MEALEY'S LITIGATION REPORT
Cyber Tech & E-Commerce

The Duty To Preserve Data Stored Temporarily In Ram: Is The Sky Really Falling?

by
J. Alexander Lawrence

Morrison & Foerster
New York, New York

A commentary article reprinted from the February 2008 issue of Mealey's Litigation Report: Cyber Tech & E-Commerce

LexisNexis®

Commentary

The Duty To Preserve Data Stored Temporarily In RAM: Is The Sky Really Falling?

By
J. Alexander Lawrence

[Editor's Note: J. Alexander Lawrence is a partner in the litigation department of Morrison & Foerster, resident in New York. He practices principally in the areas of intellectual property, corporate governance, and complex commercial litigation. He is a member of the firm's Electronic Discovery Task Force. Mr. Lawrence can be contacted at ALawrence@mofo.com. Copyright 2008 by the author. Replies to this commentary are welcome.]

Recent district court decisions from the Central District of California give litigants yet another source of electronically stored information to consider when deciding what must be preserved.[1] Specifically, litigants will need to consider whether data stored temporarily in random access memory ("RAM") must be preserved. Although whether to preserve such data should be considered in all cases — including consideration of whether preserving such data is possible — preservation of data stored temporarily in RAM will likely be appropriate only in rare circumstances.

The decisions arose from a dispute brought by members of the Motion Picture Association of America ("MPAA") against operators of search engines that enable users to locate and download dot-torrent files that are alleged to facilitate the copying and distribution of copyrighted content over peer-to-peer networks. The MPAA members sought to compel the production of server log data generated by visitors to the websites. Objecting to producing the server log data, the defendants argued that the data was stored in RAM for no more than six hours before being overwritten and that they should not be required to preserve data that would not otherwise be retained. The defendants also argued that because they contracted with a third party to act as an intermediary and direct requests to defendants' server, the defendants did not have possession, custody, or control over the server log data showing the IP addresses of the users of the site.

Although recognizing that the server log data was stored only temporarily in RAM, a United States Magistrate Judge held that: (1) the data is relevant to the dispute, (2) the data constitutes electronically stored information under Rule 34, (3) the data is within the possession, custody or control of the defendants; (4) requiring the preservation and production of the data would not be tantamount to requiring the creation of new data, and (5) requiring the production of the server log data would not be unduly burdensome. In issuing the ruling, the Magistrate Judge emphasized that:

> [the] 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 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.

In an *amicus curiae* brief in support of the defendants' objections to the Magistrate Judge's order, the Electronic Frontier Foundation ("EFF") correctly noted that "[v]irtually every business in the United States relies on digital technologies for all kinds of communications. And virtually every function carried out by those technologies depends on and results in the temporary creation of RAM data that is not ordinarily retained."[2] The EFF noted that data stored in RAM can be found in all manner of digital devices, including personal computers, digital televisions, fax machines, and telephones using VOIP technology. The EFF further correctly recognized that data stored in RAM is ephemeral and is routinely being overwritten in the course of the operation of the digital device. The EFF went on to warn that "the Order threatens the actual and potential litigants with the specter of having to capture and compile an avalanche of RAM data that would otherwise be automatically overwritten in the ordinary course of computer processing."

Agreeing with the Magistrate Judge that data stored temporarily in RAM constitutes electronically stored information under Rule 34, the district court denied the defendants' motion to review the Magistrate Judge's decision. In response to the EFF's arguments regarding the far-reaching ramifications of the decision, the district court held:

> In response to amici's concerns over the potentially devastating impact of this decision on the record-keeping obligations of businesses and individuals, the Court notes that this decision does not impose an additional burden on any website operator or party outside of this case. It simply requires that the defendants in this case, as part of this litigation, *after* the issuance of a court order, and following a careful evaluation of the burden to these defendants of preserving and producing the specific information requested in light of its relevance and the lack of other available means to obtain it, begin preserving and subsequently produce a particular subset of the data in RAM under Defendants' control.

If the court had found a general obligation to preserve data stored temporarily in RAM, it would be a matter of concern. Preserving such data poses serious challenges and in many cases may be practically impossible. Typically, data stored in RAM is in a state of flux. Although it may be possible to take a snapshot of the data at a point in time, capturing all data stored temporarily in RAM would be impossible in most instances.

Nonetheless, despite concerns regarding the potential ramifications of the recent decisions, the case should be viewed in its factual context. The case involved copyright holders combating alleged widespread infringement and defendants who were found to have refused to engage in the discovery process in good faith.[3] The finding of defendants' pattern of bad faith in the discovery process clearly informed the court's decisions on discovery matters throughout the case, including the decision regarding the duty to preserve data stored in RAM. Moreover, there is authority suggesting that in most instances data stored temporarily in RAM need not be preserved.

The recent amendments to the Federal Rules of Civil Procedure do not specifically address data stored temporarily in RAM. Nonetheless, the advisory committee notes to the amendment to Rule 26(f), which requires early discussion by the litigants of e-discovery issues, address the preservation of dynamic data like data stored temporarily in RAM. The advisory committee notes provide:

> The volume and dynamic nature of electronically stored information may complicate preservation obligations. The ordinary operation of computers involves both the automatic creation and the automatic deletion or overwriting of certain information. Failure to address preservation issues early in the litigation increases uncertainty and raises a risk of disputes. The parties' discussion [at the Rule 26(f) conference] should pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities. Complete or broad cessation of a party's routine computer operations could paralyze the party's activities. . . . The parties should take account of these considerations in their discussions, with

> the goal of agreeing on reasonable preservation steps.

Likewise, the advisory committee notes to Rule 26(b)(2) recognize that although parties are not absolved of their obligation to preserve electronically stored information which may not be reasonably accessible — such as data stored temporarily in RAM[4] — "[w]hether a responding party is required to preserve unsearched sources of potentially responsive information that it believes are not reasonably accessible depends on the circumstances of each case."

Moreover, the influential Sedona Principles for Electronic Document Production provide that "it is unreasonable to expect parties to take every conceivable step to preserve all potentially relevant electronically stored information."[5] Although the Sedona Principles do not specifically address data stored temporarily in RAM, they recognize that preserving such data may not be practical or appropriate. Comment 5.g to Principle Five of the Sedona Principles provides:

> Even though it may be technically possible to capture vast amounts of data during preservation efforts, this usually can be done only at great cost. Data is maintained in a wide variety of formats, locations and structures. Many copies of the same data may exist in active storage, backup, or archives. Computer systems manage data dynamically, meaning that the data is constantly being cached, rewritten, moved and copied. For example, a word processing program will usually save a backup copy of an open document into a temporary file every few minutes, overwriting the previous backup copy. In this context, imposing an absolute requirement to preserve all information would require shutting down computer systems and making copies of data on each fixed disk drive, as well as other media that are normally used by the system. Costs of litigation would routinely approach or exceed the amount in controversy. In the ordinary course, therefore, the preservation obligation should be limited to those steps reasonably necessary to secure evidence for the fair and just resolution of the matter in dispute.

Because the law in this area is still developing, it remains to be seen whether litigants will be required as a matter of course to preserve data stored temporarily in RAM. Nonetheless, because of the extreme difficulty (if not practical impossibility) in preserving all data stored temporarily in RAM, it is doubtful that courts will impose such obligations. There may be cases in which a duty to preserve certain data stored temporarily in RAM is appropriate. Of course, in deciding what data to preserve, no litigant should ignore such data. Nonetheless, the duty to preserve data temporarily stored in RAM will likely prove to be the rare exception to the rule.

Endnotes

1. Columbia Pictures Indus., Inc. v. Bunnell, No. 06-01093-FMC, 2007 U.S. Dist. LEXIS 46364 (C.D. Cal. May 29, 2007) (order granting plaintiffs' motion to require defendants to preserve and produce server log data); Columbia Pictures Indus., Inc. v. Bunnell, 245 F.R.D. 443 (C.D. Cal. 2007) (order denying defendants' motion to review order granting plaintiffs' motion to require defendants to preserve and produce server log data); Columbia Pictures Indus., Inc. v. Bunnell, No. 06-01093-FMC (C.D. Cal. Dec. 13, 2007) (order granting motion for terminating sanction based on defendants' willful spoliation of key evidence).

2. Brief of Amici Curiae in Support of Defendants' Objections to and Motion for Review of Order re Server Log Data, available at *http://www.eff.org/legal/cases/torrentspy/EFF_CDT_amicus.pdf* (last visited January 28, 2008).

3. On December 13, 2007, the district court granted a default judgment in favor of plaintiffs as a sanction for defendants' myriad discovery violations throughout the case, including: (1) deleting and/or modifying hundreds of postings on a user message board operated by defendants; (2) deleting direc-

tory headings maintained by defendants which identified copyrighted works that were allegedly infringed; (3) destruction of the IP addresses of users of the defendants' website; and (4) false claims by defendants that they did not know the identities of moderators of user message boards.

4. See The Sedona Commentary on Legal Holds: The Trigger and the Process (August 2007) (Public Comment Version), available at http://www.thesedonaconference.org/content/miscFiles/Legal_holds.pdf (last visited January 28, 2008) ("[T]ransient data that is not kept in the ordinary course of business, and which the organization has no means to preserve (*e.g.*, voicemail and instant messaging) may also be considered not reasonably accessible.").

5. The Sedona Principles for Electronic Document Production, Principle No. 5 (2d ed. June 2007), available at http://www.thesedonaconference.org/content/miscFiles/TSC_PRINCP_2nd_ed_607.pdf (last visited January 28, 2008); see also Miller v. Holzmann, No. 95-01231 (RCL/JMF), 2007 U.S. Dist. LEXIS 2987, at *20 (D.D.C. Jan. 17, 2007) (holding that Sedona Principle No. 5 is reasonable and in accordance with developing case law); Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 217 (S.D.N.Y. 2003) ("Zubulake IV") ("Must a corporation, upon recognizing the threat of litigation, preserve every shred of paper, every email or electronic document, and every backup tape? The answer is clearly, 'no.' Such a rule would cripple large corporations . . . that are almost always involved in litigation"). ■

MEALEY'S LITIGATION REPORT: CYBER TECH & E-COMMERCE
edited by Mark C. Rogers
The Report is produced monthly by

1018 West Ninth Ave, Third Floor, King of Prussia Pa 19406-0230, USA
Telephone: (610) 768-7800 1-800-MEALEYS (1-800-632-5397)
Fax: (610) 962-4991
Email: mealeyinfo@lexisnexis.com Web site: http://www.lexisnexis.com/mealeys
ISSN 1535-718X