture tone, emphasis, and other subtle clues provided by actual speech.<sup>63</sup> Voicemail evidence therefore has the potential to be powerful and damning evidence.<sup>64</sup> Ill-considered e-mail messages can clearly become a smoking gun, but actual voice evidence or an admission has the potential to be even more damning because of the nature of the

---

<sup>58</sup> *Id.*

<sup>59</sup> Bennett, *supra* note 77.

<sup>60</sup> *Id.*

<sup>61</sup> Boyton, *supra* note 79; Bennett, *supra* note 77.

<sup>62</sup> Bennett, *supra* note 77.

<sup>63</sup> *Id.*

<sup>64</sup> *Id.*

medium.<sup>65</sup> Advancements in technology are adding to this power as well. Archiving technology can now add date and time stamps, recipient and sender telephone numbers, and identification of actions taken such as retain, forward, or delete.<sup>66</sup> This allows voicemail to not only contain the voice and words of a person, but also help create a timeline.<sup>67</sup> Soon, increasing capacities of storage for voicemail systems may make it possible for all voicemail messages to be retained.<sup>68</sup>

Instant messaging, another emerging technological trend, appears to be quickly separating itself from the perception of being intended for personal communications among young people. A study has shown that 90% of Internet users between the ages of 13 and 21 use one variety of instant messaging service or another.<sup>69</sup> The research also showed though that four in ten adult internet users in the United States use instant messaging software and one in five instant messenger users send instant messages at work.<sup>70</sup> Some analysts have predicted that instant messaging soon will overtake e-mail as the No. 1 form of electronic communication.<sup>71</sup>

---

<sup>65</sup> Bennett, *supra* note 77 (citing United States v. Smith, 15 F. 3d 1051 (9<sup>th</sup> Cir. 1998) (in an insider trading case a voicemail provided to prosecutors revealed that the defendant had announced his stock trading intentions and awareness of insider information)).

<sup>66</sup> Boyton, *supra* note 79.

<sup>67</sup> *Id.*

<sup>68</sup> Bennett, *supra* note 77 (stating that the only real constraint is the willingness of the business to dedicate storage capacity and the resources of computer professionals to the problem).

<sup>69</sup> Leslie Walker, Instant messaging is growing up, The Washington Post (Sept. 2004) available at <http://msnbc.msn.com/id/5898217/print/1/displaymode/1098/> (last visited Nov. 1, 2004) (citing Pew Internet & American Life Project survey) (usage among ages 22 to 34 was 71%, from 35 to 54 was 55%, and was 48% for those 55 or older).

<sup>70</sup> *Id.*

<sup>71</sup> *Id.*

In modern-day business, the tool of instant messaging can be of great value.<sup>72</sup> Instant messaging has the ability to link individuals anywhere around the world in a free and instant conversation.<sup>73</sup> Employers consider instant messaging a mixed blessing.<sup>74</sup> Instant messaging can boost productivity, but also has the potential to enable idle gossip and chatter.<sup>75</sup>

There are also far more substantial risks to employee use of instant messaging than loss of productivity.<sup>76</sup> These powerful communications tools may allow an employee to “divulge corporate secrets, risk corporate liability through unregulated conversations<sup>77</sup>, and permit users to send company files and documents right under the employer’s nose.”<sup>78</sup>

This technology presents a potential goldmine of discoverable and damaging evidence.<sup>79</sup> While some employees have become aware of high profile e-mail “smoking gun” cases, instant messaging remains an area of less careful speech.<sup>80</sup> The candid, free-form nature of instant

---

<sup>72</sup> Adam Rubinger and Dean Gonsowski, Instant Messaging: New E-Discovery Frontier?, *Digital Discovery & e-Evidence*, Vol. 4, No. 6 (June 2004).

<sup>73</sup> *Id.*

<sup>74</sup> Walker, *supra* note 99 (citing Pew Internet & American Life Project survey finding that 68% of those surveyed saw more positives than negatives).

<sup>75</sup> *Id.*

<sup>76</sup> Rubinger, *supra* note 102 at 1.

<sup>77</sup> The ePolicy Institute 2004 Workplace E-mail and Instant Messaging Survey, available at <http://www.epolicyinstitute.com/survey/survey04.pdf> (finding that only 11% of employees answered that their company monitors instant messages, with 60% stating that their company does not, leaving nearly 30% unsure of their company’s monitoring capabilities for instant messaging).

<sup>78</sup> Rubinger, *supra* note 102 at 1.

<sup>79</sup> Rubinger, *supra* note 102 at 1.

<sup>80</sup> *Id.*

messaging, along with the perception that these communications are seldom monitored, leads some people to incorrectly assume that all messages disappear after the instant messenger window disappears.<sup>81</sup>

Discovery and review of instant messages presents a similar challenge as that of voicemail messages. One survey indicated that only 11% of employers have some sort of instant message management software in place that would be capable of archiving instant messages.<sup>82</sup> In addition, if a log of messages does exist they may be in unstructured lists of messages.<sup>83</sup> In some cases, the log file will be a long list of messages to and from individual users with no breaks between the messages.<sup>84</sup>

Adding to the difficulty of reviewing these logs are issues of “context.”<sup>85</sup> A new language<sup>86</sup> has emerged among instant messaging users intended to abbreviate or create acronyms for commonly used words to communicate the greatest amount of information in the fewest possible keystrokes.<sup>87</sup> This adds to the difficulty of actually searching through the text when some of the text must be translated and the context of the conversation may be quite vague.<sup>88</sup>

---

<sup>81</sup> Rubinger, *supra* note 102 at 1.

<sup>82</sup> The ePolicy Institute 2004 Workplace E-mail and Instant Messaging Survey, (The question being - Does your organization use IM gateway/management software technology to monitor, purge, retain, archive, and otherwise manage/control IM risks and use?, 11.1% answered Yes, 60% answered No, and 28.4% were unsure).

<sup>83</sup> *Id.*

<sup>84</sup> *Id.*

<sup>85</sup> Rubinger, *supra* note 102 at 3.

<sup>86</sup> Web Slang, lingo, and acronyms used in chat rooms, Instant Messages, and Text Messaging, available at <http://www.web-friend.com/help/lingo/chatslang.html> (last visited Nov. 1, 2004).

<sup>87</sup> Rubinger, *supra* note 102 at 3 (citing Katie Dean, The Language of IM, Wired News (Jan. 25, 2000) available at [http://www.wired.com/news/culture/0,1284,33821,00.html?tw=wn\\_story\\_related](http://www.wired.com/news/culture/0,1284,33821,00.html?tw=wn_story_related) (last visited Nov. 1, 2004).

### c. Rules Governing Electronic Discovery

#### 1. Federal Rules of Civil Procedure

While of the scope of potentially discoverable evidence expands with technology, the rules governing the discovery of electronic evidence in the federal courts, the Federal Rules of Civil Procedure (FRCP), have remained still. As one commentator put it, “when it comes to electronic evidence, it seems that the law changes slowly or not at all.”<sup>89</sup> To this day, electronic evidence is subjected to rules that were created to solve problems associated with paperbound discovery.<sup>90</sup>

One of the main purposes of the Federal Rules of Civil Procedure is to promote efficiency.<sup>91</sup> With this underlying intent of promoting efficiency in mind I turn our attention towards Rules 26 and 34 of the Federal Rules of Civil Procedure which govern the discovery of electronic media.<sup>92</sup> FRCP Rule 26 provides for initial disclosures of “all documents, data compilations, and tangible things” that the disclosing party may use to support its claims or defenses.<sup>93</sup> FRCP Rule 34 goes on to broadly define “documents” as including electronic data.<sup>94</sup>

---

<sup>88</sup> *Id.*

<sup>89</sup> William C. Gleisner III, *Electronic Evidence in the 21st Century*, 77 *Wis. Law* 11, 11 (2004).

<sup>90</sup> *Id.*

<sup>91</sup> *See* Fed. R. Civ. P. 1 (“[These rules] shall be construed and administered to secure the just, speedy, and inexpensive determination of every action.”)

<sup>92</sup> *See* Fed. R. Civ. P. 26; Fed R. Civ. P. 34.

<sup>93</sup> Watson, *supra* note 4 at 2; Fed. R. Civ. P. 26(a).

<sup>94</sup> Watson, *supra*\_note 4 at 2; Fed. R. Civ. P. 34.

FRCP Rule 34 was amended in 1970 in recognition of the need to include information in electronic form within the scope of the rules governing discovery.<sup>95</sup> It was amended to provide that, upon request, a party is required to produce “any designated documents,” including “writings, drawings, graphs, charts, photographs, phonorecords, and other data compilations from which information can be obtained.”<sup>96</sup> The original version of FRCP Rule 34(a) only permitted a party to request production of “documents” or “tangible things.”<sup>97</sup> The 1970 amendment adjusted the definition of “documents” to include a wide description of electronic data to adequately reflect the changes in technology.<sup>98</sup> While not specifically naming “computer data,” it makes it clear that FRCP Rule 34 now applies to electronic data compilations from which information can only be obtained with the use of detection devices.<sup>99</sup> FRCP Rule 34 does not address issues related to the manner in which information is to be disclosed.<sup>100</sup>

In continuation of FRCP Rule 1’s policy of promoting efficiency, FRCP Rule 26 protects parties from unduly burdensome, unnecessary, or inefficient discovery.<sup>101</sup> While the literal

---

<sup>95</sup> See Willinger, *supra* note 13 at 7; Fed. R. Civ. P. 34 advisory committee note.

<sup>96</sup> Willinger, *supra* note 13 at 7; Fed. Civ. P. 34.

<sup>97</sup> Jokela, *supra* note 3 at 1034 (citing 8A Charles Alan Wright et al, Federal Practice and Procedure: Federal Rules of Civil Procedure §2218, at 450 (2d ed. 1994)).

<sup>98</sup> Jokela, *supra* note 3 at 1034; Fed. R. Civ. P. 34 advisory committee note.

<sup>99</sup> See The Sedona Principles: Best Practices, Recommendations & Principles for Addressing Electronic Document Production, 5 Sedona Conf. J. 151, 152 (2004) (citing *Anti-Monopoly, Inc. v. Hasbro, Inc.*, No. 94 Civ. 2120, 1995 WL 649934, at \*2 (S.D.N.Y. Nov. 3, 1995) (“Thus, it is now “black letter law that computerized data is discoverable if relevant.”); *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000) (“[C]omputer records ... are documents discoverable under Fed. R. Civ. P. 34.”)).

<sup>100</sup> Jokela, *supra* note 3 at 1034.

<sup>101</sup> The Sedona Principle, *supra* note 140 at 152.

language of FRCP Rule 26 is silent on electronic documents, the advisory notes clarify that disclosures “include computerized data and other electronically-recorded information...”<sup>102</sup> FRCP Rule 26 operates to relieve the burden placed on responding parties by prohibiting cumulative or duplicative discovery requests.<sup>103</sup> However, FRCP Rule 26 does not directly provide us with guidance about how much information a party must actually produce or which party should bear the expenses of a potentially costly electronic discovery request.<sup>104</sup>

## 2. Proposed Amendments to the Federal Rules of Civil Procedure

The U.S. Judicial Conference Committee on Rules of Practice and Procedure has sought to answer the above questions and others in their recent draft of proposed amendments to the Federal Rules of Civil Procedure governing discovery of electronic documents.<sup>105</sup> Published in August of 2004 by a standing committee of the Judicial Conference, the proposed changes would modify FRCP Rules 16 (Pretrial conferences), 26 (General provisions), 33 (Interrogatories), 34 (production of documents), 37 (Sanctions), and 45 (Subpoenas).<sup>106</sup> Some of the proposed changes have near universal support, while others have been publicly criticized.<sup>107</sup> The changes

---

<sup>102</sup> Chan, *supra* note 21 at 812; Fed. R. Civ. P. 26 advisory committee note.

<sup>103</sup> Jokela, *supra* note 3 at 1035.

<sup>104</sup> *Id.* (citing cases where courts have laid down guidelines) *Zubulake v. UBS Warburg, L.L.C.*, 216 F.R.D. 280, 283084 (S.D.N.Y.2003); *Rowe Entm't, Inc. v. William Morris Agency, Inc.*, 205 F.R.D. 421, 429 (S.D.N.Y. 2002).

<sup>105</sup> Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee (May 17, 2004, revised August 3, 2004) available at <http://www.uscourts.gov/rules/comment2005/CVAug04.pdf> (last visited Nov. 1, 2004).

<sup>106</sup> *Id.*

<sup>107</sup> See Alfred W. Cortese, Jr., Development of New Federal “E-Discovery” Rules Advancing, Legal Backgrounder Vol. 18 No. 47 (October 31, 2003); Todd L. Krause and Brian D. Coggio, New Horizons in Patent Litigation: “Discovering” Electronic Information, 10/12/2004 N.Y.L.J. S4 (col. 1) (October 12, 2004).

are intended to focus on five main areas of electronic discovery.<sup>108</sup> First, the proposed changes deal with the need of early attention in potential litigation to electronic discovery issues.<sup>109</sup> Second, they seek to adapt FRCP Rules 33, 34 and 45 to electronic discovery.<sup>110</sup> Third, they provide procedures for asserting privilege after inadvertent production of privileged information.<sup>111</sup> Fourth, they deal with limiting discovery of electronic information that is not reasonably accessible.<sup>112</sup> Lastly, they deal with sanctions against parties for spoliation<sup>113</sup> of electronically stored information.<sup>114</sup>

The proposed amendments to FRCP Rules 16 and 26 would require parties to discuss electronic discovery at their initial conference and deals with elements of a scheduling order.<sup>115</sup> Parties would need to discuss the form in which information should be produced and whether the court needs to enter a protective order over a party's right to assert privilege if privileged

---

<sup>108</sup> Krause, *supra* note 148 at 2; Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>109</sup> *Id.*

<sup>110</sup> *Id.*

<sup>111</sup> *Id.*

<sup>112</sup> *Id.*

<sup>113</sup> The intentional destruction of a document or an alteration of it that destroys its value as evidence. *See* <http://www.hyperdictionary.com/dictionary/spoliation> (last visited Nov. 1, 2004).

<sup>114</sup> Krause, *supra* note 148 at 2; Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>115</sup> Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

information is inadvertently produced.<sup>116</sup> This results in parties discussing potential problems early, and has been widely considered a positive reinforcement of a good practice.<sup>117</sup>

Other proposed rules have been slightly more controversial. Amendments proposed to FRCP Rule 34 would specifically distinguish electronically stored information from the generic term “documents.”<sup>118</sup> The proposed Rule also updates its language to provide explicitly for the production of electronically stored information.<sup>119</sup> The broad definition given to electronic data would avoid any limitations to only existing technologies.<sup>120</sup> The proposed Rule also permits a requesting party to specify the form in which electronically stored information is to be produced but allows the responding party to object to this form.<sup>121</sup> However, the proposed Rule also states that if the particular form of production is not specific, the proposed Rule requires that the responding party produce the data in the manner in which it is ordinarily maintained or in an electronically searchable form.<sup>122</sup> As one commentator notes, this brings up two important

---

<sup>116</sup> *Id.*

<sup>117</sup> *See Cortese, supra* note 148; *The Sedona Principles: Best Practices, supra* note 140 at 162.

<sup>118</sup> Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>119</sup> *Id.*

<sup>120</sup> Proposed Federal Rules On Electronic Discovery Submitted For Public Comment, 187 Products Liability Advisory 4 (September 2004).

<sup>121</sup> Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>122</sup> “If a request for electronically stored information does not specify the form of production, a responding party must produce the information in a form in which it is ordinarily maintained, or in an electronically searchable form. The party need only produce such information in one form.”

issues.<sup>123</sup> First, if the information is ordinarily maintained and is therefore produced in its native<sup>124</sup> form, review by the requesting party may be difficult in that the information may need to be converted into a readable format.<sup>125</sup> Second, parties may be hesitant to produce vast amounts of information in a searchable format because “it could give an opponent the keys to the kingdom.”<sup>126</sup>

The proposed amendments to Rule 26 would create a procedure to assert privilege if privileged information is inadvertently produced.<sup>127</sup> New Rule 26(b)(5) allows a producing party who did not intend to waive privilege may, within a reasonable amount of time, notify the receiving party of the privilege.<sup>128</sup> After notification, the receiving party would then need to promptly “return, sequester, or destroy” the specific information until a court ruling on possible waiver is made.<sup>129</sup> Such an agreement is called a “clawback agreement” which allows for production without an actual waiver of any privileged information contained within.<sup>130</sup> These

---

Proposed Rule 34, Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>123</sup> Krause, *supra* note 148 at 5.

<sup>124</sup> “an application's native file format is the one it uses internally. For all other formats, the application must first convert the file to its native format.” See <http://www.webopedia.com/TERM/n/native.html>.

<sup>125</sup> Krause, *supra* 148 at 5.

<sup>126</sup> *Id.*

<sup>127</sup> Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>128</sup> *Id.*

<sup>129</sup> *Id.*

<sup>130</sup> Richard Acello, New E-Discovery Rules Proposed, ABA Journal E-Report (July 23,2004).

“quick peek” or “clawback” provisions are often stipulated to by individual parties as a practical way to accelerate discovery.<sup>131</sup>

Under the proposed changes to Rule 26(b)(2) a responding party would not need to provide discovery of electronic information that is not “reasonably accessible.”<sup>132</sup> Should the responding party assert this privilege, a court could still order a party to provide the information if the requesting party established “good cause.”<sup>133</sup> The comments to the proposed Rule 26 make it clear that the responding party cannot rely on this provision if they have already accessed the information.<sup>134</sup>

Arguably the most controversial proposed amendment is the new subdivision (f) of Rule 37. The new section provides that “unless a court order requiring preservation of electronically stored information is violated, the court may not impose sanctions under these rules on a party when such information is lost because of the routine operations of its electronic information

---

<sup>131</sup> Richard H. Middleton, The “Complexities” of Electronic Discovery, 5 Sedona Conf. J. 105, 108 (2004).

<sup>132</sup> Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>133</sup> “A party need not provide discovery of electronically stored information that the party identified as not reasonably accessible. On motion by the requesting party, the responding party must show that the information is not reasonably accessible. If that showing is made, the court may order discovery of the information for good cause....” Proposed Rule 26(b)(2), Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>134</sup> “But if the responding party has actually accessed the requested information, it may not rely on this rule as an excuse from providing discovery, even if it incurred substantial expense in accessing the information.” Comments to proposed rule 26(b)(2), Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

system if the party took reasonable steps to preserve discoverable evidence.”<sup>135</sup> The amendment is favored by large corporations, but is a matter of contention for plaintiff’s attorneys.<sup>136</sup>

The changes to the Federal Rules of Civil Procedure will go into effect on December 1, 2006 should they be approved, with or without revisions, by the Standing Committee on Rules of Practice and Procedure, the Judicial Conference, the U.S. Supreme Court, and then Congress.<sup>137</sup>

One of the inherent problems with the procedures of amending Federal Rules is that the amendment process is quite lengthy.<sup>138</sup> Because of constant technological changes it is possible that the amendment could be outdated by the time they are put into effect.<sup>139</sup> This makes it all the more important for the Rules to be inclusive of new technologies while providing a specific framework for existing problems.

#### d. Common Law Principles

It is important to understand the scope of where we are today with electronic discovery. As rulemaking bodies attempt to adapt the Federal Rules of Civil Procedure, these changes or guidelines surround two of the major concerns with electronic discovery. These concerns are: (1) what happens to a party when they found to have improperly disposed of digital evidence? and (2) who needs to pay for all of this?

---

<sup>135</sup> Proposed Rule 37(f), Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>136</sup> Acello, *supra* note 171 (citing comments by Virginia Llewellyn, Vice President of Applied Discovery).

<sup>137</sup> See Federal Rulemaking Process, available at <http://www.uscourts.gov/rules/newrules3.html> (last visited Nov. 10, 2004).

<sup>138</sup> See Acello, *supra* note 171

<sup>139</sup> Id.

## 1. Spoliation

Spoliation has been described in the federal courts as destruction or alternation of evidence, or the failure to properly preserve evidence in pending or reasonably foreseeable litigation.<sup>140</sup>

Spoliation, resulting from the use of electronic evidence is an issue that has not been directly addressed in the Federal Rules of Civil Procedure.<sup>141</sup> As documents become more frequently maintained in electronic form, it has become much easier to delete or alter this evidence and much more difficult for litigants to craft policies that ensure that all relevant documents to reasonably foreseeable litigation are properly preserved.<sup>142</sup>

Despite these difficulties, a party has the duty to protect and preserve evidence once it is on notice that it must do so.<sup>143</sup> This obligation is not new to electronic discovery specifically, but it “takes on new meaning in the context of electronic discovery,” because of its unique qualities.<sup>144</sup> The determination of possible sanctions due to spoliation, if any, is left “to the sound discretion of the trial judge,...assessed on a case-by-case basis.”<sup>145</sup> A court may even impose a sanction if

---

<sup>140</sup> Kevin Schlosser, *Litigation Review: Two Recent Spoliation Rulings Impose Severe Sanctions*, 9/28/2004 N.J.L.J. 16, (col. 1) (Sept. 2004) (citing *Fujitsu Ltd. v. Federal Express Corp.*, 247 F. 3d 423, 436 (2d Cir. 2001).

<sup>141</sup> Jokela, *supra* note 5 at 1048 (citing Hon. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. Rev. 327, 628 (2000) which notes that “although Rule 37(b)(2) authorizes sanction for the failure to permit discovery, this authority under the rules often has been construed as confined a to situation in which the party destroyed evidence following issuance of a discovery order.”)

<sup>142</sup> Watson, *supra*, note 4 at 32.

<sup>143</sup> Gleisner, *supra* note 130 at 55 (citing *Yu Jung Park v. City of Chicago*, 297 F. 3d 606, 616 (7th Cir. 2002).

<sup>144</sup> *Id.*

<sup>145</sup> Schlosser, *supra*, note 189 (citing *Fujitsu Ltd. v. Federal Express Corp.*, 247 F. 3d 423, 436 (2d Cir. 2001).

the destruction occurred through negligence rather than willfulness.<sup>146</sup> Potential sanctions include outright dismissal, adverse inferences, preclusion of certain evidence, and monetary fines.<sup>147</sup>

In an example that one commentator calls “the worst case scenario for electronic discovery problems,” Metropolitan Opera Association v. Local 100, Hotel Employees and Restaurant Employees International Union<sup>148</sup>, a judge awarded summary judgment to the plaintiff on the issue of liability based on the defendant’s repeated failures in discovery.<sup>149</sup>

Unfortunately, examples of spoliation and sanctions for destruction of electronic evidence are all too common.<sup>150</sup> Two recent cases on the subject have received a great deal of attention.<sup>151</sup>

First, in *Zubulake v. UBS Warburg*<sup>152</sup> an instruction of an adverse inference was granted against a company for deleting relevant e-mails during a discovery period which had gone on for

---

<sup>146</sup> *Id.*

<sup>147</sup> *Id.*

<sup>148</sup> *Metropolitan Opera Association v. Local 100, Hotel Employees and Restaurant Employees International Union*, 212 F.R.D. 178 (S.D.N.Y. 2003).

<sup>149</sup> Brian D. Walters, *Best and Worst Practices in Electronic Discovery*, available at [http://www.discoveryresources.org/pdfFiles/01\\_bigPicture\\_bwPractices.pdf](http://www.discoveryresources.org/pdfFiles/01_bigPicture_bwPractices.pdf) (last visited Oct. 26, 2004) (when the plaintiff threatened to get their own experts to examine defendant’s computers, they were replaced without notice).

<sup>150</sup> *See Kucala Enterprises, Ltd. v. Auto Wax Company, Inc* 2003 U.S. Dist. LEXIS 8833 (May 23, 2003) (Plaintiff’s case dismissed after they used a program called “Evidence Eliminator” to delete documents from his computer after litigation had begun, and just before the defendant’s forensics specialist was going to take an image of the plaintiff’s computer).

<sup>151</sup> *See* David. L. Hudson Jr., *Two U.S. Courts Come Down Hard on E-Discovery Violations*, ABA Journal E-report (2004).

<sup>152</sup> No. 02 Civ. 1243 (S.D.N.Y.).

two years.<sup>153</sup> U.S. District Judge Shira Scheindlin determined that the harsh sanction of an adverse inference was appropriate given the depth of the defendant's refusal to turn over certain documents and the deletion of others.<sup>154</sup>

Judge Scheindlin scolded the defendants and their attorneys for not monitoring the discovery situation more closely and stated "the conduct of both counsel and client thus calls to mind the now-famous words of the prison captain in 'Cool Hand Luke:' what we've got here is a failure to communicate".<sup>155</sup> Scheindlin concluded that UBS employees acted willfully in destroying relevant information and determined that it was not sufficient for counsel to just notify employees that there was a litigation hold on documents.<sup>156</sup> From this action alone counsel could not have reasonably expected that UBS would retain and produce all relevant information to the litigation.<sup>157</sup>

The very next day after the *Zubulake* opinion, the U.S. District Court for the District of Columbia ordered Philip Morris to pay a \$2.75 million sanction for their electronic discovery violations, including the deletion of relevant e-mails.<sup>158</sup> Philip Morris had failed to retain e-mails

---

<sup>153</sup> *Id.*

<sup>154</sup> The instruction given by Judge Scheindlin provides that "if you find that UBS could have produced this evidence, and that the evidence was within its control, and that the evidence would have been material in deciding facts in dispute in this case, you are permitted, but not required, to infer that the evidence would have been unfavorable to UBS" Hudson, *supra* note 204 (citing *Zubulake v. UBS Warburg*, No. 02 Civ. 1243 (S.D.N.Y.)).

<sup>155</sup> *Id.* (quoting Judge Shira Scheindlin in *Zubulake v. UBS Warburg*, No. 02 Civ. 1243 (S.D.N.Y.)).

<sup>156</sup> Thomas M. Freeman, UBS Warburg Sanctioned for Destroying Discoverable E-Mails, 22 No. 6 *Andrews Computer & Internet Litig. Rep.* 12 (August 24, 2004).

<sup>157</sup> *Id.*

<sup>158</sup> *U.S. v. Philip Morris*, No. 99-2496.

in accordance with a court order and with its own electronic discovery retention policy.<sup>159</sup> These recent cases are unlikely to deter all future instances of spoliation, but the attention that *Zubulake* has garnered is sure to alert counsel to the dangers of playing with electronic fire.

## 2. Cost Shifting

A party's justifiable concerns over the cost of electronic discovery lead to the issues of (1) what costs, if any, should be shifted from a responding party to the requesting party and (2) when these cost shifts should properly occur. In *Rowe Entertainment Inc. v. William Morris Agency Inc.*,<sup>160</sup> the United States District Court for the Southern District of New York set forth an eight factor test to determine the extent to which cost of electronic discovery should be shifted to requesting parties.<sup>161</sup> The defendants in the case estimated that production of e-mail backups would cost between \$250,000 and \$400,000 and asked that the plaintiffs take on these costs.<sup>162</sup> The court utilized a complicated eight factor balancing test and determined that the factors weighed heavily in favor of shifting the costs of production onto the plaintiffs, while requiring the defendants to bear costs of reviewing the documents.<sup>163</sup>

In 2003, *Zubulake v. UBS Warburg LLC*<sup>164</sup> modified the *Rowe* factors and divided the analysis into typically accessible forms of data and "inaccessible data."<sup>165</sup> The court concluded

---

<sup>159</sup> *Id.*

<sup>160</sup> 205 F.R.D. 421, 429 (S.D.N.Y. 2002).

<sup>161</sup> *Id.*

<sup>162</sup> *Id.*

<sup>163</sup> *Rowe Entertainment Inc. v. Williams Morris Agency Inc.*, *supra* note 213.

<sup>164</sup> 217 F.R.D. 309 (S.D.N.Y. 2003) (known as "Zubulake I").

<sup>165</sup> *Id.*

that data contained in readable formats on a machine is typically accessible and must be produced at the expense of the producing party.<sup>166</sup> Inaccessible data, like backup tapes, may require the requesting party to fund part of the financial burden of retrieval.<sup>167</sup> This decision reasoned that discovery does not automatically become burdensome merely because electronic evidence is involved.<sup>168</sup> The court recognized that “cost-shifting may effectively end discovery, especially when private parties are engaged in litigation with large corporations.”<sup>169</sup> To determine whether to shift the costs of production the court laid out its own seven factor test, which has been influential in academic and judicial circles.<sup>170</sup>

The case has not been without criticism though. One commentator chastised the court for fashioning “hard and fast rule[s] for electronic discovery.”<sup>171</sup> A standard rule or set of

---

<sup>166</sup> *Id.*

<sup>167</sup> *Zubulake v. UBS Warburg*, *supra* note 218 at 318.

<sup>168</sup> *Id.*

<sup>169</sup> *Id.* at 317

<sup>170</sup> *Zubulake I* test is based on:

1) the extent to which the request is specifically tailored to discover relevant information; 2) the availability of such information from other sources; 3) the total cost of production, compared to the amount in controversy; 4) the total cost of production, compared to the resources available to each party; 5) the relative ability of each party to control costs and its incentive to do so; 6) the importance of the issues at stake in the litigation; and 7) the relative benefits to the parties of obtaining the information. Williger, *supra* note 13 at 23-24 (citing *Zubulake v. UBS Warburg*, 217 F.R.D. 309, 324 (S.D.N.Y. 2003)).

<sup>171</sup> Dan Harshman, *Rise of the Machines: A Critical Look at the New Electronic Discovery Standards*, Vol. 11 American Bar Association, Section of Litigation Business Torts Journal No. 4 (Summer 2004).

determinative factors may deprive district courts of the “flexibility needed to handle such cases on their individual merit.”<sup>172</sup>

The test has also found approval in other cases. In *Xpedior Credit Trust v. Credit Suisse First Boston* the *Zubulake* cost-shifting test was applied and the court found that shifting was not appropriate.<sup>173</sup> The defendant was forced to bear its own costs in producing electronic data.<sup>174</sup>

The *Zubulake* test has not, however, remained entirely untouched. In *Wiginton v. Ellis*,<sup>175</sup> the Northern District of Illinois supplemented the *Zubulake* rules by adding a factor that considers the “importance of the requested discovery in resolving the issues of the litigation.”<sup>176</sup> Weighing the seven Zubulake factors, plus this new factor, the court determined cost shifting to be appropriate, but only shifted 25% of the cost back to the plaintiff because of the general presumption that a responding party should bear the expense of complying with discovery requests.<sup>177</sup>

### III. Argument

---

<sup>172</sup> *Id.* (An example is given with the network disaster recovery method of “hot sites.” These are equipment in place to synchronize the backup site to a network. Obtaining e-mails or data backups from a “hot site” is easier than from a “cold site” where tapes must be located and restored using special equipment. These differences in technology could “upset the predetermined weighing of factors.”)

<sup>173</sup> 2003 U.S. Dist. LEXIS 17497 (S.D.N.Y. Oct. 2, 2003).

<sup>174</sup> *Id.* (The court emphasized that the \$400,000 cost of production did not outweigh the \$7 billion potential value of the entire litigation.)

<sup>175</sup> 2004 WL 1895122 (N.D. Ill. August 9, 2004).

<sup>176</sup> *Id.* at 13

<sup>177</sup> *Id.*

It has become obvious from the burgeoning case law on the subject of electronic discovery that the time has come for the drafters of the Federal Rules of Civil Procedure to step up and set this house in order. To an extent, it is necessary for the Federal Rules of Civil Procedure to take the rulemaking process out of the hands of district courts so that a common rule can prevail, and parties can rest a little easier knowing they might have some semblance of order and protection. That being said, it is unwise to make a rule just to make a rule. Considering the great time and effort that goes into the process of amending any Federal Rule it is imperative that we find the happiest medium possible the first time through.

Some argue that new standards are not necessary. In comments submitted to the Committee on Rules of Practice and Procedure, Mary Alexander, President of the Association of Trial Lawyers of America (ATLA) extolled the position that there should be no revision to the Federal Rules of Civil Procedure regarding electronic discovery.<sup>178</sup> Summing up ATLA's position in a single sentence she wrote "Information is information, and electronic discovery is discovery."<sup>179</sup> She argues that rather than a change in the Federal Rules, we should provide education for judges who are unfamiliar with specific technical matters.<sup>180</sup> She also endorses relying on case law to save the day, comparing the challenge of developing standards for electronic evidence to earlier challenges with product liability, patent, and antitrust litigation.<sup>181</sup> Alexander also does not see "computer based information" as a specific problem, likening it to the technological

---

<sup>178</sup> Letter of ATLA President Mary Alexander to Advisory Committee on Civil Rules (Dec. 20, 2002).

<sup>179</sup> *Id.*

<sup>180</sup> *Id.*

<sup>181</sup> Letter of ATLA President Mary Alexander, *supra* note 235.

breakthrough of the photocopier, an advancement that did not require changes to the Federal Rules.<sup>182</sup>

However, Alexander's view does not properly account for the inherently different nature of electronic documents from paper documents. As stated above, these differences are many, ranging from the immense volume of electronic documents produced compared with paper documents, how dynamic the content is compared with a paper printout or handwritten document, the different perceptions users have about electronic data, to the numerous deletion issues that are raised. Rules that were devised for paper discovery are not adequate to accommodate disputes regarding the key issues in electronic discovery.<sup>183</sup>

Without action to amend the Federal Rules of Civil Procedure the matter would be left entirely on the laps of the federal courts. There is no way to predict whether courts will impose broad or narrow obligations to preserve and produce electronic documents.<sup>184</sup> Different courts may impose different standards based on similar factual circumstances. This could turn what is for some litigators an already confusing technological situation into even greater enigma when it comes to standards on such important rulings as spoliation. An attorney who reads the *Zubulake* or *Philip Morris* decisions should be concerned by the "sanctions noose" hanging above their heads. These courts stepped out into the forefront of this debate with these opinions and in many respects are the beginning points of formulating standards. These courts found bad faith on the part of the responding parties, but it is easy to see how parties who do act in good faith are fearful of penalties for breaking rules that have not even been established yet. Attorneys have an

---

<sup>182</sup> *Id.*

<sup>183</sup> See Jonathan M. Redgrave, *The Rules of Civil Procedure in the Electronic Age: An Opportunity to Be Heard*, 51 *Fed. Law. 5*, 5 (June 2004).

<sup>184</sup> See Bennett, *supra* note 77 at 3.

important role in protecting against the destruction of relevant evidence.<sup>185</sup> To better serve their clients and be better servants to the system, there must be something more substantial for a litigator to act on rather than the newest district court cases from far away jurisdictions. As one commentator suggests, judicial interpretation of the application of traditional discovery principles to electronic discovery is a slow process, and there are “four reasons why we will all get very old if we wait for the adjudicative process to finish that task.”<sup>186</sup>

Another wholly separate reason for wanting to amend the Rules is to avoid obstructionist tactics. There is a fear that where responding parties have previously tended to dump more paper documents on a requesting party than they could possibly handle, with the increased ability to search some electronic documents, responding parties will now do all they can to limit production.<sup>187</sup> *Zubulake* and other spoliation cases may have been decided more to curb this entire practice in electronic discovery than to harm an individual defendant.

The existence of rules and standards that specifically deal with electronic discovery’s most basic elements will likely give obstructing parties less to hide behind. Therefore, there is good reason to amend the Federal Rules of Civil Procedure in targeted ways that provide guidance to

---

<sup>185</sup> See Gregg L. Weiner, *Zubulake Presents Special Challenges To Lawyers Who Are Not IT Experts*, 10/4/2004 N.Y.L.J. T10 (col. 1) (October 4, 2004).

<sup>186</sup> “First, most reported discovery cases come from trial courts and have little precedential value. Second, there is generally very little guidance from courts of appeals, because few discovery cases get appealed. Third, when such cases are appealed, the level of appellate review is deferential, leaving most discovery determinations within the discretion of the trial judge. Fourth, the reported decisions tend to involve obstructionist conduct at the most egregious end of the spectrum, thus arguably offering insufficient guidance to those acting in a mainstream manner.” Brownstone, *supra* note 18 at 29.

<sup>187</sup> Michael J. Ryan, *Countering Defense Tactic: 10 Ways To Beat E-Discovery Abuse*, 40 September Trial 42 (September 2004).

the courts and litigants regarding notable issues in electronic discovery, but in ways that do not encourage and support obstructionist tactics.<sup>188</sup>

Though none of the proposed amendments to the Federal Rules of Civil Procedure are without controversy, one of the least controversial is the proposed amendment to Rule 26(f) concerning “Planning for Discovery.” It would require parties to discuss “any issues relating to disclosure or discovery of electronically stored information.”<sup>189</sup> Mary Alexander, who is against the Rules amendments entirely, finds this requirement unnecessary.<sup>190</sup> She explains that “no rule to advise, prompt, or require courts and parties to include computer based issues in their planning can improve on the incentives that already exist in our system.”<sup>191</sup> These incentives are based on our adversarial system and that the “price of ignorance” often is losing a case.<sup>192</sup>

Alexander notes that electronic evidence is almost always present in “significant litigation” nowadays, but does not support a Rule that would encourage or force parties to talk about this elephant in the room. However, acknowledging that a case may involve electronic evidence at the outset and developing some individualized planning and stipulations can only lower the costs of litigation. It is hardly a shame for one facet of the adversarial system to involve parties working together to avoid massive confusion and possible sanctions due to misunderstandings about technical computer jargon.

---

<sup>188</sup> Redgrave, *supra* note 240.

<sup>189</sup> Proposed Rule 26(f), Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>190</sup> Letter of ATLA President Mary Alexander, *supra* note 235

<sup>191</sup> *Id.*

<sup>192</sup> *Id.*

The proposed Rule 34(b) may be the most advisable, in principle, of all those proposed. In my opinion, however, it contains an ill advised default provision. The proposed Rule would allow a requesting party to designate the form in which it wants electronic data produced.<sup>193</sup> Because of the varying forms in which electronic data can be produced this becomes a more important element than with paper discovery. If the requesting party desires, they can request that electronic data be produced in hard copy format.<sup>194</sup>

There is, however, a default provision in the proposed Rule where if no specific form is requested, the responding party must produce the information in the manner it is usually maintained (presumably its “native” format) or in a searchable form.<sup>195</sup> Microsoft Corporation, in commentary sent to the Advisory Committee on Rules revealed their displeasure over this provision.<sup>196</sup> Microsoft states that it is their belief that “the rules should not favor or specify any particular format of production.”<sup>197</sup> They suggest a rule where the requesting party can specify a form of production, but if the parties do not concur to the method, it would be brought to the attention of the court, which would presumably decide the form of production.<sup>198</sup>

In my opinion, the greatest value in this provision is that it gives a degree of power to party who requests a specific format. If the requesting party asks for production in “.doc” (Word) files

---

<sup>193</sup> Proposed Rule 34(b), Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>194</sup> *Id.*

<sup>195</sup> *Id.*

<sup>196</sup> Letter of Thomas W. Burt, Vice President & Deputy General Counsel, Microsoft Corporation, to Advisory Committee on Civil Rules (Mar. 8, 2004).

<sup>197</sup> *Id.*

<sup>198</sup> *Id.*

or other searchable text files, the responding party would be obligated to comply. I can imagine a situation in the electronic context similar to a party requesting a single paper file, only to receive a warehouse full of documents in return. A requesting party who asks for information without specifying form may receive their information in a form that is unreadable to the human eye like ASCII.<sup>199</sup>

Therefore, agree with Microsoft that the default provision may be unwise as it is written. My fear is that if the requesting party is unsure of what format to request they could be stuck with a “native” format that is entirely unusable without added conversion. This is a gaping hole in the proposed Rule and for fairness’ sake the Rule should not favor “native” formats per se, but rather it would be advisable to follow Microsoft’s advice of having the parties meet to discuss format issues, and if no consensus is reached, defer to the decision of the court.

Proposed Rule 26(b)(5) seeks to address the problem of inadvertent disclosure of privileged information.<sup>200</sup> Inadvertent disclosure has always been a problem in discovery, whether electronic or otherwise.<sup>201</sup> Electronic discovery however, increases the risk by often presenting more information than can be sifted through for privileged information.<sup>202</sup> Proposed Rule 26(b)(5) tries to address this with its “quick peek” provision discussed above. In this single instance I think it may be unwise to tinker with the Federal Rules. Though electronic discovery

---

<sup>199</sup> ASCII is a code for representing English characters as numbers, with each letter assigned a number from 0 to 127. See <http://www.webopedia.com/TERM/A/ASCII.html> (last visited Nov. 10, 2004).

<sup>200</sup> Proposed Rule 26(b)(5), Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>201</sup> Anita Ramasastry, The Proposed Federal E-Discovery Rules: While Trying to Add Clarity, the Rules Still Leave Uncertainty, available at <http://writ.findlaw.com/ramasastry/20040915.html> (last visited Nov. 10, 2004).

<sup>202</sup> *Id.*

admittedly makes the inadvertent disclosure problem worse, I am not certain that codifying the “quick peek” idea is the right solution to the problem. The Sedona Conference’s Sedona Principles list four reasons why this Rule would be ill-advised.<sup>203</sup>

It is the fourth reason, the “Pandora’s box of issues regarding the possible rights of employees (privacy) and third parties (privacy and commercial trade secrets) that I find the most compelling. For a Federal Rule to come out and deny privacy rights of employees and third parties by allowing their private electronically held information to be sent to an opposing party on the stipulation that they will give it back when they find it seems plainly unfair. The fact that this will speed up the process is not sufficient to overcome these concerns. In this one instance it seems that this problem would be best handled by private stipulations of the willing parties as to privilege waiver, so that there is no “wholesale” damage to the rights of either party by the enactment of a blanket Rule.

Proposed Rule 26(b)(2) would allow that a responding party would not need to provide discovery of electronic information that is not “reasonably accessible.”<sup>204</sup> It is a well accepted

---

<sup>203</sup> “First, the voluntary production of privileged and confidential materials to one’s adversary, even in a restricted setting, is inconsistent with tenets of privilege law...Second, despite the strongest possible language in any “clawback” or “quick peek” order to protect against waiver of privileges and dissemination of information, there is no effective way to limit the arguments of non-parties regarding the legal effect of the production in other jurisdictions and forums. Third, counsel has an ethical duty to zealously guard the confidences and secrets of the client. It is possible that questions could arise as to whether voluntarily entering into a “clawback” production could constitute a violation of Model Rules of Professional Conduct 1.1 (requiring a lawyer to use diligence and care in representation) or Model Rules of Professional Conduct 1.6 (protection of client secrets and confidences)...  
...Fourth, there is a Pandora’s box of issues regarding the possible rights of employees (privacy) and third parties (privacy and commercial trade secrets) that may be implicated.” The Sedona Principles: Best Practices, *supra* note 140 at 189.

principle that even deleted electronic information is subject to electronic discovery.<sup>205</sup> Deleted information may be quite difficult and costly to recover. A Rule allowing a party to effectively render documents un-discoverable until a court says otherwise could be read to conflict with this notion that information, even deleted, must be produced. However, as discussed in *Zubulake* the rationale behind cost-shifting was in understanding that some electronic data may be “inaccessible” and the requesting party may need to want the evidence so badly that they will cough up money, just to receive the information.

The *Zubulake* court did express fears that large companies would move towards paper free environments and that a frequent use of cost-shifting would have a crippling effect on discovery in discrimination and retaliation cases.<sup>206</sup>

Also of significant consideration are the genuine fears that corporations and insurance companies, typical responding parties, have. Theresa M. Marchlewski, in her comments to the Advisory Committee on Civil Rules explained how she is often required by the courts to produce information of “marginal relevance but extremely costly to obtain.”<sup>207</sup> These experiences are

---

<sup>204</sup> Proposed Rule 26(b)(5), Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>205</sup> The Sedona Principles: Best Practices, *supra* note 140 at 186 (citing *Antioch Co. v. Scrapbook Borders, Inc.*, 210 F.R.D. 645, 652 (D. Minn. 2002) (“[I]t is a well accepted proposition that deleted computer files, whether they be e-mails or otherwise, are discoverable.”); *Rowe Entm’t, Inc. v. The William Morris Agency, Inc.*, 205 F.R.D. 421, 428 (S.D.N.Y. 2002) (stating that “[e]lectronic documents are no less subject to disclosure than paper records);” *Simon Prop. Group L.P. v. mySimon, Inc.*, 194 F.R.D. 639, 640 (S.D. Ind. 2000) (“[C]omputer records, including records that have been ‘deleted’, are documents discoverable under Fed. R. Civ. P. 34.”).

<sup>206</sup> Williger, *supra* note 13 at 19 (citing *Zubulake v. UBS Warburg LLC*, 217 F.R.D. 309, 317-318 (S.D.N.Y. 2003).

<sup>207</sup> E-mail of Theresa M. Marchlewski, First Vice President and Senior Counsel, Washington Mutual Bank, to Advisory Committee on Civil Rules (Jun. 30, 2003).

echoed in a number of responses to the committee. Don Tierney commented on how his greatest concerns are over attorneys trying to win their cases in discovery through sanctions rather than on the merits.<sup>208</sup> Attorneys like the ones Mr. Tierney describes use the fact that it is becoming increasingly expensive for parties to pay for forensic experts to convert data from backup tapes. They try to capitalize on the opportunity for lost data. In his comments to the Advisory Committee, Peter Oesterling went so far as to ask that cost-shifting language be written into the Rule, rather than just leaving this to the discretion of the courts.<sup>209</sup>

On its own, Rule 26(b)(2) is a sensible, possibly necessary rule to make the process of electronic discovery reasonable for responding parties. However, its application in light of proposed Rule 37(f) calls into question the more sinister ways these two provisions could interact.

Proposed Rule 37(f) seeks to create a “safe harbor” provision from discovery sanctions for a party that fails to produce electronically stored information if that party “took reasonable steps” to preserve discoverable information and this failure resulted from routine operation of the party’s electronic information system.<sup>210</sup> The Committee Notes to the proposed rule point out

---

<sup>208</sup> E-mail of Don Tierney, Claims Litigation Manager, American International Companies, to Advisory Committee on Civil Rules (Jul. 3, 2003).

<sup>209</sup> E-mail of Peter J. Oesterling, Assistant General Counsel, Nationwide Insurance, to Advisory Committee on Civil Rules (Jul. 1, 2003).

<sup>210</sup> Proposed Rule 37(f), Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

that it only addresses sanctions for the loss of electronic data after the commencement of an action.<sup>211</sup>

While the Rule would create a “reasonableness” standard to weigh what the party knew or should have known when it took (or did not take) steps to preserve electronic information, it does nothing to protect data prior to the commencement of an action.<sup>212</sup> If a producing party has a liberal deletion policy for electronic data, prior to the commencement of legal action, this could easily make electronic evidence “inaccessible.” If the evidence is then “inaccessible” it would be protected by proposed Rule 26(b)(2) and the requesting party would need to show cause to force the producing party to give up the information. Further, under the current status of cost-shifting after *Zubulake*, the costs or part of the costs of retrieving this “inaccessible” data can be shifted back to the requesting party. This would give many potential defendants (often large corporations) the ability to burden plaintiffs seeking information by making evidence inaccessible as to qualify for protection and cost-shifting.<sup>213</sup> As such, at a minimum, Rule 26(b)(2) may need to further define “reasonably accessible” so that it doesn’t become an excuse not to offer a plaintiff relevant records.

---

<sup>211</sup> Committee Notes, Proposed Rule 37(f), Committee On Rules of Practice and Procedure of the Judicial Conference of the United States, Report of the Civil Rules Advisory Committee, *supra* note 146.

<sup>212</sup> *Id.*

<sup>213</sup> See Robert S. Peck, ATLA’s Law Firm Takes ‘Reform’ Fight To The Courts, 40 Trial 50 (July 2004) (stating that “under such a rule, parties could design their own document destruction programs, require an extremely high level of proof before plaintiffs can obtain a preservation order, and then be excused for any information destroyed in the interim.”); See also Jokela, *supra* note 5 at 1050 (citing *Gumbs v. Int’l Harvester, Inc.*, 718 F. 2d 88, 96 (3d Cir. 1983) (“a corporation cannot blindly destroy documents and expect to be shielded by an innocuous document retention policy).

The key to the above cycle is in what is considered “reasonable deletion under routine business operations.” One such policy conducted in the course of regular business was that of the now infamous Arthur Anderson accounting firm. In May 2002, when one Arthur Anderson partner pled guilty to federal charges, he testified that “I obstructed justice...I instructed people on the engagement team to follow a document-retention policy which I knew would result in the destruction of documents.”<sup>214</sup> In terms of electronic data, one section of their policy ordered that “deletion of all information from electronic files will be accomplished in such a way that precludes the possibility of subsequent retrieval by Arthur Anderson personnel or third parties.”

In their comments to the Advisory Committee, Microsoft voiced their strong support for the “safe harbor” provision of proposed Rule 37(f) and argued that the Committee should “clarify” that the rule “does not implicate the routine recycling or disposal of backup tapes in the ordinary course of business.”<sup>215</sup> They also argue for clarification that while willful or reckless destruction of data should be sanctionable, the routine recycling of backup tapes is neither willful nor reckless.<sup>216</sup> Microsoft, however, is hardly the poster-company for good faith retention of electronic documents.

In current antitrust litigation with Burst.com Inc., Microsoft is accused of numerous discovery violations.<sup>217</sup> Burst.com’s reply brief paints the picture of a system that defaults to swift

---

<sup>214</sup> Middleton, *supra* note 172 at 109.

<sup>215</sup> Letter of Thomas W. Burt, Vice President & Deputy General Counsel, Microsoft Corporation, to Advisory Committee on Civil Rules, *supra* note 253.

<sup>216</sup> *Id.*

<sup>217</sup> Burst’s Reply to Compel Microsoft To Produce Documents Relating To Its Document Preservation Policy, In Re Microsoft Corp. Antitrust Litigation, United States District Court of Maryland, Civil Action No. JFM-02-cv-2952,

destruction of employee e-mails and identifies the wrong people so that retained records are useless and “relevant” employees’ e-mails are not retained.<sup>218</sup> One known fact is that Microsoft executive Jim Allchin instructed Windows division employees to delete emails from their hard drives after thirty days.<sup>219</sup> The exceptions to this order were for those employees who received specific instruction to retain documents or e-mail related to pending litigation.<sup>220</sup> There are, however, several glaring examples where Microsoft failed to identify relevant employees and send them retention notices.<sup>221</sup> In one such case the key negotiators in negotiations with RealNetworks were not notified to retain their e-mail messages.<sup>222</sup> That deal became known as the “Chris Phillips” deal, named after the lead negotiator, but ironically he was never instructed to retain e-mails concerning those negotiations.<sup>223</sup> Only the attorney who was assigned to draft the contract was given a retention instruction, and conveniently those e-mails are barred from discovery by privilege.

These are but two frightening examples of what is happening in the business world concerning electronic document retention policies. Stephanie Middleton, Chief Counsel for CIGNA Corporation warns that “contrary to the picture some like to paint, we do not wake up

---

available at [http://www.pbs.org/cringely/links/burstbrief\\_1.pdf](http://www.pbs.org/cringely/links/burstbrief_1.pdf) and

[http://www.pbs.org/cringely/links/burstbrief\\_2.pdf](http://www.pbs.org/cringely/links/burstbrief_2.pdf)

<sup>218</sup> *Id.* See also John Lettice, How key Microsoft Emails “Autodestruct,” The Register (October 11, 2004) available at [http://222.theregister.co.uk/2004/10/11/ms\\_legal\\_mail\\_autodestruct/print.html](http://222.theregister.co.uk/2004/10/11/ms_legal_mail_autodestruct/print.html).

<sup>219</sup> Burst’s Reply to Compel, *supra* note 276.

<sup>220</sup> *Id.*

<sup>221</sup> *Id.*

<sup>222</sup> Burst’s Reply to Compel, *supra* note 276.

<sup>223</sup> *Id.*

each day with a desire or plan to destroy evidence.”<sup>224</sup> Regardless of the good intentions of some, the above discovery horror stories are too prevalent to ignore.

It is possible that the biggest problem with proposed Rule 37(f) is not with the Rule itself, but with the lack of sound electronic retention standards. Some businesses are required by state or federal law to retain certain electronic documents for specified periods of time.<sup>225</sup> However, the policies are not as clear for other business documents. One recent survey revealed that nearly 55% of employees knew their businesses did not have a written e-mail retention and deletion policy.<sup>226</sup> Nearly 24% of those polled said they did not know the difference between electronic business records that must be retained versus an insignificant message that may be deleted.<sup>227</sup> This reveals that a disturbingly high percentage of businesses and employees may not be currently prepared to comply with the proposed Rule 37(f) in good faith, even if they wanted to.

Unless there are wholesale changes in the electronic document retention policies of many businesses, there is no place in the amended rules for Rule 37(f). As it currently reads, and in light of proposed Rule 26(b)(2,) Rule 37(f) may actually encourage bad faith, may reward companies who have deplorable retention policies, and may undermine the progress made in

---

<sup>224</sup> Letter of Stephanie Middleton, Chief Counsel, Litigation, CIGNA Corporation, to Advisory Committee on Civil Rules (March 12, 2004).

<sup>225</sup> Examples include Securities and Exchange Commission (SEC), Internal Revenue Service (IRS), and Occupational Safety & Health Administration (OSHA) regulations.

<sup>226</sup> The ePolicy Institute 2004 Workplace E-mail and Instant Messaging Survey, available at <http://www.epolicyinstitute.com/survey/survey04.pdf> (35% answered their organization has a policy, while 10% are unsure) (last visited Nov. 10, 2004).

<sup>227</sup> *Id.* (63% answered that they knew the difference, while 13% were unsure).

alerting businesses and attorneys to the seriousness of “electronic” spoliation in the post *Zubulake* and *Philip Morris* environment.

#### IV. Conclusion

When all is said and done, the proposed amendments to the Federal Rules of Civil Procedure are just that - proposals. They are an excellent starting point and represent the consciousness that something needs to be done to right this ship. If these Rules are going to be successful and fair, however, they need to address the uniqueness of electronic discovery from paper discovery, but protect both the requesting parties and responding parties as well as third parties and employees that are affected.

However, I am not currently in the trenches dealing with the processes, pitfalls, and personalities involved with the discovery of electronic evidence. The rather radical views that requesting and responding parties introduce in their comments to the Advisory Committee on Rules of Practice and Procedure speak volumes of the divisions within the legal field. It is my sincere hope that when this long and arduous rulemaking process comes to an end, that there are firm rules in place dealing with the unique features of electronic discovery, but that they actually move us forward towards a more fair, more co-operative, and most importantly, a more certain system.