



DIGITAL DISCOVERY & E-EVIDENCE



VOL. 8, NO. 2 33-36

REPORT

FEBRUARY 1, 2008

Reproduced with permission from Digital Discovery & e-Evidence, Vol. 08, No. 02, 02/01/2008, pp. 33-36. Copyright © 2008 by The Bureau of National Affairs, Inc. (800-372-1033) <http://www.bna.com>

CASE ANALYSIS

Battering RAM: Default Judgment Entered in *Columbia Pictures v. Bunnell* for Defendants' Spoliation of Evidence

BY MARTIN J. JARON, JR. & WILLIAM F. HAMILTON

On December 13, 2007, Judge Florence-Marie Cooper entered a default judgment¹ against Justin Bunnell, Wes Parker and other defendants who operate the TorrentSpy² website, which enables users to locate and download from each other dot-torrent files. Using dot-torrent files and a software program, a "Bit-Torrent" client's individual users become part of a peer-to-peer network where they can download, view, store, and distribute what plaintiffs' alleged were copyrighted motion pictures and television shows.

The surprising default judgment in *Columbia Pictures* brings to a partial conclusion³ a case that has stirred significant response and debate in the electronic

discovery community. It also leaves open for discussion many of the concerns expressed about whether random access memory (RAM) should be preserved by litigants, when and under what circumstances it should be preserved, and—if preserved—the difficulties and cost of doing so.

Prior Rulings. The earlier rulings in this case by Magistrate Judge Jacqueline Chooljian⁴ and Judge Cooper⁵ had required defendants to preserve certain information present in the RAM of defendants' Bit Torrent servers located in the Netherlands. It is important to note that the specific data in RAM ordered to be preserved was the log files of Bit Torrent user downloads and IP addresses. The rulings did not require general preservation of all information contained in defendants' server RAM.

Nevertheless, the rulings sparked much debate and hand-wringing in the e-discovery community because of the inherent difficulties and cost of preserving RAM,

¹ *Columbia Pictures Inc. v. Bunnell*, Order Granting Plaintiffs' Motion For Terminating Sanctions, entered December 13, 2007) Case No. 2:06-cv-01093 FMC-JCx (C.D. Cal.) (hereinafter "the December 13, 2007 Order").

² <http://www.torrentspy.com>

³ The December 13, 2007 Order enters default but does not address damages, which presumably will be the subject of

proof, or the election of statutory damages, at a future hearing. Appeals may follow.

⁴ *Columbia Pictures, Inc. v. Bunnell*, 2007 WL 2080419 (C.D. Cal. 2007) (decided May 29, 2007)

⁵ *Columbia Pictures, Inc. v. Bunnell*, 245 F.R.D. 443, 2007 U.S. Dist. LEXIS 63620 (C.D. Cal. 2007) (decided August 24, 2007).

Martin J. Jaron, Jr. and William F. Hamilton are partners and co-chairs of the e-discovery team at Holland & Knight LLP.

coupled with the fear that RAM might have to be preserved generally as a result of this decision.

Default Judgment. In her December 13, 2007 Order, Judge Cooper entered default judgment after finding that defendants had engaged in willful or bad faith spoliation or destruction of evidence that was relevant to the litigation. The court found that defendants, and specifically Wes Parker and Justin Bunnell, willfully engaged in spoliation of evidence in a number of ways, including:

- Deleting and modifying TorrentSpy user forum postings, including references to copyright infringers; replacing the names of copyrighted works with names such as “some movie 2”;
- deleting entire forum threads; and closing piracy related threads from public view.

- Deleting alphabetical directory headings in TorrentSpy referencing copyrighted works, including listings for major television shows, instead moving such listings to “TV-Unsorted”, without previously producing the unaltered versions of their directory listings, contrary to defendants’ prior representations to the Court.

- Destruction of TorrentSpy user IP addresses by eliminating the fourth octet⁶ of the address. Although defendant Wes Parker testified that TorrentSpy did not record full IP addresses, the testimony of moderators who referred to users by full IP addresses, and who banned certain users by username and IP address, demonstrated that Parker’s testimony was false.

- Falsely claiming that the identities and addresses of site moderators were unknown to defendants, when moderators who were deposed indicated they often used their real names in communications with defendant Parker; that the real names and addresses of moderators were provided to defendant Parker so he could send them T-shirts; and that Parker took several of the moderators to Las Vegas as a thank-you gift.

- As to defendants Parker and Bunnell, attempting to influence the testimony of moderators by indicating that legal fees would only be paid if the moderators agreed to testify to certain things, or withheld requested evidence such as computer hard drives, or delayed producing the drives until after the discovery cutoff date.

Taking these facts into consideration, Judge Cooper reasoned that:

“After oral argument, and further consideration of the history of this case, the Court concludes that no lesser sanctions would be appropriate or effective. A rule excluding evidence would be futile, since the issue here is not the efforts made by Defendants to introduce evidence which could be excluded, but rather Defendants’ destruction or concealment of evidence, forcing Plaintiffs to go to trial with ‘incomplete or spotty evidence’ at trial.”

The Court also noted that monetary sanctions, previously imposed, have been ineffective, and concluded by stating:

“Defendants’ conduct during discovery in this case has been obstreperous. They have engaged in widespread and systematic efforts to destroy evidence and have provided false testimony under oath in an effort to hide evidence of such destruction. Indeed, Defendants’ lateness and incom-

⁶ The court explained that an IP address consists of four numbers (e.g. “165.228.130.11”) separated by a dot. Each of the numbers is called an octet, and the numbers in each octet range from 0 to 255. December 13, 2007 Order, at 6.

plete responses to discovery have led the Magistrate Judge to warn or sanction them on more than one occasion. Although termination of a case is a harsh sanction appropriate only in ‘extraordinary circumstances,’ *Halaco Eng’G Co. v. Costle*, 842 F.R.D2d at 380, the circumstances in this case are sufficiently extraordinary to merit such a sanction. Lesser sanctions would not be adequate to punish the defendants for the wrongful conduct and ameliorate the prejudice and harm to the plaintiffs.”

Harsh words, to be sure, but not unexpected after the court found clear evidence of defendants’ systematic destruction of evidence and false testimony.

The default in *Columbia Pictures* was entered because the court found that defendants destroyed evidence—not because the defendants failed to preserve the server log files present in RAM that were the subject of the earlier rulings in the case.

Commentary. The heated debate generated by earlier rulings in *Columbia Pictures* over preservation of RAM will continue, but perhaps some needed perspective can now be achieved. This case is ending with a whimper, not a bang, and in a manner that does not provide any new insights on whether litigants must routinely expect to preserve RAM in the future. The default in *Columbia Pictures* was entered because the court found that defendants destroyed evidence—not because the defendants failed to preserve the server log files present in RAM that were the subject of the earlier rulings in the case.

Despite the somewhat panicked initial reaction in the e-discovery community about the practical and technological difficulties and cost of implementing an order to preserve RAM data, in reality the facts of this case are so specialized—and the log files in question so easily preserved—that the industry reaction can now be seen as somewhat of an overreaction. We submit that the likelihood future litigants will be required to preserve RAM data on a broad scale, at least based on *Columbia Pictures*, is slim, and that future preservation will likely be limited in scope and volume, as it was in *Columbia Pictures*.

Limited Scope. Albert Einstein once observed, “Not everything that can be counted counts, and not everything that counts can be counted.” While that might be true in theoretical physics, the *Columbia Pictures* court found that user log file information in defendants’ server RAM both “counts” and that it “can be counted.”

In the prior rulings in this case, Magistrate Judge Chooljian and Judge Cooper rejected defendants’ arguments that the defendants lacked the ability to capture and preserve the BitTorrent log files present in RAM in their servers. Magistrate Judge Chooljian found that the logging function of the defendants’ web server could be enabled or disabled, that defendants’ web server programs did in fact contain logging functionality, that defendants’ decision to turn off the logging function was related to making their site more attractive to users who did not want their identities known, and that the log file

data was stored in RAM for up to six hours.⁷ In short, the RAM in question could be preserved easily by enabling an existing function in defendants' web server software.

Judge Cooper noted the same in her August 24, 2007 decision, concluding:

"It is undisputed that the Server Log Data Plaintiffs seek can be copied from RAM in Defendants' computers and produced to Plaintiffs. Rule 34 requires no greater degree of permanency from a medium than that which makes obtaining the data possible. As information can be obtained from RAM, it is within the scope of Rule 34 and subject to discovery under the appropriate circumstances."

To deal with concerns that the wholesale preservation of RAM would be a difficult and costly task for litigants, Judge Cooper carefully narrowed the scope of her August 24, 2007 ruling, stating:

"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 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."⁸

Although not stated in either prior ruling of the court, to the outside observer the simple fact that the reason defendants chose to turn off their server user logging function—to protect the identities of users—speaks volumes when viewed in the context of this case, which alleged improper pirating of the plaintiffs' movies and television programs. Turning off the user log data function in order to hide user identities was the software equivalent of wearing a mask in a bank robbery. Both are intended to hide or mask user identities when performing an unlawful act.

RAM as ESI. *Columbia Pictures* held that RAM is within the definition of electronically stored information (ESI). That holding in turn creates additional issues for counsel managing electronic data preservation at the outset of a dispute or investigation.

ESI requires specific preservation attention because of its volatile character, and no ESI is more volatile than RAM. Early identification and preservation is tricky enough when dealing with storage in hard drives and archival and backup media. Counsel is now faced with assessing the risks associated with whether to preserve data present in RAM which is designed and intended to disappear rapidly within minutes or hours during a computer's routine operation.

The Rule 26(f) safety net is of limited value in providing guidance here. Fleeting and ephemeral data may be long gone before the Rule 26(f) conference is scheduled. The potential litigation relevance of some limited

slice of data stored in RAM, however temporarily or permanently, is likely to be the exception rather than the rule. Absent facts similar to those in *Columbia Pictures*, where it was simply a matter of activating a pre-existing logging function on defendants' server software to capture user data in the context of a copyright piracy case, no general requirement that RAM be routinely preserved appears to exist.

If, on the other hand, a case involves data present in RAM which can be captured and which is relevant to or evidences an alleged scheme to engage in a conspiracy or commit a tort, crime, or fraud, you, as counsel, should consider whether such data can and should be preserved. And note that even in *Columbia Pictures*, such preservation was not required until a court order was entered.

Looking Forward. Absent (1) a specific and well-reasoned demand from opposing counsel to preserve some specific RAM data, (2) the clear and obvious litigation relevance of some RAM data, or (3) a court order, we submit that preservation of RAM should not be part of a litigant's routine duties at the onset of litigation.

Columbia Pictures' conclusion that RAM data is ESI will undoubtedly stand. The court's rationale is beyond reproach. Clearly RAM holds data utilized by the computer. A computer locates certain data in RAM for speed, efficiency, and processing. The court had little difficulty extrapolating from such common sense words such as "store," "retain," "memory," and "hold" to conclude that data in RAM is, in fact, ESI. The magistrate and the district court also noted that the drafters of the Rules Amendments pertaining to ESI intended a broad interpretation:

"Fed.R.Civ.P. 34(a)(1) (2006 amendments) advisory committee's note. Such clear evidence that Rule 34(a)'s scope was intended to be as broad as possible, and cover data stored "in any medium from which information can be obtained," leaves no room to interpret the Rule to categorically exclude information written in a particular medium simply because that medium stores information only temporarily. Information in the RAM of Defendants' computers "can be obtained" by Defendant. It is undisputed that the Server Log Data Plaintiffs seek can be copied from RAM in Defendants' computers and produced to Plaintiffs. Rule 34 requires no greater degree of permanency from a medium than that which makes obtaining the data possible. As information can be obtained from RAM, it is within the scope of Rule 34 and subject to discovery under the appropriate circumstances." 425 F.R.D. at 443.

Lastly, the court relied upon *MAI Systems Corp. v. Peak Computer, Inc.*, 991 F.2d 511 (9th Cir. 1993), where software loaded into RAM was considered sufficiently fixed to constitute a copyright violation. Thus, *Columbia Pictures* dispelled the perception that RAM held data too ephemeral to constitute ESI.

⁷ May 29, 2007 Order (1) Granting In Part And Denying In Part Plaintiffs' Motion To Require Defendants To Preserve And Produce Server Log Data And For Evidentiary Sanctions; And (2) Denying Defendants' Request For Attorneys' Fees And Costs, at 6-7, 11-17.

⁸ 245 F.R.D.443, 2007 U.S.Dist. Lexis 63620.

We submit that the likelihood future litigants will be required to preserve RAM data on a broad scale, at least based on *Columbia Pictures*, is slim, and that future preservation will likely be limited in scope and volume . . .

In Practice. What is the practical impact for litigation counsel of the *Columbia Pictures* holding that data held in RAM is ESI which, under some circumstances, must be preserved?

First, RAM is merely another of the rapidly expanding data locations that litigation counsel must consider in the original preservation plan. ESI locations are expanding and will continue to do so.

Counsel must now check the availability of data on a wide variety of PDAs, “integrated” cell phones (think “iPhone”), VOIP servers, image metadata, wireless tool payment devices, Global Positioning Systems, and more. Instant messaging software (where IM communications between parties can be logged or not, depending on user settings in the IM software), presents an additional area of potential preservation for companies who use IM as a regular communications tool. The reach and scope of ESI subject to federal and state civil procedure rules will continue to expand as technology advances.

Second, counsel must expand his or her computer knowledge to a higher level. The computer’s basic operations must be more broadly understood.

For example, whereas most counsel now know that Word documents contain a vast amount of metadata, fewer counsel know that the Word application loaded into RAM may contain data not stored on the hard drive and which will be lost on shutdown. Counsel will need to expand working knowledge to include what data is utilized and present in RAM on a computer when it is “on,” not merely what data is retained when the computer it is turned “off.”

Understanding the creation, use, and preservation, when necessary, of both static RAM and dynamic RAM will become an essential kernel of knowledge for coun-

sel handling e-discovery in a case. Litigation counsel must become increasingly cognizant of the varieties and flavors of volatile and non-volatile computer memory.

Third, counsel should pay attention to both dollars and common sense. A little discussed section of Magistrate Judge Chooljian’s opinion concerned the cost analysis applicable to RAM data preservation. The preservation and search costs of all RAM on desktops and servers would clearly be both burdensome and cost prohibitive in most cases.

In *Columbia Pictures*, the defense expert estimated that the servers in question would generate 40 to 60 gigabytes of data per day. A single gigabyte of data yields approximately 75,000 TIFF images and, when printed, will fill the bed of a pickup truck.

Magistrate Judge Chooljian, however, dispatched defendants’ cost argument by ruling that all of the servers’ RAM data need not be preserved, only the applicable server logs which plaintiffs’ expert estimated to amount to perhaps a single gigabyte of data per day. Additionally, Magistrate Chooljian also suggested that sampling technology might prove to be useful to the parties.

The holding in *Columbia Pictures* that RAM may contain ESI required to be preserved is tempered by the court’s conclusion that the duty to preserve and produce will be governed by the currently evolving case law regarding the cost and marginal value of both preservation and production of ESI.

The burden on any party seeking RAM data is extremely high. RAM data must be shown to be highly important to the case (in *Columbia Pictures*, RAM data was “essential”); it must be shown to be separable and capable of being captured and separated from other RAM data; and it must be demonstrated not to unfairly burden the preserving and producing party. If the RAM in question also demonstrates conduct that constitutes an unlawful act, the likelihood that production may be ordered will likely increase.

However, the preservation, review, and production of RAM should not be a routine or common occurrence in the e-discovery phase of the majority of commercial cases. And, as the most recent decision in *Columbia Pictures* holds, destruction of relevant electronic evidence, like any other form of evidence, can lead to severe sanctions, including default judgment.

Full text of Columbia Pictures Inc. v. Bunnell.