New York Law Journal

RAM and FRCP 34 Lock Horns

Kelly Talcott
06-27-2007

A recent e-discovery decision from the U.S. District Court for the Central District of California provides an opportunity to reflect a bit on the permanence of storage media. It has also inspired debate as to when temporarily stored information becomes "electronically stored information" that needs to be preserved and, where relevant, produced in response to discovery requests.

The May 27, 2007, order directs defendants in an ongoing copyright infringement lawsuit to collect and produce information stored in the random-access memory of their servers. [FOOTNOTE 1]

Depending on the ideological and topical bent of the commentator, this decision (a) heralds a substantial victory in the war against copyright infringement; (b) sounds the death knell for Internet user privacy, or (c) could require anyone involved in a lawsuit to turn over information stored by their computers' RAM hardware. Closer inspection of the federal magistrate judge's decision reveals the correct answer is probably (d) none of the above.

A number of motion picture studios (referred to hereafter as the MPAA) sued defendants who operate a Web site called "TorrentSpy" that offers users "dot-torrent" files to download. The dot-torrent files are used by a "BitTorrent" application running on the user's computer to locate and download content -- in this case, the plaintiffs contend that the content includes their copyrighted motion picture content -- over a computer network, typically the Internet. Because the dot-torrent files were not themselves infringing, and because much of the allegedly infringing content was not hosted by TorrentSpy, the relevant claims for purposes of the RAM discovery ruling were contributory in nature: vicarious infringement, contributory infringement and inducement.

As an aside, it is in the nature of the BitTorrent application that a consumer of content becomes a distributor of content. Unlike, say, a typical iTunes download where the entire mp3 file is downloaded to the user's computer from a single source, BitTorrent assembles whole files in pieces from a variety of sources simultaneously, all at a high rate of speed. A BitTorrent download is thus particularly effective for large files, such as full-length TV programs or feature films.

Once a user downloads a particular file, the user's computer becomes another source for other users to acquire all or part of that file, and the more BitTorrent files the user has available for others, the faster that user's own downloads will be. Thus knowing what requests were made for which dot-torrent files and knowing the IP addresses of the requesting computers are two pieces of information that could help the MPAA plaintiffs identify direct infringers and make their contributory case against the TorrentSpy defendants.

The MPAA served discovery requests on the TorrentSpy defendants asking for, among other things, IP addresses of users of the TorrentSpy site who requested dot-torrent files, records of requests for dot-torrent files, and the dates and times of such requests. The MPAA later filed a Rule 37 motion seeking an order requiring TorrentSpy to preserve and produce certain server log data, as well as for sanctions.

Magistrate Judge Jacqueline Chooljian noted that the TorrentSpy servers were capable of creating a log of the requests made for dot-torrent files, including a log of the IP addresses of the requesting users' computers, but that TorrentSpy had elected to disable the logging function. As a result, the dot-torrent requests were being stored only in the servers' random access memory, or RAM, where in the normal course of things they would be overwritten after approximately six hours.

Before arriving at the question of whether this temporarily stored information should be preserved and produced, the magistrate judge considered whether it was relevant to the dispute. Given that the MPAA's claims were based on the defendants' contributory infringement, the logs of requests made by users for dot-torrent files -- files that in some cases could point the users' BitTorrent client to allegedly infringing content -- were "extremely relevant and may be the key" to the lawsuit.

Having established the relevance of the requested information, the magistrate judge then turned to the question of whether the server log information that resided temporarily on the servers' RAM constituted "electronically stored information" under rule 34(a) of the Federal Rules of Civil Procedure. Applying a straightforward analysis, she noted the advisory committee comment 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," and that the rule "is expansive and includes any type of information that is stored electronically," and "is intended to be broad enough to cover all current types of computer-based information."

The key question here was whether storing the server log information in RAM was "fixing" it in a tangible medium. The court turned to copyright cases from the 9th U.S. Circuit Court of Appeals that found that software copied into RAM was "fixed" in a tangible medium, and determined that the same rationale applied in the discovery context. [FOOTNOTE 2] The server log information was thus electronically stored information under rule 34(a).

NOT A NEW RECORD

Another issue addressed by the magistrate judge was whether requiring the defendants to preserve and produce the server log data was tantamount to forcing them to create new

data, since the defendants' systems had not created these types of logs before. The court noted that the information in question does exist; it is temporarily stored in RAM, and it is in the defendants' possession, custody or control. [FOOTNOTE 3] Because of that, the court held that an order requiring defendants to preserve and produce the information was not tantamount to ordering the creation of new data.

While a number of commentators have made ominous predictions that orders to preserve information stored in RAM are likely to become commonplace, thus becoming a "weapon of mass discovery," [FOOTNOTE 4] a closer reading of the court's opinion suggests this is not likely.

The MPAA was required to make a clear showing of relevance and need, and in fact the court considered three sets of briefs and conducted an evidentiary hearing before issuing its ruling, which has been stayed pending appeal. The cost associated with establishing the relevance of and need for this information was thus substantial.

The magistrate judge also took pains to emphasize 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 noted that the decision to require retention and production of the server log data was based on the facts of the particular case, "the key and potentially dispositive nature of the Server Log Data which would otherwise be unavailable," and defendants' failure to show undue burden or cost.

In the vast majority of cases, this situation is unlikely to exist. The information temporarily stored in RAM will not be relevant to the dispute in question, or it will eventually find its way from RAM to a hard disk, backup tape or some printed document. Only in a very small portion of disputes will information stored only on RAM be of sufficient importance to the issues to warrant special preservation and production efforts.

That said, there may be times where the only place relevant information is recorded is in RAM. The simple fact that RAM is by definition a transient form of storage should not by itself rule out requiring a party to preserve and produce relevant information that is not available in any other medium. Parties seeking production of information stored in RAM face a high burden given the fleeting nature of the storage medium and the extra efforts associated with preserving and producing that information.

PRODUCTION OF IP ADDRESSES

A second issue the court faced was the MPAA's request for the IP addresses associated with the dot-torrent requests made to the TorrentSpy site. That information would in many cases allow one to identify the computer from which the request was placed, which could be the basis for further actions against users for direct copyright infringement.

The magistrate judge ordered that, at the initial production stage at least, all IP addresses were to be masked by the TorrentSpy defendants, though the TorrentSpy defendants were to do so in a way so the MPAA could identify when the same user made multiple dot-torrent file requests. The court further ordered the MPAA plaintiffs not to attempt to unmask those addresses. While this may alleviate some privacy concerns that have been raised by the defendants and third parties, there is nothing that would prevent the court from ordering those IP addresses to be disclosed.

While the TorrentSpy decision appears to be the first under the newly revised Federal Rules that specifically identifies information stored on RAM as electronically stored information subject to Rule 34 preservation and production requirements, it did so on its unique set of facts and after a careful application of the existing tests for requiring production of disputed information. It is likely to be the special cases, not the usual ones, that will require information stored only on RAM to be preserved and produced.

Kelly D. Talcott, a partner at K&L Gates, practices intellectual property and technology law.

::::FOOTNOTES::::

FN1 *Columbia Pictures Industries v. Bunnelli*, CV 06-1093 FMC (JCx), U.S. District Court for the Central District of California.

FN2 See *MAI Systems Corp. v. Peak Computer*, Inc., 991 F.2d 511, 518-19 (9th Cir. 1993) (software copied into RAM is fixed in a tangible medium and is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration); *Perfect 10, Inc. v. Amazon.com, Inc.*, 2007 WL:1428632 (9th Cir. May 16, 2007) ("The image stored in the computer is the 'copy' of the work for purposes of copyright law," citing MAI).

FN3 The control issue was also disputed because defendants had recently outsourced some of their operations to a third party that hosted the TorrentSpy application on its own servers. The magistrate judge determined that the defendants retained sufficient control over the server log information because they retained the ability to manipulate how that server log information was routed.

FN4 "TorrentSpy ruling a 'weapon of mass discovery,'" *Cnet News*, June 14, 2007, available via www.news.com.