

COMMENTARY

Reprinted From E-Discovery: A Thomson West Report

The *Columbia Pictures* Order: The Scope of Ephemeral ESI

By Paul Brabant, Esq.

Given the heightened awareness of issues relating to discovery obligations and electronically stored information, a recent decision from the U.S. District Court for the Central District of California ensures that the debate will remain lively. The order entered by Magistrate Judge Jacqueline Chooljian in *Columbia Pictures v. Bunnell* expands the definition of ESI to include random access memory because it is a temporary but tangible form of data storage.¹

The *Bunnell* case involves the Motion Picture Association of America's copyright infringement allegations against TorrentSpy, which operates a file-sharing service that allows users to retrieve video and audio content stored on other users' computers. Its technology is based on ".torrent" files that enable fast download speeds by aggregating the content shared by its users.

The MPAA filed a motion to require TorrentSpy to preserve and produce server logs that record search terms submitted by TorrentSpy's users, which could help the plaintiff determine whether TorrentSpy users sought to download copyrighted material. TorrentSpy argued that the server log data is not ESI because it exists only temporarily in random access memory and was not available for production because TorrentSpy's servers did not record this data.²

Granting the MPAA's motion in part, the judge ordered TorrentSpy to preserve and produce the server log data stored in RAM by activating logging on its servers. TorrentSpy appealed this decision, which was denied by Judge Florence-Marie Cooper Aug. 24.³

The *Bunnell* decision is particularly significant because it settles that RAM is electronically stored information and it expands the definition of ESI to include temporarily stored information, or *ephemeral ESI*. Indeed, this decision reflects the foresight of the Advisory Committee on the Federal Rules of Civil Procedure in creating an expansive definition of ESI in Rule 34(a), anticipating that the full range of technical nuances could not be codified in the rules and would be developed at common law.⁴

Is RAM the Tip of the Iceberg?

On its surface, the *Bunnell* decision is an unsettling precedent. Enterprises working on a litigation readiness effort are most certainly not factoring RAM and other temporary storage devices into their plans. Should they be? What are the implications for information flowing through RAM, disk cache and other sources of ephemeral data that may exist on servers, workstations and other hardware that store ESI?

A closer reading of the decision should ease some of the fears expressed by observers of the case that it could dramatically increase the scope of e-discovery.⁵ The judge's order shows a careful deliberation leading to the conclusions that:

- The information temporarily stored in RAM is relevant;
- Server log data temporarily stored in RAM constitutes ESI under Rule 34 of the Federal Rules of Civil Procedure; and
- A preservation order was not unduly burdensome for the defendant.

This decision is fact-specific and should be limited to the situation and the type of service provided by TorrentSpy. The judge took care to emphasize that her 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.”⁶

Additionally, the judge understood that TorrentSpy could not have anticipated this obligation, rejecting the MPAA's assertion that the defendant's failure to preserve the server log data amounted to spoliation. The judge found that evidentiary sanctions were not appropriate because TorrentSpy had “a good-faith belief that preservation of data temporarily stored in RAM was not legally required.”⁷

Nonetheless, the judge's reasoning raises important questions about the data that flows through information systems and the nature of ephemeral ESI. TorrentSpy argued that random access memory is not ESI because the information it contains is transient in nature and that logging this information would amount to creating a new record.

Certainly, requiring the defendant to log temporary server data that was not previously logged seems at odds with Rule 34, which only requires a party to produce information that is permanently in existence.⁸ If server log data needs to be recorded temporarily in order to be preserved and produced, was it truly stored in the first place? The parties stipulated that the server log data existed in RAM for up to six hours, but even so, it was never readily accessible.

To illustrate this point, consider a hypothetical lawsuit in which a plaintiff alleges that a defendant engaged in unlawful sales practices. The defendant's sales are conducted entirely by phone and are not recorded. The plaintiff's expert testifies that the defendant's voice system has a recording capability that could be enabled at marginal cost. In this case the defendant would likely argue that voice communications are not ESI because the voice data was never stored.

Using the *Bunnell* precedent, however, if the plaintiff can demonstrate that voice data flowed through RAM or some other temporary storage device, an argument can be made that turning on the phone system's recording capability would not amount to creating a new record.

This seems like splitting hairs. With information systems that store data for milliseconds in order to process a transaction, it is difficult to distinguish between data that is stored ephemeraly and data that is not stored but can be recorded. Going forward, technical details about storage media and the length of time data

is stored will likely be less important than the availability of the information and the analysis of cost and burden associated with collecting information relevant to the facts of the case.

Indeed, in her opinion denying TorrentSpy's appeal, Judge Cooper said "data stored in RAM, however temporarily, is electronically stored information subject to discovery under the circumstances of the instant case."⁹ As the judge broadly interprets Rule 34, she appears to accord more weight to the probative value of the server log data than any other consideration.

Conclusion

The *Bunnell* decision was extremely disruptive for TorrentSpy. After the MPAA filed its complaint, TorrentSpy implemented a content-filtering tool named File-Rights to protect copyrighted material.¹⁰ On Aug. 26 TorrentSpy started to block access to its site for users based in the United States.¹¹ However, this decision should have a limited impact for most online content providers because relatively few have a similar business model.

Beyond TorrentSpy, the *Bunnell* decision highlights the tension between the semantics of the Federal Rules of Civil Procedure and the technical details that have a direct impact on litigants' obligations relating to ESI.

As the courts delve deeply into novel technical areas, their decisions will require interpretation and will depend in part on the input and credibility of expert witnesses. This process may lead to controversial decisions as judges explore more gray areas not fully defined by the rules.

For those involved in litigation readiness efforts, it is therefore advisable to take a broad view of preservation and production obligations, based on an evaluation of the company's business model and the factors that could lead to litigation or a government investigation.

For certain businesses, the *Bunnell* decision is a warning that data flowing through their information systems may constitute ESI requiring preservation in the event of the threat of litigation. Taking a broad view of these obligations will help anticipate the type of information that may be helpful (or not) in a particular matter, the burdens associated with preserving and producing information, and the need for expert testimony to defend a chosen approach.

Eventually, the Federal Rules of Civil Procedure will likely require additional amendments to provide specific guidance on the application of the rules to temporarily stored information and other technologies, particularly if the common law does not evolve as quickly as technology and its various implementations.

Paul Brabant is vice president of consulting at Epiq Systems. He has 13 years of experience applying technological solutions to legal practice. Epiq Systems is a leading provider of integrated technology products and services for the legal profession.

■ Notes

- ¹ *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093, 2007 WL 2080419 (C.D. Cal. May 29, 2007).
- ² This decision addresses several issues outside the scope of this article, such as privacy concerns, control of servers operated by a third party, sanctions and violations of various statutes.
- ³ *Columbia Pictures Indus. v. Bunnell*, No. CV 06-1093, 2007 WL 2702062 (C.D. Cal. Aug. 24, 2007).
- ⁴ "Rule 34(a)(1) is intended to be broad enough to cover all current types of computer-based information and flexible enough to encompass future changes and developments." FED. R. CIV. P. 34(a)(1) (2006 amendments), Advisory Committee's note.
- ⁵ Ken Withers, director of Judicial Education at the Sedona Conference, said he feared Judge Chooljian's decision "may mean a 'tremendous expansion' of the scope of discovery in civil litigation." Greg Sandoval, *TorrentSpy ruling a 'weapon of mass discovery'*, CNET News.com (June 14, 2007). See also Jessie Seyfer, *RAM Ruling Portends a New e-Discovery Brawl*, THE RECORDER (June 2007), at 2.
- ⁶ *Bunnell*, No. CV 06-1093, at *31 n.31 (C.D. Cal. May 29, 2007). In her order affirming Judge Chooljian's decision, Judge Cooper also emphasized that her decision was limited to "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." *Bunnell*, No. CV 06-1093, at 4 (C.D. Cal. Aug. 24, 2007).
- ⁷ *Bunnell*, No. CV 06-1093, at 33 (C.D. Cal. May 29, 2007). Specifically, Judge Chooljian ruled that a finding of spoliation was not appropriate "in the absence of (1) prior precedent directly on point in the discovery context; (2) a specific request by defendants to preserve server log data present solely in RAM; and (3) a violation of a preservation order." *Id.* at 32. Consider also another recent copyright infringement case in which the plaintiff sought a spoliation inference due to the defendants' failure to preserve images viewed on a public Web site and stored in their computers' cache. *Healthcare Advocates Inc. v. Harding, Earley, Follmer & Frailey*, No. 05-3524, 2007 WL 2085358 (E.D. Pa. July 20, 2007). In this case, the court denied the plaintiff's request, explaining that the defendants did not intentionally destroy these images. The court explained that "to impose a sanction on the [defendant] for not preserving temporary files that were not requested, and might have been lost the second another Web site was visited, does not seem to be a proper situation for an adverse spoliation inference." *Id.* at *21.
- ⁸ *Alexander v. FBI*, 194 F.R.D. 305, 310 (D.C. 2000).
- ⁹ *Bunnell*, No. CV 06-1093, at 2 (C.D. Cal. Aug. 24, 2007).
- ¹⁰ FileRights will allow movie studios to upload a digital signature to identify copyrighted material that may be indexed by the TorrentSpy search engine. Nate Anderson, *TorrentSpy Starts Filtering Copyrighted Content*, ARS TECHNICA (June 25, 2007), at 1.
- ¹¹ See Greg Sandoval, *TorrentSpy Shuts Down in the U.S.*, CNET News.com, (Aug. 27, 2007). A search entered on its site now produces the following message: "TorrentSpy Acts to Protect Privacy. Sorry, but because you are located in the USA you cannot use the search features of the TorrentSpy.com Web site. TorrentSpy's decision to stop accepting U.S. visitors was NOT compelled by any court but rather an uncertain legal climate in the U.S. regarding user privacy and an apparent tension between U.S. and European Union privacy laws."