An ALM Website

LAW.COM

Online Feature

January 27, 2010

An ALM Publication

Honey, I Forgot the Cell Phone: The 411 on 'Outlier' ESI

FARRAH PEPPER

Special to Law.com

January 27, 2010

A popular advertisement for cellular services asks consumers: "Can you hear me now?" After years of static on the line about how parties in federal courts should handle the preservation and production of so-called "outlier" electronically stored information -- such as that found on cell phones and PDAs, voice mail systems, instant messaging systems, chat rooms, and websites -- the message is starting to come through. [FOOTNOTE 1] While these data sources may have been neglected or even completely overlooked in years past, recent events in courtrooms and in the news emphasize that these sources should not be ignored. One need look no further than headlines about voice mail and text messages apparently sent by a celebrity golfer to his alleged mistress to realize the potential significance of outlier ESI data.

That scandal reminds us of the importance of managing text messages, instant messages, voice mail and other outlier ESI before they become evidence in litigation. In fact, under certain circumstances, failure to preserve and produce certain outlier ESI could constitute spoliation and result in sanctions such as an adverse inference.[FOOTNOTE 2] Consequently, counsel should actively consider the legal and strategic benefits of incorporating outlier ESI into their litigation response plans (via inclusion in litigation hold notices and preservation efforts, discussion at meet and confer sessions with opposing counsel, and incorporation into discovery plans presented to the court).[FOOTNOTE 3] Whether it is appropriate for outlier ESI data to be preserved and produced in any given litigation is highly fact specific.

NEW TECHNOLOGY, NEW CHALLENGES

The collision of new technologies with established discovery duties has forced federal courts to determine whether new data types and sources fall under well-settled traditional preservation and production requirements. [FOOTNOTE 4] Courts and parties have grown relatively accustomed to dealing with data sources that are common in modern-day discovery, including hard drives, networks, databases and external media (e.g., thumb drives and backup drives) and data types, such as scanned images of paper files, e-mail, electronic documents (e.g., Microsoft Word files) and even "legacy data."[FOOTNOTE 5] However, they have also had to grapple with fitting new data sources and types -- the "outliers" -- into the traditional paradigm.[FOOTNOTE 6]

Under the existing framework, some basic questions courts must answer with regard to each outlier ESI source include: (1) whether the source contains relevant data under the responding party's custody or control, (2) whether data from this source is "not reasonably accessible" due to undue burden or cost and therefore not required to be produced,[FOOTNOTE 7] and (3) if so, whether there is good cause nonetheless for the data to be produced. [FOOTNOTE 8] The framework favors an early assessment of outlier ESI data sources, given that it is the responding party's responsibility to proactively identify data sources, by category and type, which are not reasonably accessible.[FOOTNOTE 9] When dealing with outlier ESI data sources under this framework, there may be a greater chance that the data is deemed to be not reasonably accessible due to added burden or cost associated with retrieving the data in question. [FOOTNOTE 10]

FARRAH PEPPER

While federal case law is still developing with regard to the preservation and production requirements for outlier ESI data and sources, a few courts have provided some guidance.

Websites and hyperlink images. Issues relating to websites and hyperlink images -- the website reached when a recipient clicks on a link -- have generated arguably the most settled law relating to outlier ESI data sources.[FOOTNOTE 11] Custody and control have been key aspects of the reported decisions addressing websites and hyperlink images. Courts have held that there is a duty to preserve a website for litigation when the responding party maintains custody or control over that website. [FOOTNOTE 12] Decisions addressing hyperlink images did not find any duty to preserve or produce the data when the responding party lacked custody or control.[FOOTNOTE 13]

Instant messaging (IM) and chat room systems. No federal court has explicitly held that a proactive duty exists to preserve IM or chat room communications for litigation. Without deciding the issue, however, courts have implied that if IM or chat room conversations are routinely stored by a party in the general course of its business, then they may reasonably be required to be preserved and produced in litigation.[FOOTNOTE 14] Moreover, when parties agree that instant messages are to be preserved as part of litigation, courts have upheld those agreements.[FOOTNOTE 15]

Audio recordings, including voice mail systems. While no obligation has been articulated for parties to proactively record relevant conversations for litigation,[FOOTNOTE 16] courts have ordered the production of preexisting relevant voice recordings and sanctioned parties for destroying them.[FOOTNOTE 17] Voice mail systems are considered to be sources of discoverable ESI, whether they are in analog or digital form.[FOOTNOTE 18] Notably, emerging voice mail technology offers unified messaging systems which integrate telephony and computer systems. In certain systems, recipients receive e mails notifying them of an incoming voice mail that may also attach the voice mail as a WAV audio file, thus creating additional forms of voice mail messages.[FOOTNOTE 19]

Non-audio data on cell phone and personal digital assistant (PDA) devices. Cell phone and PDA devices (e.g., BlackBerries and iPhones) may contain various types of data in addition to voice messages, including text messages, e-mail, images, calendar entries and contacts. Courts have ordered parties to preserve relevant data on cell phones and PDAs, such as text messages, e-mails from personal accounts, calendar items, call logs[FOOTNOTE 20] and cell phone images.[FOOTNOTE 21] These orders extend to data hosted by third parties when the data remains under the responding party's custody or control.[FOOTNOTE 22]

THE CLEAR MESSAGE

Courts have only just begun to address the discovery obligations attaching to outlier ESI. In fact, courts have yet to articulate clear discovery standards for a number of new data sources, including collaborative tools, such as wikis and Microsoft SharePoint, and social networking sites like Twitter, Facebook, MySpace, and LinkedIn.[FOOTNOTE 23] Although many of the details still remain to be clarified in future opinions, the general message could be viewed as follows: manage and consider the litigation impact of outlier ESI now, or ignore it and potentially face issues that could have been avoided down the road.

Farrah Pepper is of counsel in the New York office of Gibson, Dunn & Crutcher LLP and vice chair of the firm's Electronic Discovery and Information Law practice group. She can be reached at fpepper@gibsondunn.com. Jonathan Fortney, an associate at the firm, assisted in the preparation of this article.

::::FOOTNOTES::::

FN 1 This article employs the phrase "outlier" ESI to refer to ESI that may exist "out of sight" and/or "out of mind" for parties subject to discovery obligations and, therefore, may be more likely to be overlooked. Currently, few court decisions address the preservation and production requirements of outlier ESI in litigation.

FN 2 See, e.g., *Vagenos v. LDG Fin. Servs. LLC*, No. 09-cv-2672 (BMC), 2009 WL 5219021, at *2 (E.D.N.Y. Dec. 31, 2009) (ordering adverse inference instruction for failure to preserve relevant voice mail recording on cellular phone); *Se. Mech. Servs., Inc. v. Brody*, Case No. 8:08-CV-1151-T-30EAJ, 2009 WL 2883057, at *7 (M.D. Fla. Aug. 31, 2009) (Jenkins, Mag. J.) (ordering adverse inference instruction for the wiping of data from BlackBerry devices); *Arteria Prop. PTY Ltd. v. Universal Funding V.T.O.*, Civil Action No. 05-4896 (PGS), 2008 WL 4513696, at *5 (D.N.J. Oct. 1, 2008) (Salas, Mag. J.) (ordering adverse inference instruction for failure to preserve website content).

FN 3 When the issue is raised proactively, parties may mutually agree that certain outlier ESI data sources are not likely to contain relevant information (or that they contain relevant information the value of which does not justify any undue burden or cost associated with preservation and production) and further agree to exempt those sources from discovery.

FN 4 A basic principle of discovery is the obligation to preserve relevant ESI when litigation is pending or reasonably anticipated. See *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, 218 (S.D.N.Y. 2003). Production of ESI, however, is not automatically required when it is "not reasonably accessible because of undue burden or cost" -- unless "good cause" for its production is demonstrated by the requesting party. FED R. CIV. P. 26(b)(2)(B).

FN 5 Legacy data is ESI that was created or stored in software or hardware that subsequently became obsolete or replaced and which can be expensive to restore if needed for litigation. See, e.g., *Phoenix Four, Inc. v. Strategic Res. Corp.*, No. 05 Civ. 4837 (HB), 2006 WL 1409413, at *5 (S.D.N.Y. May 22, 2006) (awarding monetary sanctions against defendant, a defunct company, and its counsel for discovery delay caused by failure to identify 25 gigabytes of unmapped data located on a partitioned, dormant section of defendant's old server).

FN 6 The Federal Rules of Civil Procedure Advisory Committee's Notes acknowledge that Rule 34(a)(1), which is expansively worded to include all types of ESI, was intentionally left "flexible enough to encompass future changes and developments" in electronic technology. FED R. CIV. P. 34 Advisory Committee's Notes (2006) ("The wide variety of computer systems currently in use, and the rapidity of technological change, counsel against a limiting or precise definition of electronically stored information.").

FN 7 See FED R. CIV. P. 26(b)(2)(B). Parties are not automatically relieved of the preservation obligation for outlier ESI data sources that are not reasonably accessible, because the analysis is fact specific. FED R. CIV. P. 26(b)(2) Advisory Committee's Notes (2006) ("Whether 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. It is often useful for the parties to discuss this issue early in discovery.").

FN 8 See FED R. CIV. P. 26(b)(2)(B).

FN 9 See FED R. CIV. P. 26(b)(2) Advisory Committee's Notes (2006).

FN 10 In evaluating whether outlier ESI data is reasonably accessible, one factor may be the relative permanence of the ESI. The Sedona Conference has proposed that inaccessible data should be evaluated based on the media type and the data complexity, including factors such as the transient nature of the data. "The Sedona Conference Commentary on Preservation, Management and Identification of Sources of Data that are Not Reasonably Accessible," 10-12 (July 2008). At least one court has opined that, absent a court order requiring preservation, the ephemeral nature of data not routinely stored for business purposes weighs against the imposition of sanctions for spoliation if that data is not preserved for litigation. See *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, 177 (S.D.N.Y. 2004) (distinguishing between semi-permanent data, which are "transmitted to others, stored in files, and are recoverable as active data until deleted," and ephemeral data, which have a fleeting life span that ends upon routine operations of a computer system). For more in-depth treatment of ephemeral data and the handful of cases that have analyzed the topic to date, see Kenneth J. Withers, "Ephemeral Data" and the Duty to Preserve Discoverable Electronically Stored Information, 37 *U. Balt. L. Rev.* 349 (2008).

FN 11 As one court stated, there is "no reason to treat websites differently than other electronic files." Arteria, 2008 WL 4513696, at *5. No federal courts have yet commented specifically on preservation and production obligations related to a "blog" -- a website consisting of periodic postings that often focus on a particular subject, sometimes with a commenting feature enabled for visitors.

FN 12 *Arteria*, 2008 WL 4513696, at *5 (ordering adverse inference instruction for failure to preserve website content where defendants retained "ultimate authority" over the website's content) (emphasis in original).

FN 13 *Ferron v. Echostar Satellite, LLC*, Civil Action No. 2:06-CV-453, 2009 WL 2370623, at *5 (S.D. Ohio July 29, 2009) (King, Mag. J.) (declining to apply sanctions for defendant's failure to preserve the websites and images to which its e-mails hyperlinked, because they were not under defendant's control); *Phillips v. Netblue, Inc.*, No. C-05-4401

SC, 2007 WL 174459, at *3 (N.D. Cal. Jan. 22, 2007) (denying motion to dismiss complaint based on plaintiff's failure to preserve hyperlink images that were not under its custody or control).

FN 14 See *Malletier v. Dooney & Bourke, Inc.*, No. 04 Civ. 5316 RMB MHD, 2006 WL 3851151, *2 (S.D.N.Y. Dec. 22, 2006) (Dolinger, Mag. J.) (holding that a party had no duty to preserve messages in a customer service chat room when it did not already preserve them in the ordinary course of business); *Convolve*, 223 F.R.D. at 177 n.4 (noting that instant messenger programs increasingly "have the capability, like e-mail, of storing messages" but offering no opinion "on the circumstances under which the failure to preserve instant message communications would be considered spoliation"). At least one court has ordered the preservation and production of instant messages, albeit in a situation where documents subject to a confidentiality order had been disclosed and were ordered retrieved by the court. *In re Zyprexa Prod. Liab. Litig.*, MDL No. 1596, 2006 WL 3821491, at *1 (E.D.N.Y. Dec. 28, 2006) (ordering plaintiffs' expert witness to preserve and produce instant messages relevant to the litigation).

FN 15 See, e.g., *In re Genetically Modified Rice Litig.*, No. 4:06 MD 1811 CDP, 2007 WL 1655757, at *2, *5 (E.D. Mo. June 5, 2007).

FN 16 See, e.g., *Malletier*, 2006 WL 3851151, at *2.

FN 17 *Vagenos*, 2009 WL 5219021, at *2 (issuing adverse inference instruction due to plaintiff's failure to preserve relevant voice mail recording on cellular phone); *Martin v. Redline Serv. LLC*, No. 08-CV-6153, 2009 WL 959635, at *1 (N.D. Ill. Apr. 1, 2009) (Cole, Mag. J.) (ordering the production of 188 voice message recordings and all existing recordings of telephone calls made by defendant's employee).

FN 18 *Vagenos*, 2009 WL 5219021, at *2 (sanctioning plaintiff for failure to preserve relevant voice mail recording on cellular phone); *Wangson Biotechnology Group, Inc. v. Tan Tan Trading Co., Inc.*, No. C-08-04212 SBA, 2008 WL 4239155, at *8 (N.D. Cal. Sept. 11, 2008) (ordering party to preserve relevant voice mail); *Skeete v. McKinsey Co., Inc.*, No. 91 Civ. 8093 (PKL), 1993 WL 256659, at *4 (S.D.N.Y. July 7, 1993) (holding that plaintiff had a duty to preserve cassette tape recordings of telephone conversations and voice mails upon commencement of litigation).

FN 19 *In re Seroquel Prod. Liab. Litig.*, 244 F.R.D. 650, 661 (M.D. Fla. 2007) (sanctioning party for, inter alia, failing to produce any voice mails when unified voice mail system had delivered messages to employees' inboxes). For more in-depth treatment of the issues to consider regarding the preservation and production of digital voice mail, see Mark S. Sidotti & Paul E. Asfendis, "E-Discovery Issues with Digital Voicemail," *N.Y.L.J.* Oct. 9, 2009.

FN 20 *Se. Mech. Servs., Inc.*, 2009 WL 2883057, at *7 (awarding adverse inference against defendants for failure to preserve and produce relevant data on BlackBerry devices, including text messages, e-mail from personal accounts, calendar items and call logs, in violation of court's preservation order).

FN 21 *Smith v. Café Asia*, 246 F.R.D. 19, 21-22 (D.D.C. 2007) (ordering the preservation and inspection of relevant images stored on plaintiff's cell phone). No federal court appears to have yet addressed the preservation and production issues surrounding BlackBerry PIN messages, which are sent directly between devices via a wireless network rather than through a traditional server -- a fact that may further complicate their preservation and production.

FN 22 *Flagg v. City of Detroit*, 252 F.R.D. 346, 366 (E.D. Mich. 2008) (ordering a party to produce relevant text messages preserved by a third-party service provider and noting that text messages "fit comfortably within the scope of the materials that a party may request under Rule 34").

FN 23 Social networking sites can present an array of features that blend elements of websites, e-mail, instant messaging and chat room technology. *Maldonado v. Municipality of Barcelona*, Civil Action No. 07-1992, 2009 WL 636016, at *2 (D.P.R. Mar. 11, 2009) (Arenas, Mag. J.) (attempting to define social networking sites and their features for the first time in federal court). While no cases yet have held that a party must affirmatively preserve data on social networking sites in anticipation of litigation, courts have recently begun dealing with the evidentiary nature of those sites. See, e.g., *Nguyen v. Starbucks Coffee Corp.*, No. CV 08-3354 CRB, 2009 WL 4730899, at *2, *5 (N.D. Cal. Dec. 7, 2009) (granting summary judgment in favor of defendant company; defendant presented evidence of threats made on plaintiff's MySpace page in support of its motion). It seems likely that it is only a matter of time before courts address the preservation and production obligations inherent to data on social networking sites.