University of Baltimore Law Review

Volume 37
Issue 3 *Spring 2008*

Article 4

2008

"Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information

Kenneth J. Withers
The Sedona Conference

"EPHEMERAL DATA" AND THE DUTY TO PRESERVE DISCOVERABLE ELECTRONICALLY STORED INFORMATION

Kenneth J. Withers†

I. ELECTRONICALLY STORED INFORMATION AND THE DUTY OF PRESERVATION UNDER THE RULES OF CIVIL PROCEDURE

The duty to take reasonable steps to preserve evidence discoverable in pending or anticipated civil litigation is well established in U.S. civil jurisprudence.[1] Courts differ about when the duty of preservation is triggered, the particular scope of that duty, and what steps of preservation are considered reasonable on a case-by-case basis,[2] but the general rule is clear: parties have a duty to preserve

---

† Kenneth J. Withers is Director of Judicial Education and Content for The Sedona Conference®, a non-profit law and policy think-tank based in Arizona. The author wishes to thank David W. Degnan, a second-year law student at Oklahoma City University School of Law, for his initial drafts of many sections of this article and his able assistance with research, editing, and citations, without which this article would not have been possible. The opinions expressed in this article are entirely those of the author.

1. *See* THE SEDONA CONFERENCE WORKING GROUP ON ELECTRONIC DOCUMENT RETENTION & PRODUCTION, THE SEDONA CONFERENCE COMMENTARY ON LEGAL HOLDS: THE TRIGGER AND THE PROCESS (drft. ed. 2007), *available at*, http://www.thesedonaconference.org/dltForm?did=Legal_holds.pdf [hereinafter SEDONA CONFERENCE COMMENTARY].

2. *Compare* Turner v. Resort Condominiums Int'l, LLC, No. 1:03-cv-2025-DFH-WTL, 2006 WL 1990379, at *8 (S.D. Ind. July 13, 2006) (holding that the defendant did not have to initiate a litigation hold in response to opposing counsel's "overly broad" form letter), *and* Conderman v. Rochester Gas & Elec. Corp., 262 A.D.2d 1068, 1069 (N.Y. App. Div. 1999) ("In the absence of pending litigation or notice of a specific claim, a defendant should not be sanctioned for discarding items in good faith and pursuant to its normal business practices."), *with* Kronisch v. United States, 150 F.3d 112, 126 (2d Cir. 1998) (noting the "obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation—most commonly when suit has already been filed, providing the party responsible for the destruction with express notice, but also on occasion in other circumstances, as for example when a party should have known that the evidence may be relevant to future litigation").

evidence in their possession, custody, or control that is relevant to pending or reasonably anticipated litigation.[3]

When evidence consists primarily of documents, photographs, and physical objects, the steps needed to locate and preserve these items are relatively straightforward, if occasionally convoluted or botched.[4] However, the forms and formats of evidence have changed significantly in the past few years, as recognized by the December 2006 e-discovery amendments to the Federal Rules of Civil Procedure[5] (the Rules) and subsequent efforts to amend the discovery rules in several states.[6] These amendments make provision for the discovery of electronically stored information (ESI),[7] which is quickly replacing paper, film, and other physical media as the primary storage method for information in business, government, and daily life.[8]

While the Federal Rules of Civil Procedure and their state equivalents address many of the recurring problems unique to the

---

3. Zubulake v. UBS Warburg LLC (*Zubulake IV*), 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("While a litigant is under no duty to keep or retain every document in its possession . . . it is under a duty to preserve what it knows, or reasonably should know, is relevant in the action, is reasonably calculated to lead to the discovery of admissible evidence, is reasonably likely to be requested during discovery and/or is the subject of a pending discovery request.") (quoting Turner v. Hudson Transit Lines, 142 F.R.D. 68, 72 (S.D.N.Y. 1991)).

4. *See, e.g.*, Jackson v. Harvard Univ., 721 F. Supp. 1397, 1409–13 (D. Mass. 1989) (finding accidental destruction of relevant paper files by a third party, despite Harvard Business School's complex procedure for records management and preservation, did not merit spoliation sanctions).

5. *See* FED. R. CIV. P. 26, 37 and accompanying advisory committee's notes to the 2006 amendments.

6. Nathan Drew Larsen, Note, *Evaluating the Proposed Changes to Federal Rule of Civil Procedure 37: Spoliation, Routine Operation and the Rules Enabling Act*, 4 NW. J. TECH. & INTELL. PROP. 212, 218 (2006); *see, e.g.*, Proposed Arizona Rules of Civil Procedure 16, 26, 26.1, 33, 34, 37, 45 Public Comments Forum, http://www.dnnsupremecourt.state.az.us/AZSupremeCourtMain/AZCourtRulesMain/CourtRulesForumMain/CourtRulesForum/tabid/91/view/topic/postid/227/forumid/2/tpage/1/Default.aspx; *see also* NATIONAL CONFERENCE OF COMMISSIONERS ON UNIFORM STATE LAWS, UNIFORM RULES RELATING TO THE DISCOVERY OF ELECTRONICALLY STORED INFORMATION (2007), http://www.law.upenn.edu/bll/archives/ulc/udoera/2007_final.pdf.

7. *See* FED. R. CIV. P. 26, 34, 37(e), 45, and accompanying advisory committee's notes to the 2006 amendments.

8. Peter Lyman & Hal R. Varian, *How Much Information? 2003* (2003), http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf (reporting ninety-two percent of all new information was created and stored on magnetic media).

discovery of ESI, they only make passing reference to the question of preservation.[9] Rule 26(f) instructs parties to "discuss any issues about preserving discoverable information."[10] The advisory committee's note accompanying Rule 37(e),[11] while addressing sanctions that may result from the loss of discoverable ESI, does not establish a duty of preservation, stating that "[a] preservation obligation may arise from many sources, including common law, statutes, regulations, or a court order in the case."[12] It is well established at common law that the duty of preservation might arise before litigation has been filed;[13] thus it is unlikely that any rules of procedure would directly address each issue.

ESI is the product of complex computer systems and has an essentially ephemeral nature.[14] The advisory committee's note to Rule 37(e) states "[t]he 'routine operation' of computer systems includes the alteration and overwriting of information, often without the operator's specific direction or awareness, a feature with no direct counterpart in hard-copy documents."[15] Rules 26(f) and 37(e) recognize this important difference between information recorded on physical media (such as paper) and ESI.[16] However, Rule 37(e) does not excuse litigants from a duty to take reasonable good-faith steps to preserve ESI.[17] The advisory committee's note explains:

> Good faith in the routine operation of an information system may involve a party's intervention to modify or suspend certain features of that routine operation to prevent the loss

---

9. *See, e.g.*, FED. R. CIV. P. 26(f) advisory committee's note to the 2006 amendments.
10. FED. R. CIV. P. 26(f)(2).
11. An amendment, effective Dec. 1, 2007, restyled the Federal Rules of Civil Procedure and relocated 37(f) to 37(e), and 37(g) to 37(f). *See* FED. R. CIV. P. 37 advisory committee's note to 2007 amendments. Thus, any reference in the main text of this article to the advisory committee's note to Rule 37(e) refers back the advisory committee's note to Rule 37(f). *See infra* notes 12, 16, 18.
12. FED. R. CIV. P. 37(f) advisory committee's note to the 2006 amendments.
13. Fujitsu Ltd. v. Fed. Express Corp., 247 F.3d 423, 436 (2d Cir. 2001) ("The obligation to preserve evidence arises when the party has notice that the evidence is relevant to litigation or when a party should have known that the evidence may be relevant to future litigation.").
14. Shira A. Scheindlin & Jeffrey Rabkin, *Electronic Discovery in Federal Civil Litigation: Is Rule 34 Up to the Task?*, 41 B.C. L. REV. 327, 331–36 (2000) (defining "electronic evidence" and transformation and storage in binary form).
15. FED. R. CIV. P. 37(e). Despite such protection, the rule does contain a heightened "[a]bsent exceptional circumstances" caveat. FED. R. CIV. P. 37(e). *See also* Larsen, *supra* note 6, at 215–16 (discussing the safe harbor provision).
16. *See* Fed. R. Civ. P. 26(f), 37(f) advisory committee's notes to the 2006 amendments.
17. *See* FED. R. CIV. P. 37(e).

> of information, if that information is subject to a preservation obligation . . . . When a party is under a duty to preserve information because of pending or reasonably anticipated litigation, intervention in the routine operation of an information system is one aspect of what is often called a "litigation hold."[18]

During the first year the e-discovery amendments to the Rules were in effect, several courts directly confronted the intertwined issues of whether the obligation of preservation extended to ephemeral ESI and if so, what steps would be considered reasonable to meet that obligation.[19] The apparent inconsistency in the imposition of sanctions by courts created considerable unease among counsel and client regarding the extent of their ESI preservation obligations.[20] In Part II of this article, we will explore the most high-profile of those cases,[21] *Columbia Pictures Indus. v. Bunnell*.[22] In Part III, we will attempt to define, in non-technical terms, "ephemeral data," and illustrate how it may or may not be relevant in a variety of litigation scenarios.[23] In Part IV, we will place the *Columbia Pictures* case in the context of other recent cases involving various types of ephemeral ESI.[24] Finally, we will develop a set of recommended actions and alternatives for parties, both requesting parties and responding parties, facing questions about the preservation of ephemeral ESI.[25]

II. *COLUMBIA PICTURES INDUS. V. BUNNELL*

On February 23, 2006, a group of motion picture studios that owned rights to numerous Hollywood movies and television shows filed a complaint in the United States Federal District Court, Central District of California against the operators of a web site which, according to the plaintiffs, allowed Internet users to locate and

---

18. FED. R. CIV. P. 37(f) advisory committee's note to the 2006 amendments.
19. *See* Columbia Pictures, Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419 (C.D. Cal.), *motion for review denied sub nom.* Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal. 2007); Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627 (E.D. Pa. 2007). *See also infra* Parts II, IV.
20. *Id.*
21. *See infra* Part II.
22. No. CV 06-1093FMCJCX, 2007 WL 2080419.
23. *See infra* Part III.
24. *See infra* Part IV.
25. *See infra* Part V.

download unauthorized copies of their works.[26] It became known in the press as the "BitTorrent" case, after the software technology employed to enable Internet users to join a peer-to-peer network to share large computer files.[27] It was also known as the "TorrentSpy" case, after the web site operated by the defendants.[28]

The case was filed as part of the industry's effort to combat movie piracy.[29] However, the plaintiffs did not sue the actual infringers for unauthorized copying or possession of the protected works.[30] Rather, they sued the operators of the web site for secondary or contributory infringement, alleging that the "[d]efendants knowingly enable[d], encourage[d], induce[d], and profit[ed] from the online piracy of [p]laintiffs' copyrighted works."[31]

In formal discovery under Federal Rule of Civil Procedure 34, the defendants sought:

> [A]ll documents that identify the dot-torrent files that have been made available by, searched for, or downloaded by users of TorrentSpy, including documents that identify the users who have made available, searched for, or downloaded such dot-torrent files . . . [and] all documents, including server logs, databases of a similar nature, or reports derived from such logs or databases that [defendants] maintain, have ever maintained, or have available that record the activities of TorrentSpy or its users, including documents concerning . . . Electronic communications of any type between TorrentSpy and [users]; . . . Logs of user activities; and . . . Logs or records of dot-torrent files made available, uploaded, searched for, or downloaded on TorrentSpy.[32]

In practical terms, the plaintiffs asked for information identifying users of the TorrentSpy web site who were requesting movie, video or song files from other TorrentSpy users, to support their allegation

---

26. *Columbia Pictures*, 245 F.R.D at 445.
27. *See, e.g.*, Eric Sinrod, *The Aftermath: Examining the E-Discovery Landscape After the 2006 Rule Changes*, TECH. L. CENTER, Oct. 16, 2007, http://technology.findlaw.com/articles/00006/011010.html.
28. *See generally* Douglas L. Rogers, *Decision to Produce RAM in Columbia Pictures Should Not Change Companies' E-Commerce Practices*, E-COMMERCE L. & STRATEGY, Sept. 24, 2007, http://www.law.com/jsp/article.jsp?id=1190624573330.
29. Press Release, Motion Picture Association of America, Studios Move to Thwart Illegal File Swapping on Major Pirate Networks (Feb. 23, 2006), http://www.mpaa.org/press_releases/2006_02_23.pdf.
30. *Columbia Pictures*, 245 F.R.D. at 445.
31. *Id.*
32. *Columbia Pictures*, 2007 WL 2080419, at *1 n.2 (alterations in original).

that the TorrentSpy web site operators intentionally facilitated the distribution of copyrighted materials.[33] Specifically, the plaintiff wanted to obtain "(a) the IP[34] addresses of [web site visitors who] request[ed] 'dot-torrent' files; (b) the requests for 'dot-torrent files'; and (c) the dates and times of such requests."[35]

This information, collectively known as "Server Log Data," would need to be derived from the stream of digital information that is processed in the Random Access Memory (RAM) of the defendants' web servers.[36] Such data is stored in RAM momentarily until the computer acts on the information by sending the requested file to the web site visitor, after which the data is routinely overwritten by new information.[37] The routine overwriting of data in RAM can take place within a fraction of a second or up to six hours later.[38]

To extract Server Log Data from RAM and preserve it, the website operator would need to enable a logging or tracking function on the web server.[39] Many web site operators routinely enable this function to do general maintenance on their servers and record information for later marketing purposes.[40] However, the operators of the TorrentSpy web site specifically chose not to activate the web server's logging capability, taking the position that enabling that function would violate the web site's confidentiality policy and would negatively impact business.[41] In fact, the company's confidentiality policy stated that it "will not collect any personal information" about its users unless the user "specifically and knowingly provide[s] such information."[42]

On May 15, 2006, the plaintiffs sent a formal notice to the defendants' counsel, reminding them of their obligation to "preserve

33. *Id.* at *1.

34. An IP (Internet Protocol) address is "a standard way of identifying a computer that is connected to the Internet." *Id.* at *2 n.7; *see generally IP Addresses Explained*, http://www.whatismyip.com/IP-address.asp (last visited Feb. 29, 2008).

35. *Columbia Pictures*, 2007 WL 2080419, at *1.

36. *Id.* at *1 n.3.

37. *Id.* at *2–3; Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 446 (C.D. Cal. 2007).

38. *Columbia Pictures*, 2007 WL 2080419, at *2–3.

39. *Id.* at *2.

40. *Id.* at *2 n.8.

41. *Id.* at *8.

42. *Id.* at *3 n.10. The court noted that the defendants "presented no evidence" that defined "personal information" in their privacy policy. *Id.* Therefore, the court concluded that it was unclear whether "IP addresses, let alone the other components of the Server Log Data," were "personal information" in the defendants' privacy policy. *Id.*

all potentially discoverable evidence in their possession, custody or control related to the litigation, including all logs for the TorrentSpy website, and records of all communications between defendants and users of the website, including instant-messaging and other chat logs."[43] However, the "notice did not specifically request [the] defendants [to] preserve Server Log Data temporarily stored only in RAM."[44]

Throughout discovery, the defendants failed to produce Server Log Data, taking the position that the data was not "electronically stored information" within the meaning of Federal Rule of Civil Procedure 34, because the information found only in RAM is not "stored" in the ordinary sense of the word.[45] Alternatively, or as a corollary, the defendants objected that recording the Server Log Data would constitute the creation of ESI for the sole purpose of discovery, which is outside the scope of ordinary discovery and constituted injunctive relief and beyond the power of a magistrate judge.[46]

As a threshold matter, the court determined that the requested Server Log Data came within the scope of relevant discovery, defined by Rule 26(b)(1) as "any matter, not privileged, that is relevant to the claim or defense of any party."[47] The court held that in a case of contributory infringement, "[t]here can be no serious dispute that the Server Log Data in issue is extremely relevant and may be key to the instant action."[48]

Relying in large part on Ninth Circuit precedent, the magistrate judge found,[49] and the district judge confirmed, that the requested Server Log Data is discoverable under the Federal Rules of Civil Procedure as electronically stored information.[50] Rule 34(a) states the requesting party may:

> [I]nspect, copy, test, or sample any designated documents or electronically stored information . . . stored in *any* medium from which information can be obtained—translated, if necessary, by the respondent into reasonably usable form, or

---

43. *Id.* at *4. The court mistakenly wrote that "defendants sent a notice to plaintiffs' counsel."
44. *Id.*
45. Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 446 (2007).
46. *Columbia Pictures*, 2007 WL 2080419, at *6.
47. *Columbia Pictures*, 245 F.R.D. at 448.
48. *Columbia Pictures*, 2007 WL 2080419, at *4 (citing FED. R. CIV. P. 26(b)(1)) (making no distinction between secondary and contributory copyright infringement).
49. *Id.*
50. *Columbia Pictures*, 245 F.R.D. at 447–48.

> to inspect, copy, test, or sample any designated tangible things which constitute or contain matters within the scope of Rule 26(b) and which are in the possession, custody or control of the party upon whom the request is served . . . .[51]

The advisory committee's note accompanying Rule 34 states that the rule "applies to information that is fixed in a tangible form and to information that is stored in a medium from which it can be retrieved and examined."[52] The advisory committee's note further states that Rule 34 "is expansive and includes any type of information that is stored electronically," and that it "is intended to be broad enough to cover *all* current types of computer-based information, and flexible enough to encompass future changes and development."[53]

The court compared the advisory committee's use of the term "fixed" to explain the scope of discoverable information with the Ninth Circuit's use of the term "fixed" to describe the scope of digital information subject to copyright.[54] In *MAI Systems Corp. v. Peak Computer, Inc.*,[55] the Ninth Circuit concluded that a copy of a program copied into RAM is fixed in a manner that is "sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration," giving rise to copyright infringement liability.[56] More recently, in *Perfect 10, Inc. v. Amazon.com*,[57] the Ninth Circuit held that a digital photographic image is "'fixed' in a tangible medium of expression,"[58] when stored in a computer's server, giving rise to copyright infringement liability.[59] Based on these precedents, the court determined that the defendant is under an obligation to preserve and produce the Server Log Data, as it is "fixed" while stored in RAM for processing and is therefore "electronically stored information" within the meaning of Rule 34.[60]

The court acknowledged that as a general rule, a producing party cannot be compelled to create new information to meet a discovery

---

51. FED. R. CIV. P. 34(a) (emphasis added).
52. FED. R. CIV. P. 34 advisory committee's note to the 2006 amendments.
53. *Id.* (emphasis added).
54. *Columbia Pictures*, 2007 WL 2080419, at *4–5.
55. 991 F.2d 511 (9th Cir. 1993).
56. *Id.* at 518 (quoting 17 U.S.C. § 101 (1992)).
57. 487 F.3d 701 (9th Cir. 2007).
58. *Id.* at 716.
59. *Id.*
60. *Columbia Pictures*, 2007 WL 2080419, at *5.

request.[61] But the court rejected the defendant's argument, based on *Paramount Pictures Corp. v. Replay TV*[62] and *Alexander v. FBI*,[63] that the proposed order would require that it create new information.[64] Distinguishing the cases cited by the defendant,[65] the court found that the Server Log Data requested by the plaintiffs exists at any given moment, so the court is not asking that this data be created, but preserved on an ongoing basis.[66] In *Paramount Pictures* and *Alexander*, the requested data never existed in the first place.[67]

Finding that the request for Server Log Data was within the scope of Rules 26 and 34, the court then weighed whether an order for the preservation of the data was appropriate.[68] Utilizing the three-part test from *Capricorn Power Co. v. Siemens Westinghouse Power Corp.*,[69] the court weighed:

> (1) the level of concern . . . for the continuing existence and maintenance of the integrity of the evidence in the absence of an order directing preservation; (2) any irreparable harm likely to result to the party seeking the preservation of the evidence absent an order directing preservation; and (3) . . . the physical, spatial and financial burdens created by ordering evidence preservation.[70]

Noting that the defendants objected to the retention of Server Log Data and that the data had "key relevance" in the action, the court determined that consideration of the first two factors weighed "clearly . . . in favor of requiring preservation of the Server Log Data."[71]

However, the court's consideration of the third factor, the potential burden of a preservation order, required findings of fact similar to

---

61. *Id.* at *6 (citing Alexander v. FBI, 194 F.R.D. 305, 310 (2006)) ("Rule 34 only requires a party to produce documents that are already in existence.").
62. No. CV 01-9358FMC(Ex), 2002 WL 32151632, at *3 (C.D. Cal. May 30, 2002) (denying production of customer data because such information "is not now and never has been in existence").
63. 194 F.R.D. 305, 310 (D.D.C. 2000) (denying production of a certain list of names because there was no evidence that such a list existed or that the responding party was in possession of such list).
64. *Columbia Pictures*, 2007 WL 2080419, at *6.
65. *Id.*
66. *Id.* at *6, *14.
67. *Id.* at *6.
68. *Id.* at *7.
69. 220 F.R.D. 429, 433–34 (W.D. Pa. 2004).
70. *Columbia Pictures*, 2007 WL 2080419, at *7.
71. *Id.*

those required when considering the burden of an order compelling production under Rule 26(b)(2)(C).[72] Here, the court was faced with the conflicting testimony of the plaintiffs' expert and the defendants.[73] The court found the plaintiffs' expert witness "to be the most credible of the three technical declarants/witnesses."[74] The defendants represented that their preservation and production of all data in RAM would require between thirty and forty gigabytes of storage per day and the costs would be prohibitive.[75] The plaintiffs' expert estimated that by selectively saving only the data in RAM, relevant to the Server Log Data, the volume would be about one-one hundredth of the defendants' estimate.[76] The defendants estimated that the cost of reconfiguring their server would be approximately $10,000 and the purchase of a new server about $50,000, while the plaintiffs estimated that the cost of storing the requested information would be about five to ten minutes of time and less than a dollar in media costs per day.[77] Perhaps of greater concern for the plaintiffs, however, was the impact the proposed preservation order and discovery would have on the web site's stated privacy policy.[78] Characterizing the concerns the defendants expressed about the loss of customers and advertisers as "largely speculative, conclusory and without foundation,"[79] the court concluded that the preservation of the Server Log Data "is appropriate in light of . . . the key relevance and unique nature of the Server Log Data in this action, [and] the lack of a reasonable alternative means to obtain such data."[80] Under a protective order, the IP addresses would be masked from disclosure in any production of the Server Log Data.[81]

In sum, the court determined that the Server Log Data requested by the plaintiff was relevant and unique; that the requested information was momentarily stored or "fixed" in RAM but had not been

---

72. *Id.* FED. R. CIV. P. 26(b)(2)(C) provides that the court may limit the "frequency or extent of use of the discovery methods . . . if it determines that: . . . (iii) the burden or expense of the proposed discovery outweighs its likely benefit, taking into account . . . the parties' resources . . . and the importance of the proposed discovery in resolving the issues."

73. *Columbia Pictures*, 2007 WL 2080419, at *2 n.6.

74. *Id.*

75. *Id.* at *8.

76. *Id.*

77. *Id.* at *8 nn.17 & 20.

78. *Id.* at *8.

79. *Id.* at *11.

80. *Id.*

81. *Id.* at *8.

preserved; that the preservation of the information did not require the creation of new data; and the information could be preserved in a manner that did not constitute an undue burden on the defendant.[82] Therefore, the court held that Server Log Data could be preserved and produced.[83] However, this holding turns specifically on the defendants' ability to log the IP addresses prospectively.[84] Relying on the testimony of the plaintiffs' expert, the court found that the Server Log Data could be logged without undue burden on the producing party,[85] and if the producing party could log discoverable data before the data was deleted through the routine operation of its information system, it was required to do so.[86]

Despite a finding that the defendant did not comply with Rules 26(b) and 34(a), and had an ongoing obligation to preserve Server Log Data found in RAM, the court determined that sanctions under Rule 37(f) were not appropriate.[87] The Rule prohibits sanctions, absent extraordinary circumstances, for failing to provide electronically stored information lost as the result of the routine, good-faith operation of an electronic information system.[88] The court declined to find that the defendant did not act in good faith, given that RAM may be considered "not reasonably accessible" electronically stored information, the lack of prior precedent on point in the discovery context, the lack of a specific request from the plaintiff, and the lack of a preservation order.[89] In addition, the court, in a footnote, stressed the very limited and fact-specific nature of its ruling in this case:

> The court emphasizes that its ruling should *not* be read to require litigants in all cases to preserve and produce electronically stored information that is temporarily stored only in RAM. The court's decision in this case to require the retention and production of data which otherwise would be temporarily stored only in RAM, is based in significant

82. *Id.* at *1, *5.
83. *Id.* at *14.
84. *Id.* (requiring the defendants to preserve server log within seven days of the opinion until the end of trial).
85. *Id.* at *8. The expert explained the usefulness of logging data, implicitly suggesting that logging is commonplace for upkeep purposes. *Id.* at *2 n.8.
86. *Id.* at *13–14.
87. *Id.* at *6, *13–14.
88. *Id.* at *13–14.
89. *Id.* ("As a general rule, the litigation hold does not apply to inaccessible electronically stored information, such as back-tapes, which may continue to be recycled on the schedule set forth in the company's policy.").

> part on the nature of this case, the key and potentially dispositive nature of the Server Log Data which would otherwise be unavailable, and defendants' failure to provide what this court views as credible evidence of undue burden and cost.[90]

Nonetheless, the defendant appealed the magistrate judge's ruling to the district judge,[91] and was joined in the appeal by *amici*, who filed briefs decrying the potential violations of privacy and expansion of the scope of discovery that they feared the decision would justify in future cases.[92] The district court upheld the magistrate judge's ruling in a detailed opinion.[93] A few months later, the district court found that the defendant had engaged in "widespread and systematic efforts to destroy evidence" unrelated to its failure to preserve Server Log Data, and the district judge granted the plaintiffs' Motion for Terminating Sanctions.[94]

III. WHAT IS "EPHEMERAL DATA"?

The American Heritage Dictionary defines ephemeral as: "1. Lasting for a markedly brief time . . . 2. Living or lasting only for a day, as certain plants or insects do."[95] Similarly, Merriam-Webster's Dictionary defines ephemera as "something of no lasting significance"[96] and ephemeral as "lasting a very short time."[97]

Outside the context of discovery, ephemeral data can refer to data on "satellite geometry, position, and movement."[98] However, judges

---

90. *Id.* at *13 n.31.
91. Columbia Pictures, Inc. v. Bunnell, 245 F.R.D. 443, 445 (C.D. Cal. 2007).
92. *See, e.g.*, Brief for Electronic Frontier Foundation and the Center for Democracy & Technology as Amici Curiae in Support of Defendant's Objections To and Motion for Review of Order re Server Log Data, *Columbia Pictures*, 245 F.R.D. 443 (No. 06-01093 FMC), *available at* http://w2.eff.org/legal/cases/torrentspy/EFF_CDT_amicus.pdf.
93. *Columbia Pictures*, 245 F.R.D. at 453.
94. Columbia Pictures, Inc. v. Bunnell, 85 U.S.P.Q. 2d 1448, 1454 (C.D. Cal. Dec. 13, 2007).
95. THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 599 (Houghton Mifflin Co. ed., 4th ed. 2000).
96. MERRIAM-WEBSTER'S COLLEGIATE DICTIONARY 419 (Merriam-Webster, Inc. ed., 11th ed. 2003).
97. *Id.*
98. G. M. Brilis, R. J. van Waasbergen, P. M. Stokely & C. L. Gerlach, *Remote Sensing Tools Assist in Environmental Forensics: Part II—Digital Tools*, 2 ENVTL. FORENSICS J. 1, 5 (2001), *available at* http://www.epa.gov/esd/gqc/pdf/RS%20Pt2.pdf.

and legal commentators in the electronic discovery field use the ephemeral data to refer specifically to data found in RAM, as in the *Columbia Pictures* case,[99] and more broadly to other types of data that are briefly stored on computers.[100]

Paper documents may also be characterized as ephemeral.[101] Telephone messages, meeting notes, desktop calendar entries, drafts, photocopies, Post-It Notes, and a myriad of other documents are created in enormous quantities in government, business, and daily life.[102] Beyond their immediate business purpose, ephemeral paper documents have little or no value and are routinely disposed of with no legal consequence.[103] In professional records management circles, these documents are considered non-records, and employees of well-managed enterprises are instructed to dispose of them in short order.[104] Absent any specific legal, regulatory, or statutory records retention requirement, businesses are free to do so.[105]

However, paper ephemera are not always disposed of immediately or properly, and accumulate in all organizations.[106] If it is relevant

---

99. Hon. Lee H. Rosenthal & Hon. James C. Francis IV, Panel Discussion, *Managing Electronic Discovery: Views from the Judges*, 76 FORDHAM L. REV. 1, 19 (2007) ("The other area where this becomes a major problem is in what is called ephemeral or transitory data."); Conrad J. Jacoby, *E-Discovery Update—Discovery of Ephemeral Digital Information*, LAW LIBRARY RESOURCE EXCHANGE, July 27, 2007, http://www.llrx.com/columns/fios19.htm.

100. *See, e.g.*, RONALD. J. HEDGES, DISCOVERY OF ELECTRONICALLY STORED INFORMATION: SURVEYING THE LEGAL LANDSCAPE 103–04 & n.44 (BNA Books 2007) (discussing oscilloscope readings and Instant Messaging); Jacoby, *supra* note 99 (referring to "active data stored in volatile memory").

101. Collecting and trading historic ephemera, such as political tracts, advertising handbills, and theater programs, is a lucrative business. On January 8, 2008, the category "Ephemera" on the popular auction web site eBay listed 3,471 items for sale. http://ebay.com (follow "Collectibles" hyperlink; then follow "Paper" hyperlink; then follow "Ephemera" hyperlink).

102. *See* Lyman & Varian, *supra* note 8, at 5 ("[A]nnually each of the inhabitants of North America consumes 11,916 sheets of paper . . . .").

103. THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE iv (Charles R. Ragan et al., eds., Sept. 2005), http://www.thesedonaconference.com/content/miscFiles/TSG9_05.pdf.

104. *See generally* Robert L. Sanders, *Record, Pre-Record, Non-Record?*, ARMA RECORDS MGMT. Q., July 1994 http://findarticles.com/p/articles/mi_qa3691/is_199407/ai_n8710568/pg_1.

105. THE SEDONA GUIDELINES, *supra* note 103, at iv. Guideline 3 states that "[a]n organization need not retain all electronic information ever generated or received." *Id.*

106. *See* Laura Ariane Miller, W. Scott O'Connell & J.P. Ellison, *Document Retention Policies Revisited*, FINDLAW, June 26, 2003, http://library.findlaw.com/2003/

and non-privileged,[107] paper ephemera may be subject to discovery as a document within the meaning of Federal Rule of Civil Procedure 34,[108] and therefore may be subject to the common law duty of preservation if litigation is reasonably anticipated.[109] If litigation is anticipated, even a well-intentioned decision to clean up the files of ephemera could constitute spoliation.[110]

Computer-based information systems generate a tremendous volume and variety of electronic communications and documents, many of which have become commonplace in discovery.[111] There is no dispute that email comes within the definition of a document under Rule 34; email has been routinely requested and produced in discovery for many years prior to the December 1, 2006 amendment to Rule 34 that explicitly incorporated electronically stored information within the scope of document discovery.[112] Many organizations depend on email communications as much as they depended on paper correspondence and memoranda for communications in the past, and they may treat email as a record in their records management policies.[113] Other organizations may treat email as ephemeral non-records, with very short retention policies.[114] Email messages may be deleted from the system (or otherwise rendered inaccessible to the user) within days of receipt, if the

---

Jun/26/132835.html; *cf.* Sanders, *supra* note 104, at ¶ 7 ("For example, in dealing with paper records, it has been easy to prove that the presence of inactive records in active files wastes valuable office space.").

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

108. FED. R. CIV. P. 34(a)(1)(A).

109. *Zubulake IV*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003).

110. *See, e.g.*, Rambus, Inc., v. Infineon Techs. AG, 220 F.R.D. 264, 280 (E.D. Va. 2004) (ruling plaintiff's corporate-wide "Shred Day" on the eve of filing patent infringement suit constituted spoliation).

111. BARBARA J. ROTHSTEIN, RONALD J. HEDGES & ELIZABETH C. WIGGINS, MANAGING DISCOVERY OF ELECTRONIC INFORMATION: A POCKET GUIDE FOR JUDGES 15 (2007), *available at* http://www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf.

112. *See* HEDGES, *supra* note 100, at 46–51; *see, e.g.*, Sattar v. Motorola, Inc., 138 F.3d 1164, 1171 (7th Cir. 1998) (allowing Motorola to provide email data to Sattar by transferring the requested data onto a hard drive).

113. *See* Sarah D. Scalet, *The Seven Deadly Sins of Record Retention,* CSO, July 1, 2006, http://www.csoonline.com/read/070106/record-retention.html; *see also The Sedona Conference Commentary on Email Management: Guidelines for the Selection of Retention Policy*, 8 SEDONA CONFERENCE J. 239, 239, 244–45 (2007), *available at* http://www.thesedonaconference.org/content/miscFiles/Commentary_on_Email_Management___revised_cover.pdf [hereinafter *Sedona Conference*].

114. *See* Scalet, *supra* note 113; *see also Sedona Conference*, *supra* note 113, at 239, 242, 244–45, 249.

messages are not moved into designated files or if the user's allocated email storage space is exceeded.[115] As with paper ephemera, the law allows such strict policies.[116] However, "[o]nce a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents."[117] Because email has become so essential to routine business operation, and therefore highly relevant in litigation, organizations have invested tremendous resources in developing systems to better manage email, reduce email volume, and meet preservation requirements.[118]

Instant Messaging (IM) is another form of computer-mediated communication, common in business and daily life,[119] but rarer in discovery.[120] While similar in some respects to email, IMs are more likely to be considered ephemeral by users and system administrators, and therefore fall outside the records management policy.[121] Email is more analogous to a physical document, in that it is composed, sent by the author (and simultaneously saved on the author's computer), routed via servers and networks to the recipient, and stored until retrieved by the recipient.[122] IM, however, is a virtually simultaneous transmission, during which the author composes a message on one computer that appears on the screen of the recipient's computer, and when the recipient closes the communication, the IM conversation disappears.[123] Unlike email, IM users do not exchange electronic documents, but rather engage in an electronic conversation, analogous to a telephone call. Behind the scenes, however, much

115. *See, e.g.*, Broccoli v. Echostar Commc'ns Corp., 229 F.R.D. 506, 510 (D. Md. 2005) (noting employee email was "deleted" after seven days, and "deleted" emails purged from the system after fourteen days).

116. *Id.* ("[U]nder normal circumstances, such a policy may be a risky but arguably defensible business practice undeserving of sanctions.").

117. *Zubulake IV*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003).

118. *See, e.g.*, *Sedona Conference, supra* note 113, at 239, 242.

119. U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2003, at 11–13 (2005), *available at* http://www.census.gov/prod/2005pubs/p23-208.pdf.

120. *See, e.g.*, Children's Legal Servs. v. Kresch, 2007 WL 4098203 No. 07-CV-10255 (E.D. Mich. Nov. 16, 2007) (denying unduly broad request for instant messages).

121. *See infra* note 124 and accompanying text (describing the transient, therefore ephemeral, nature of instant messages).

122. Marshall Brain & Tim Crosby, *How Email Works*, http://communication.howstuffworks.com/email.htm/printable (last visited Jan. 24, 2008); *see also Sedona Conference*, *supra* note 113.

123. *See, e.g.*, Leslie Walker, *Instant Messaging Is Growing Up, Going to Work*, WASH. POST, Sept. 2, 2004, at E01, *available at* http://www.washingtonpost.com/ac2/wp-dyn/A54261-2004Sep1.html.

more is happening with IM, and that activity is what calls the ephemeral nature of IM into question.[124]

Fundamentally, all computer activity, from simple word processing to Internet communications, is the result of the input of digital code, processing of that code by chips and software following a complex set of mathematical instructions, and the output of resulting digital code in a form we perceive.[125] Using an IM application, for instance, a sender might type "ephemeral data" on the keyboard. The action of pressing the keys "e-p-h-e-m-e-r-a-l- -d-a-t-a" is translated by the keyboard input software into a binary code, specifically:

01000101 01010000 01001000 01000101 01001101
01000101 01010010 01000001 01001100 00100000
01000100 01000001 01010100 01000001.[126]

The computer's graphics processor, in conjunction with the IM application, quickly transforms this binary code into the words "ephemeral data" which appear on the sender's screen in the appropriate place, with the appropriate font and color.[127] In what appears to be a simultaneous action, the IM application sends the same binary code, embedded in a digital packet, via a network, to the recipient's computer.[128] There the recipient's computer, graphics processor, and IM application recreate the same image of the words "ephemeral data" on the recipient's screen, where it remains until it is scrolled away by additional words, or the IM session is terminated. But although the image is gone from the screen, the tracks of this communication remain.[129] At each step of the process, the binary code (as well as other data generated by the process) was copied to one or more virtual workbenches where the appropriate software application transformed the code to send to the next step.[130] At the

124. *Id.*; *see also* Mike Musgrove, *Instant Messages, Lingering Paper Trail; HP, Foley Cases Illustrate Risk*, WASH. POST, Oct. 6, 2006, at A61 (explaining that individuals erroneously believe that IM conversations are not recorded).

125. Marshall Brain, *How Bits and Bytes Work*, http://computer.howstuffworks.com/bytes.htm/printable (last visited Jan. 22, 2008) (describing how information is encoded into a computer's memory by binary code).

126. *Id.* *See also* DANIEL ZWILLINGER, STANDARD MATHEMATICAL TABLES AND FORMULAE 260 (2003) (providing a table for translating English text into binary code).

127. Brain, *supra* note 125 and accompanying text.

128. *See, e.g.*, ENCYCLOPEDIA OF COMPUTER SCIENCE 1130 (Anthony Ralston, Edwin Reilly, David Hemmendinger eds., 4th ed. 2000).

129. *See* Musgrove, *supra* note 124 and accompanying text.

130. *See supra* notes 124–25 and accompanying text.

speed of light, these strings of digital code replicate themselves from one place to another, both inside the computer and on the network.[131]

In simple terms, IM is the 21st century version of the 19th century telegraph. At the railway station in Deadwood the sender would have the telegraph operator tap the word "ephemeral" to the recipient in Tombstone in the digital language of the day, Morse code:

. .--. .... . -- . .-. .- .-..[132]

The operator at Tombstone would hear the taps, transcribe the code, and deliver it to the recipient. While the sender might not have written anything and the recipient might have destroyed the message upon receipt, written records of the transmission were likely made by the operators at both ends of the transmission in the routine course of their duties and kept for some period of time. The correspondents in Deadwood and Tombstone could have exchanged letters—paper ephemera. By doing so, they would likely know that they were creating artifacts they could manage. But they chose instead to engage in a mediated transmission, which routinely generated copies of their transmission over which they had no control.[133]

Similarly, we are accustomed to thinking of computer operations, the digital code that we perceive as text, images, and sounds, as a stream of information; although on close inspection the stream is actually a series of pools and eddies.[134] The pools and eddies of the digital stream have various names (memory, RAM, virtual memory, swap or SWP files, file cache, buffer, printer spool, Internet cache), various characteristics, and varying levels of accessibility. Some of these sources, like RAM, are considered "volatile"; they are erased if the power is shut down or the system rebooted.[135] Other sources, such as an Internet cache, reside on the hard drive and are considered both persistent and ephemeral, like quiet pools of data inviting

131. *Id.*

132. ZWILLINGER, *supra* note 126, at 260 tbl.3.6.4.

133. Recognizing this problem, several states adopted statutes regulating the disclosure of telegraph messages during the 19th century, which Congress debated as early as 1877. *See Privacy of the Telegraph*, N.Y. TIMES, Jan. 6, 1877, at 1, *available at* http://query.nytimes.com/mem/archive-free/pdf. Later, Congress developed statutory prohibitions against disclosure of wire transmissions, some of which have carried over into protections for digital communications, such as the Electronic Communications Privacy Act, 18 U.S.C. §§ 2701–2712.

134. *See supra* note 126 and accompanying text (illustrating how digital information is grouped in sections of eight pieces of binary code).

135. Apple Computer, Inc. v. Franklin Computer Corp., 714 F.2d 1240, 1243 (3d Cir. 1983).

reflection.[136] Still other sources, such as swap files or residual data from deleted files, are old and not likely to be accessed, like stagnant swamps full of debris.[137]

The common feature among all types of ephemeral data is that they are created by the computer system as a temporary byproduct of digital information processing, not consciously created, viewed, or transmitted by the user.[138] While the ephemera are neither apparent nor routinely accessed by the user, they may be essential to the efficient operation of the information system and may be accessible to technicians and system administrators.[139] The data are ephemeral to the extent that they are not intended to be stored for any length of time beyond their operational use and may be susceptible to being overwritten at any point during the routine operation of the information system.[140] However, under the holding of *Columbia Pictures*, ephemeral data may be considered electronically stored information:[141] they are "fixed in a tangible medium of expression . . . sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration";[142] therefore, they are "within the scope of discoverable information under Federal Rule of Civil Procedure 34."[143]

Law enforcement has long recognized the value of ephemeral data in criminal investigations.[144] Search warrants for ESI routinely request the seizure of whole computer systems, so that volatile

136. Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 640 (E.D. Pa. 2007).

137. THE SEDONA CONFERENCE, THE SEDONA PRINCIPLES: BEST PRACTICES RECOMMENDATIONS & PRINCIPLES FOR ADDRESSING ELECTRONIC DOCUMENT PRODUCTION, 50 cmt. 9.b (2nd ed. 2007), http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf [hereinafter SEDONA PRINCIPLES].

138. *See, e.g.*, MAI Sys. Corp. v. Peak Computer, Inc., 911 F.2d 511, 518 (9th Cir. 1993) (stating an example of automatic processing is the operating system loading into RAM when the computer is turned on).

139. *See, e.g.*, *Apple Computer*, 714 F.2d at 1243 (explaining the interaction between the CPU, the code it reads, and the storage medium, RAM).

140. *Id.* at 1243 n.3.

141. Columbia Pictures Inc. v. Bunnell, 245 F.R.D. 443, 446–47 (C.D. Cal. 2007).

142. *Id.* at 448 (quoting *MAI Sys. Corp.*, 991 F.2d at 517–18).

143. *Id.*

144. *See, e.g.*, U.S. v. Meek, 366 F.3d 705, 720, 722 (9th Cir. 2004) (sustaining the use of Internet chat room conversations to catch online predators who are trying to induce minors to engage in sexual activity).

computer memory found on the hard drive can be preserved.[145] Forensic analysis of a computer system starts with the creation of a bitstream image of the computer, a process developed to preserve the ephemeral data and non-apparent system files that may be evidence of criminal activity or data that sophisticated cyber criminals have attempted to hide.[146] Developing procedures to preserve ephemeral data in criminal investigations is a priority in law enforcement.[147]

But civil discovery is not conducted as a criminal investigation. Absent a showing that potential evidence is likely to be destroyed, thus prejudicing the requesting party's case, a court will not authorize the requesting party to have direct access to computer hard drives or the seizure of evidence.[148] The parties are expected to identify and implement the steps necessary to fulfill their data preservation

145. *See, e.g.*, COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, SEARCHING & SEIZING COMPUTERS & OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, app. F.II.D.1.b (2002), http://www.cybercrime.gov/s&smanual2002.htm ("Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover 'hidden,' erased, compressed, encrypted or password-protected data . . . . Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted.").

146. *See generally* NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, FORENSIC EXAMINATION OF DIGITAL EVIDENCE: A GUIDE FOR LAW ENFORCEMENT 15 (2004), *available at* http://www.ncjrs.gov/pdffiles1/nij/199408.pdf.

147. *See, e.g.*, John Malcolm, Deputy Assistant Attorney General, U.S. Dep't of Justice, Remarks Before the OECD-APEC Global Forum (Jan. 15, 2003), *available at* http://www.usdoj.gov/criminal/cybercrime/JGM_OECD.htm ("Because of the speed and sophistication of cyberattacks and the ephemeral nature of the evidence left behind, law enforcement officials must get timely access to information and to traffic data . . . ."); *see also* G8 GOVERNMENT/INDUSTRY CONFERENCE ON HIGH-TECH CRIME TOKYO, REPORT OF WORKSHOP 2: DATA PRESERVATION (2001), http://www.mofa.go.jp/policy/i_crime/high_tec/conf0105-5.html ("[H.]6. Examine the applicability of preservation requests to transient or 'ephemeral' data in order to provide network 'trap and trace' information (real-time or historical) where 'ephemeral' data is data held within the network for network management, such as network address translation tables and routing tables.").

148. *In re* Ford Motor Co., 345 F.3d 1315, 1316 (11th Cir. 2003) (ruling plaintiff was not entitled to direct, unlimited access to defendant's computer database); Balfour Beatty Rail, Inc. v. Vaccarello, No. 3:06-cv-551-J-20MCR, 2007 WL 169628, at *3 (M.D. Fla. Jan. 18, 2007) (ruling plaintiff may not inspect the defendant's computer without good cause).

obligations;[149] the standard they must meet is reasonableness, not perfection.[150] As suggested by the magistrate judge in the *Columbia Pictures* case, the duty of preservation is tempered by proportionality considerations, analogous to those in discovery under Rule 26(b)(2)(C).[151]

IV. OTHER COURTS CONSIDER EPHEMERAL DATA PRESERVATION

The United States District Court, Central District of California was not the only court to consider the preservation of ephemeral data in 2007. In *Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey,*[152] the United States District Court, Eastern District of Pennsylvania addressed whether the failure to preserve automatically deleted data merited spoliation sanctions in a copyright case.[153] In *Healthcare Advocates*, the defendant was a law firm that had successfully represented clients in an unrelated case against Healthcare Advocates.[154] The firm used an Internet resource during discovery to locate pages from Healthcare Advocates's web site as the pages would have appeared on specific dates in the past and printed images of those web pages to use in the litigation.[155] Later, Healthcare Advocates sued Harding, Earley, Follmer & Frailey for copyright infringement for accessing and printing the web pages[156] and sought sanctions for spoliation, claiming that the firm violated its duty to preserve the cache files the computer would have temporarily created while firm employees were viewing and printing Healthcare Advocates's old web pages.[157]

---

149. SEDONA PRINCIPLES, *supra* note 137, at ii princ. 6 ("Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information.").

150. *Id.* at ii Principle 5 ("The obligation to preserve electronically stored information requires reasonable and good faith efforts to retain information that may be relevant to pending or threatened litigation. However, it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information."); *see also Zubulake IV,* 220 F.R.D. 212, 218 (S.D.N.Y. 2003) (referencing the duty to preserve back-up tapes).

151. Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *31–35 (C.D. Cal. May 29, 2007).

152. 497 F. Supp. 2d 627 (E.D. Pa. 2007).

153. *Id.* at 639.

154. *Id.* at 630.

155. *Id.* at 630–31.

156. *Id.* at 633.

157. *Id.* at 640 ("A cache file is a temporary storage area where frequently accessed data can be stored for rapid access. When a computer accesses a web page, it will

Cache is a common form of ephemeral data that is generally less volatile and more accessible than RAM.[158] Cache is created on the computer's hard drive whenever a user visits a web page.[159] Elements of the web page are temporarily stored in cache files, so that when a user revisits a page, it can be quickly recomposed on the screen without having to retrieve the data from the remote web server.[160] This increases the speed and efficiency of web surfing sessions,[161] but storing cache can result in the accumulation of a large volume of data in the computer's hard drive.[162] Users can limit the size of their cache[163] manually or periodically delete cache altogether.[164] In *Healthcare Advocates*, the cache files temporarily stored on the defendant's hard drive were automatically deleted before the plaintiff formally requested the electronically stored information.[165]

In determining whether sanctions against the defendant for failing to preserve the cache were appropriate, the court applied a three-factor test: "(1) the degree of fault of the party who altered or destroyed the evidence, (2) the degree of prejudice suffered by the opposing party, and (3) whether there is a lesser sanction that will avoid substantial unfairness to the opposing party . . . ."[166] The court found that the law firm's fault level for the loss of the cache was minor because "the Harding firm did not affirmatively destroy the evidence."[167] The degree of prejudice suffered by the plaintiffs from being unable to view the cache files was minor, because the plaintiffs were "able to piece together what occurred from the data available."[168] Finally, the court believed that no sanction would be

---

sometimes store a copy of the web page in its cache in case the page is needed again.").

158. *Cf. id.* at 650.

159. *See id.* at 640.

160. *Id.*

161. *See id.*

162. Ty E. Howard, *Don't Cache Out Your Case: Prosecuting Child Pornography Possession Laws Based on Images Located in Temporary Internet Files*, 19 BERKELEY TECH. L.J. 1227, 1230–31 (2004).

163. *See* Microsoft Help and Support, How to Adjust Cache Size for Temporary Internet Files, http://support.microsoft.com/kb/155353/en-us (last visited Feb. 14, 2008).

164. *See* Microsoft Help and Support, How to Delete the Contents of the Temporary Internet Files Folder, http://support.microsoft.com/kb/260897/en-us (last visited Feb. 14, 2008).

165. *Healthcare Advocates*, 497 F. Supp. 2d at 641.

166. *Id.* at 639.

167. *Id.* at 641.

168. *Id.*

necessary because "[t]he Harding firm did not purposefully destroy evidence."[169]

The court in *Healthcare Advocates* was not faced with the question of whether to order the preservation of cache, but whether the failure to preserve cache was a sanctionable violation of the duty of preservation.[170] In *Healthcare Advocates*, this analysis is retrospective and based on the fact that other evidence, in the form of the printed screenshots and testimony of the employees who performed the web searches, was readily available to the plaintiff.[171] In *Columbia Pictures*, this element is prospective and based on the relevance and unique nature of the data requested.[172] While the two courts necessarily applied different analyses,[173] both cases share an important element: the degree of prejudice posed to the requesting party by the failure to preserve ephemeral data.[174]

Commentators have pointed to other federal court decisions involving ephemeral data as instructive.[175] *Convolve, Inc. v. Compaq Computer Corp.*[176] was a patent infringement action involving computer hard drive technology.[177] The plaintiff alleged that the defendant infringed on plaintiff's patented electronic device when the defendant used "an oscilloscope to evaluate how closely the actual performance matched the ideal wave form, and adjusted the parameters accordingly . . . repeat[ing] this process multiple times until satisfactory results were achieved."[178] However, there were no records kept of the results of each of the iterations of the tuning process.[179] The plaintiff alleged that the failure to preserve images of the oscilloscope readings or saving the data violated a duty of

169. *Id.* at 641–42.
170. *Id.* at 639.
171. *Id.* at 630–32.
172. Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *13 (C.D. Cal. May 29, 2007).
173. *See id.* at *7–13.
174. *Compare id.* at *13 (balancing the burden and benefit of the proposed discovery) *with Healthcare Advocates*, 497 F. Supp. 2d at 639–41 (balancing the proposed discovery with the available data).
175. Shira A. Scheindlin & Kanchana Wangkeo, *Electronic Discovery Sanctions in the Twenty-First Century*, 11 MICH. TELECOMM. & TECH. L. REV. 71, 80–84 (2004).
176. 223 F.R.D. 162 (S.D.N.Y 2004).
177. *Id.* at 164.
178. *Id.* at 176.
179. *Id.*

preservation and constituted spoliation.[180] The court rejected this contention, saying:

> [T]he preservation of the wave forms in a tangible state would have required heroic efforts far beyond those consistent with Seagate's regular course of business. To be sure, as part of a litigation hold, a company may be required to cease deleting e-mails, and so disrupt its normal document destruction protocol. But e-mails, at least, normally have some semi-permanent existence. They are transmitted to others, stored in files, and are recoverable as active data until deleted, either deliberately or as a consequence of automatic purging. By contrast, the data at issue here are ephemeral. They exist only until the tuning engineer makes the next adjustment, and then the document changes. No business purpose ever dictated that they be retained, even briefly.[181]

The court then commented that the situation might be analogous to the use of Instant Messaging, but "[t]here the question may be a closer one both because at least some Instant Messenger programs have the capability, like e-mail, of storing messages . . . ."[182]

The court in *Malletier v. Dooney & Bourke, Inc.*[183] was faced with a similar request from a plaintiff that sanctions be imposed for failing to preserve ephemeral data.[184] The case was brought by the fashion design house Louis Vuitton against the defendant for selling handbags that infringed on the Vuitton trademark.[185] The defendant maintained a web site that featured a customer-relations chat room, and the plaintiff alleged that chat room conversations may have been relevant to its trademark infringement claim.[186] Web-based chat room conversation is like IM for multiple participants—the conversation appears on the participants' screens simultaneously while all are logged on to the same site.[187] The data that constitutes the conversation is transmitted synchronously and perceived by the

180. *Id.* at 175–77.
181. *Id.* at 177.
182. *Id.* at 177 n.4.
183. No. 04 Civ. 5316, 2006 WL 3851151 (S.D.N.Y. Dec. 22, 2006).
184. *Id.* at *1.
185. *See id.*
186. *Id.*
187. *See* Matthew T. Rollins, *Examination of the Model Rules of Professional Conduct Pertaining to the Marketing of Legal Services in Cyberspace*, 22 J. MARSHALL J. COMPUTER & INFO. L. 113, 117 (2003).

participants in real time, unlike with email where messages are composed and transmitted by the senders as discreet files, to be retrieved and opened by each recipient.[188] The court noted that the chat room did not open until after the allegedly infringing sales had ceased, so that any conversations were unlikely to be relevant.[189] Moreover, the defendant did not have the capacity to record the chat room conversations until eighteen months after the chat room opened, and then it could keep transcripts for only two weeks.[190] Declining to find any basis for sanctioning the defendant, the court characterized the plaintiff's motion as "akin to a demand that a party to litigation install a system to monitor and record phone calls coming in to its office on the hypothesis that some of them may contain relevant information. There is no such requirement, and in this case no indication that defendant acted improperly in this regard."[191]

The courts in *Convolve* and *Malletier* addressed the question of sanctioning parties for their retrospective failures to preserve data, but not the question of issuing prospective preservation orders.[192] The intertwined considerations of whether there is any on-going business purpose for the data and whether a mechanism exists for the routine capture and preservation of the data were central to both courts' holdings that the failure to preserve ephemeral oscilloscope data did not warrant sanctions.[193] The considerations were central to the *Columbia Pictures* holding that an order for the preservation of ephemeral Server Log Data was appropriate.[194]

This leads us to an exploration of the factors that parties should consider when evaluating whether a duty to preserve ephemeral data exists, and if so, what steps a court would consider reasonable and proportionate under the circumstances.[195]

---

188. Frank G. Evans et al., *Enhancing Worldwide Understanding Through ODR: Designing Effective Protocols for Online Communications*, 38 U. TOL. L. REV. 423, 432 n.15 (2006) (citing Janet Sternberg, *It's All in the Timing: Synchronous Versus Asynchronous Computer-Mediated Communication*, Mar. 21, 1998, www.pages.nyu.edu/~js15/p-time.htm).

189. *Malletier*, 2006 WL 3851151, at *2.

190. *Id.*

191. *Id.*

192. Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 176–77 (S.D.N.Y. 2004); *Malletier*, 2006 WL 3851151, at *3.

193. *Convolve*, 223 F.R.D at 175–77; *Malletier*, 2006 WL 3851151, at *2–3.

194. Columbia Pictures Indus. v. Bunnell, No. CV 06-1093FMCJCX, 2007 WL 2080419, at *13–14 (C.D. Cal. May 29, 2007).

195. *See infra* Part V.

V. RESOLVING THE DILEMMA OF EPHEMERAL DATA

The courts in *Healthcare Advocates*, *Convolve,* and *Malletier,* considering different forms of ephemeral data, declined to sanction the parties for failing to preserve Internet cache, oscilloscope readings, and chat room conversation, respectively.[196] The court in *Columbia Pictures* held that the definition of discoverable electronically stored information under the 2006 amendments to the Federal Rules of Civil Procedure can extend, in particular cases, to data from sources that are considered ephemeral, such as RAM.[197] Although the court did not sanction the defendant for failing to preserve relevant data derived from RAM, it imposed an obligation, on a going-forward basis, on the defendant to use readily available technology to preserve relevant information that is momentarily stored in the computer's RAM.[198]

The plain language of Rule 37(e) appears to prevent the imposition of sanctions, "[a]bsent exceptional circumstances," for the failure to preserve ephemeral data, which by its nature, can be lost in the routine operation of electronic information systems.[199] We have not seen a reported case in which sanctions have been imposed explicitly for failing to preserve ephemeral data.[200] But future litigants may wonder what those exceptional circumstances are that give rise to a duty to preserve ephemeral data and, in turn, give rise to the possibility of sanctions for failing to preserve ephemeral data.

The following are some questions that litigants may ask themselves to assess the scope of their duty to preserve ephemeral data, or ask the opposing party to assess the need for a preservation agreement addressing ephemeral data.

---

196. *See* Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 641 (E.D. Pa. 2007); *Convolve*, 223 F.R.D. at 176; *Malletier*, 2006 WL 3851151, at *3.

197. *Columbia Pictures*, 2007 WL 2080419, at *5.

198. *Id.* at *14.

199. FED. R. CIV. P. 37(e) ("Failure to Provide Electronically Stored Information. Absent 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.").

200. There are many cases in which parties have been sanctioned for failing to preserve entire hard drives, which would have the effect of destroying ephemeral data as well as more persistent and otherwise accessible forms of electronically stored information. *See, e.g.*, Leon v. IDX Sys. Corp., 464 F.3d 951, 956–57 (9th Cir. 2006); Paramount Pictures Corp. v. Davis, 234 F.R.D. 102, 113 (E.D. Pa. 2005); Advantacare Health Partners v. Access IV, No. C 03-04496 JF, 2004 WL 1837997, at *1, *11 (N.D. Cal. Aug. 17, 2004).

A. Is the Ephemeral Data Uniquely Relevant to Pending or Anticipated Litigation?

The duty of preservation does not encompass everything that might possibly be relevant. In particular, the duty does not extend to duplicative material.[201] To the extent that a particular source of ephemeral data is unique—that is, likely to contain highly relevant information not duplicated in more accessible, persistent form elsewhere—a duty to take reasonable steps to preserve that ephemeral communication may be necessary. In *Columbia Pictures*, the court pointed out that the RAM contained Server Log Data that was central to the plaintiff's claims and not replicated in any more persistent form.[202]

However, most forms of ephemeral data are the building blocks and residual by-products of more persistent forms of electronically stored information. For example, swap files consist largely of data left over from the creation and editing of active files, such as word-processing documents;[203] printer spool files are copies of documents ordinarily composed and saved on the computer hard drive, but stored temporarily on the printer's operating system to save time during the printing operation.[204] In *Healthcare Advocates*, the ephemeral Internet cache at issue consisted of copies of web pages, the byproduct of the process of downloading and viewing the pages, which were printed and preserved in paper form.[205] Therefore, unless the requesting party has taken steps to put the responding party on notice of the relevance and unique nature of the ephemeral data it plans to request, the responding party could make a reasonable assessment that the data that can be derived from ephemeral sources is more readily available from more persistent ESI, such as the documents themselves.

---

201. *Zubulake IV*, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) (holding that parties need not preserve every shred of paper, every email or electronic document, and every back-up tape).

202. *Columbia Pictures*, 2007 WL 2080419, at *4.

203. WEBSTER'S ONLINE DICTIONARY, DEFINITION: SWAP FILE, http://www.websters-online-dictionary.org/definition/swap+file (last visited Feb. 14, 2008).

204. WEBSTER'S ONLINE DICTIONARY, DEFINITION: SPOOL, http://www.websters-online-dictionary.org/definition/SPOOL (last visited Feb. 14, 2008) (defining spool as "transfer data intended for a peripheral device (usually a printer) into temporary storage").

205. Healthcare Advocates, Inc. v. Harding, Earley, Follmer & Frailey, 497 F. Supp. 2d 627, 640 (E.D. Pa. 2007).

B. *How Is the Ephemeral Data Treated in the Ordinary Course of Business?*

The way information is treated in the ordinary course of business indicates its potential relevance to litigation and the foreseeability that it will be relevant to reasonably anticipated litigation. It is an important factor in considering whether a duty exists to preserve that information in pending or reasonably anticipated litigation.

Most litigation arises from circumstances that occur in the ordinary course of business. Most discovery involves facts that, if documented, were documented in the ordinary course of business. One can easily imagine instances where the facts related to reasonably anticipated litigation do not arise from the ordinary course of business (e.g., a workplace accident giving rise to a lawsuit for injuries) or instances where a business keeps information in persistent form that it does not need to conduct business (e.g., outdated disaster recovery backup tapes or caches of employee email). However, in most cases there is a close correlation between the information kept in the ordinary course of business and the information that will likely be relevant to litigation arising from that business. Conversely, there is a much lower correlation between information that has been treated as ephemeral in the ordinary course of business and information likely to be relevant to litigation arising from that business. Unless the requesting party has taken steps to put the responding party on notice of the relevance and unique nature of the ephemeral data it plans to request, the responding party could make a reasonable assessment that the preservation of more persistent forms of ESI will fulfill its obligations.

In *Healthcare Advocates* and *Convolve*, the courts made it clear that there was no reason for the parties to keep ephemeral data not at issue in the ordinary course of business, and therefore the courts were hesitant to find a duty of preservation after the fact.[206]

Likewise in *Columbia Pictures*, the court found that the ephemeral data in question was being captured and used in the ordinary course of business by the defendant[207] and was routinely captured and used by similarly situated companies.[208] Even so, it did not sanction the defendant for its failure to preserve relevant ephemeral data.[209]

---

206. *Id.* at 640–42; Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 177 (S.D.N.Y. 2004).

207. *Columbia Pictures*, 2007 WL 2080419, at *3.

208. *Id.* at *2–3.

209. *Id.* at *1.

C. Are There Undue Costs or Burdens Associated with the Preservation of the Ephemeral Data?

In discovery, the court is allowed to place conditions on the conduct of discovery or limit the scope of discovery altogether, based on considerations of fairness and proportionality embodied in the Rules.[210] However, no reported decision has explicitly extended the proportionality considerations of Rule 26(b)(2) of the Federal Rules of Civil Procedure to the preservation of electronically stored information. This concept is consistent with the Sedona Principles[211] and has been advanced by at least one commentator.[212] However, the decision to limit discovery is made by a court upon consideration of a motion for a protective order or a motion to compel. Both parties are required to have met and conferred to resolve their dispute prior to filing their motions.[213] The decision to preserve data is often made unilaterally by a party early in the litigation or before litigation has been filed, usually before any meaningful exchange with the opposing party.

Unless the requesting party has taken steps to put the responding party on notice of the relevance and unique nature of the ephemeral data it plans to request, the responding party could make a reasonable decision, after balancing the projected burden and cost of preservation against the likelihood that the ephemeral data will be subject to discovery, to forego preservation efforts, particularly since ephemeral data is seldom relevant, unique, or easily preserved. In close cases, however, it would be dangerous to use proportionality considerations to justify a unilateral decision not to take steps to preserve ephemeral data. Ideally, the party with control over the data would use proportionality considerations to open a dialogue with the opposing party to limit the scope of and shift the costs of preservation.

D. Are There Readily Available Technologies to Capture and Preserve the Ephemeral Data?

In *Convolve*, there was no simple method proposed to capture the ephemeral oscilloscope readings at issue.[214] In *Malletier*, the

---

210. FED. R. CIV. P. 26(b)(2), (c).

211. SEDONA PRINCIPLES, *supra* note 137, at ii princ. 8.

212. Conor R. Crowley, *A Shifting View of Preservation: How Ephemeral Are Current Views on Shifting Costs of Preservation?*, DIGITAL DISCOVERY & E-EVIDENCE, Jan. 1, 2008, at 9.

213. FED. R. CIV. P. 26(c)(1), 37(a)(2)(A).

214. Convolve, Inc. v. Compaq Computer Corp., 223 F.R.D. 162, 177 (S.D.N.Y. 2004).

testimony established that the option to record the Internet chat room conversations at issue was not exercised until more than two years after the relevant time frame when the conversations would have occurred.[215] The court considered this in holding that the defendants had no duty to preserve the ephemeral data in question.[216]

In contrast, in *Columbia Pictures* there was testimony that the Internet server used by the defendant had an option to capture the ephemeral data and migrate it to a database for analysis and use.[217] Although a business decision was made by the defendant not to implement that feature of the server, the technology to preserve the ephemeral data at issue was readily available and did not represent an undue burden or cost, a factor in the court's decision to order preservation of the ephemeral data on a going-forward basis.[218]

VI. THE IMPORTANCE OF THE MANDATE TO CONFER ON PRESERVATION ISSUES

Rule 26 of the Federal Rules of Civil Procedure mandates that the parties confer before the Rule 16(b) pretrial scheduling conference with the court to discuss and attempt to reach agreement on "any issues about preserving discoverable information."[219] For the requesting party, the preservation of ephemeral data depends in large measure on clear notice that the data will be requested in discovery and a convincing argument that the ephemeral data is both relevant and unique. Absent those elements, a court is unlikely to find the exceptional circumstances necessary to impose sanctions on the responding party for the loss of ephemeral data under Rule 37(e) of the Federal Rules of Civil Procedure. For the responding party, a unilateral decision to forego preservation of ephemeral data is fraught with uncertainty. The courts have not expressly applied proportionality considerations analogous to Rules 26(b)(2)(C) and 26(c) of the Federal Rules of Civil Procedure to the context of preservation; if they were to do so, courts would not automatically consider any cost or burden associated with the preservation of ephemeral data to be undue. The holding in *Columbia Pictures* demonstrates that at least one court was willing to order the preservation of ephemeral data in appropriate cases.

---

215. Malletier v. Dooney & Bourke, Inc., No. 04 Civ. 5316, 2006 WL 3851151, at *2 (S.D.N.Y. Dec. 22, 2006).

216. *Id.*

217. *Columbia Pictures*, 2007 WL 2080419, at *3.

218. *Id.* at *14.

219. FED. R. CIV. P. 26(f)(2).

The timing of the Rule 26(f) conference, however, presents a practical difficulty. It typically takes place approximately three weeks before the first Rule 16 scheduling conference with the judge.[220] Several weeks may have elapsed since the suit was initially filed, and the duty of preservation, as defined in common law, may have arisen well before the filing date, when litigation could have reasonably been anticipated. Ephemeral data, by its nature, is volatile and has a short life expectancy. By the time the parties sit down at the Rule 26(f) conference, the preservation issues surrounding ephemeral data may be moot: the requesting party will have missed the opportunity to request the data, and the fate of the responding party may already be sealed, if sanctions are later found to be warranted. The time to confer regarding the preservation of ephemeral data is as close as practicable to the time when either party believes the duty of preservation arises.[221]

An early conference of the parties can address the preservation of ephemeral data in a variety of ways and should not be regarded as an adversarial "winner-take-all" confrontation. A productive conference, or a series of collaborative exchanges, can result in an agreement that narrowly defines the scope of ephemeral data to be preserved, assuring the requesting party that the data they plan to request will be available and assuring the responding party that the cost of preservation will be reasonable, without the necessity of either party resorting to the court for resolution of these issues.

In addition to resolving the considerations of scope and cost, an early conference may also explore options for the wholesale preservation or destruction of ephemeral data. The author proposes the following options:

1. The use of a deposition under Rule 27(a)(3) of the Federal Rules of Civil Procedure prior to the filing of the suit to determine the extent and nature of ephemeral data that may fall within the scope of potential discovery, and lay the groundwork for its timely preservation.

220. FED. R. CIV. P. 26(f)(1).

221. *See, e.g.*, SEDONA CONFERENCE COMMENTARY, *supra* note 1, at 3 guideline 1 (providing an overview of the common law regarding the trigger point of the duty of preservation).

2. The use of statistical sampling[222] to determine the potential relevance of ephemeral data and to estimate the burden and cost of preservation.

3. The consideration and resolution of any potential problems of copyright, privacy, or privilege implicated by the preservation or ultimate production of ephemeral data. The determination of the most appropriate form or forms in which relevant ephemeral data should be preserved.

4. The consideration of alternatives to discovery of ephemeral data under Rule 34 of the Federal Rules of Civil Procedure to obtain the same information, such as expedited depositions under Rule 30 or interrogatories under Rule 33, thus reducing the scope, cost, and duration of ephemeral data preservation.

5. The possibility of shifting or sharing of the costs of preservation.

While such options are best explored at the outset of the litigation, they can be valuable cost-saving considerations for any stage of the litigation where the preservation of ephemeral data is an issue and may be raised at the Rule 16 pretrial scheduling conference or at a discovery status conference if the parties have reached an impasse regarding ephemeral data preservation.

VII. CONCLUSION

The *Columbia Pictures* case, a high-profile decision in the first year of the amended Federal Rules of Civil Procedure, established that ephemeral data is electronically stored information within the meaning of the Rules. The court ordered the defendant to preserve relevant ephemeral data for discovery on a going-forward basis, but declined to sanction the defendant for its previous failure to do so.[223] Other federal courts considering sanctions for the failure to preserve ephemeral data have also declined to do so. However, Rule 37(e) of the Federal Rules of Civil Procedure raises the possibility of sanctions for the loss of discoverable ephemeral data under

222. Zubulake v. UBS Warburg LLC (*Zubulake I*), 217 F.R.D. 309, 324 (S.D.N.Y. 2003) (permitting plaintiff to select a sample of backup tapes for restoration); *see also* McPeek v. Ashcroft, 202 F.R.D. 31, 34–35 (D.D.C. 2001) (ordering sampling of email from backup media).

223. *See supra* Part II.

"exceptional circumstances."[224] Thus, while the duty to preserve ephemeral data is very narrow, a duty may exist where the responding party is on notice that the ephemeral data is highly relevant and unique, and where the burden and cost of preserving the ephemeral data does not outweigh the value of its preservation. To ensure that reasonable steps are taken to preserve relevant ephemeral data, and to avoid sanctions, both the requesting and responding parties need to enter into early negotiations to come to an agreement regarding the preservation of the ephemeral data.

224. *See supra* notes 199–217 and accompanying text.