

IMs As ESI: When To Save Instant Messages And How To Properly Authenticate Retained IMs

Timothy J. Carroll

VEDDER PRICE

Reading through the many eDiscovery vendor whitepapers on the topic, one would think that instant message ("IM") retention and archiving should be the focus of every good eDiscovery preparedness initiative. In a thinly veiled effort to boost demand for their products, these vendors have made the blanket assertion that all companies must retain IM for discovery purposes as a result of the amendments to the Federal Rules of Civil Procedure (the "Amended Federal Rules"), which went into effect on December 1, 2006. According to these vendors, this is so because IM falls within the definition of electronically stored information ("ESI") as set forth in the Amended Federal Rules. While organizations must account for the Amended Federal Rules in their eDiscovery undertakings, the impact of IM on information management policies is debatable.

These vendors have been pushing organizations to save and archive IMs for later production in the eDiscovery setting, but the IM-as-ESI dialogue should occur long before and focus on two other critical areas: (i) does your organization need to retain IM; and (ii) if so, how can it authenticate IMs that may be used as evidence in a legal proceeding?

IM has been around for several years, and its popularity in the business environment is increasing. Gartner analyst David Smith predicts that by 2013 IM will be used by 95 percent of employees as their de facto communications tool for voice, video and text chatting.¹ Gartner also states that IM use in business – currently hovering around 25 percent – will reach the 100 percent level as soon as 2010.² That same year, Gartner predicts that the IM market will be more than \$680 million, dispelling any lingering notions that IMs are just for teenagers.³

While the proliferation of IM usage may continue for business reasons (similar to that of E-mail usage in the mid-1990s), the risks associated with IM may be even greater. On this point, the ePolicy Institute asserts that more than 50 percent of IM users send or receive potentially risky and legally harmful information such as workplace gossip, jokes and confidential information via instant messaging.⁴

Putting aside the liability considerations associated with creating and then retaining harmful communications, before an organization decides to monitor and save its

Timothy J. Carroll co-chairs Vedder Price's records management and eDiscovery practice, which is a leading business law firm with offices in Washington, DC, Chicago, New Jersey and New York. Carroll leads a robust information management and eDiscovery practice, having counseled numerous Fortune 500 companies on adopting and implementing lawfully compliant records management programs, electronic communications policies and eDiscovery preparedness initiatives. Carroll also has vast experience in commercial litigation matters, including those relating to securities fraud, misappropriation of confidential information and trade secrets and other business tort actions.

employees' IM, it should also consider whether its actions will violate any privacy laws. For example, the Federal Electronic Communications Privacy Act ("ECPA"),⁵ protects against unwarranted interception or retrieval of electronic communications. Title I of the ECPA, known as the Wiretap Act, makes it a criminal offense to "intentionally intercept[...any wire, oral or electronic communication."⁶ Because IM chats are conversations occurring in real time, similar to telephone calls, an employer's monitoring of IM conversations may also implicate the provisions of the Wiretap Act. Where data access, rather than message interception, is the issue, Title II of the ECPA, the Stored Wire and Electronic Communications and Transactional Records Act (the "Stored Communications Act") applies.⁷

The volume of new information to manage, coupled with the potentially harmful content being transmitted via IM and the privacy risks, may send many IT and in-house counsel into a panic over the financial and legal risks associated with IM preservation and production. But before your organization decides to archive IM, there are a few important facts that it should examine.

While the Amended Federal Rules define ESI as a separate class of discoverable information, they do not explicitly define ESI. However, the committee notes clarify Rule 34(a), governing the production of documents and ESI, noting that the rule "applies to...information that is stored in a medium from which it can be retrieved and examined."⁸ Accordingly, a party must search and produce records from "reasonably accessible" sources, identifying to the requesting party a description of where potentially relevant evidence – including electronic records and repositories – exists.⁹

It is accepted that E-mails, Word documents, Excel spreadsheets and the like are included within the definition of ESI. What is not so clear is where and how IM fits into the ESI definition. According to some, it would seem obvious that IM is the same as E-mail. However, a thorough reading of the hearings that occurred prior to the enactment of the Amended Federal Rules and recent case law suggests that IMs are not per se to be considered ESI.¹⁰ Additionally, IM is not typically stored in a medium from which it can be retrieved and examined.

While the distinction between E-mails and IM seems minor at first, the different treatment makes sense when one considers the use of each tool. IM is more similar to live conversations. They happen in real time with the expectation that the recipient will be available at that moment to receive the message. E-mails, however, more closely mimic traditional letters in which the sender is unsure of when the recipient will get the message. Letters and E-mails are also more formal, lengthier and likely more thought out (at least in theory) than live chats and IM. The most crucial difference for eDiscovery purposes, however, is that E-mails and hand-written letters are expected to be saved for future retrieval



Timothy J. Carroll, Esq.

and production, whereas live conversations and IM are thought to exist only in that moment and are not stored in an IT environment. Organizations must be aware of this practical difference and the early case law on the subject before deciding whether to archive and retain IMs.

Given the difficulties in managing E-mail, few in the in-house legal community should rush to begin archiving and retaining IMs. The first step in the analysis is to determine whether IMs are subject to the same retention and production requirements as other business records generated and/or stored by your organization. For some organizations, the Securities and Exchange Commission ("SEC") and the National Association of Securities Dealers ("NASD") have resolved that issue for you by promulgating rules that explicitly place a three-year retention requirement on IMs.¹¹ Companies regulated by these bodies must therefore take active steps to record and retain IM conversations. For those organizations that do not fall within the jurisdiction of those regulatory bodies, cautious scrutiny should be given to the issue of IM retention and production. Moreover, legal considerations, and not technology capabilities, should drive the debate.

Retention Alone May Not Be Enough

For organizations that must record and save IM exchanges,¹² there are two critical steps to ensuring that your IMs are properly maintained. First, a comprehensive retention policy and archiving system that allows for storage of IMs constituting business records is necessary. Second, organizations must have a secure and effective data authentication system in place to ensure that IMs can be admitted into evidence. As noted by U.S. Magistrate Judge Paul Grimm in his opinion in *Lorraine v. Markel*, "[i]f it is critical to the success of your case to admit into evidence computer stored records, it would be prudent to plan to authenticate the record by the most rigorous standard that may be applied."¹³ Without proper data authentication measures, the opposing party may contend that the relevant (and potentially helpful) IMs were altered, backdated or otherwise tampered with in an attempt to help your case.

Electronic tools such as IMs may be a quick means to communicate, but they, like many other forms of unstructured data, can be vulnerable to tampering. A person with some tech savvy can readily falsify or alter critical aspects of electronic records. In fact, employees who have been using IM for years would have little trouble altering IM or important metadata about IM conversations such as time and date or the conversation.

Because so many IMs are transmitted between users in a short span, an organization that saves such conversations would have a staggering amount of retained information to manage, making it difficult to detect tampering done to a minuscule portion of that data. However, it is easy to envision when such an alteration could make a huge difference in a lawsuit.

To avoid such scenarios, use of a trusted third-party digital time-stamping solution may be the most secure way to prove that your company's IMs and other electronic data have not been altered. Digital time-stamping solutions, such as Surety's AbsoluteProof, use a patented hash chain

linking method to prove, independent of any bias or human efforts, that records have not been altered since being sealed. In *Lorraine v. Markel*, Judge Paul Grimm noted that "hash values can be inserted into original electronic documents...to provide them with distinctive characteristics that will permit their authentication under [FRCP] Rule 901(b)(4)."¹⁴

Secure digital timestamps work by providing an electronic record with a file-agnostic hash function and then sending the hash to a third-party server via a secure Internet connection. The server then combines the hash, a secure timestamp and other traceable information to create a timestamp token. This token is affixed to the file and then securely archived. For added security, each file's hash and time value are linked to an unbroken hash chain that is widely published in order to guarantee long-term integrity by allowing anyone to validate the token. The widely witnessed publication of the hash chain also proves that no one, not even those with access to the tokens, has altered the hash chain.

If considering a data authentication solution, confirm that it meets the American National Standards Institute's standard for secure time-stamping. Using a solution like AbsoluteProof may allow an organization to gain a level of comfort on the issue of IM tampering and secure retention. Now that 93 percent of a business's records are kept electronically, a method of proving timing and content integrity is an integral part of a business's litigation readiness strategy. While the focus for now has been on what constitutes ESI and how to retain electronic records, organizations should take measures to properly authenticate these records so that all the time and money spent on retention and archiving is not wasted on inadmissible evidence.

¹ InternetNews.com, Gartner: Instant Messaging Reigns Supreme (June 26, 2007), <http://www.internetnews.com/ent-news/article.php/3685626>.

² Id.

³ Id.

⁴ ePolicy Institute, *Thirty-Two Instant Messaging Rules: Best Practices to Keep You and Your Business Out of Court* (May 2004), <http://www.epolicyinstitute.com/imr/32rules.pdf>.

⁵ 18 U.S.C. §§ 2510-22.

⁶ 18 U.S.C. § 2511(1)(a) (2006).

⁷ 18 U.S.C. §§ 2701-11 (2006).

⁸ *Amendments to Federal Rules of Civil Procedure, Rule 34(a)* (2006), http://www.uscourts.gov/rules/eDiscovery_w_Notes.pdf.

⁹ *Federal Rules of Civil Procedure, Rule 26(b)(2)(B)* (2006), <http://judiciary.house.gov/media/pdfs/printers/109th/31308.pdf>.

¹⁰ One of the contributors to the Judicial Conference noted that, because unsaved IMs exist in random access memory ("RAM"), they are retrievable only through significant effort, and that placing companies under an obligation to restore RAM would severely burden companies in the discovery setting. See Statement of Theodore Itallie, Associate General Counsel, Johnson & Johnson Public Hearing on Proposed Amendments to the Federal Rules of Civil Procedure (Feb. 11, 2005), available at www.uscourts.gov/rules/e-discovery.html. See also *Malletier v. Dooney & Bourke, Inc.*, No. 04 Civ. 5316, 2006 WL 3851151, slip op. at *2 (S.D.N.Y. Dec. 22, 2006) (holding that a party to a litigation hold is not required to install a system "to monitor and record phone calls coming in to [sic] its office on the hypotheses that some of them may contain relevant information").

¹¹ See 17 C.F.R. § 240.17a-4(b)(4) (2005); NASD Rule 3110 (2006).

¹² 17 C.F.R. § 240.17a-4(b)(4) (2005); NASD Rule 3110 (2006). See also *re Celera and Lexapro Prods. Liab. Litig.*, No. MDL 1736, 2006 WL 3497757, slip op. at *1 (E.D. Mo.) (ordering plaintiffs to preserve all instant messaging devices within a certain time frame).

¹³ *Lorraine v. Markel*, No. PWG-06-1893 at 48 (D. Md. May 4, 2007).

¹⁴ Id. at 25.

Please email the author at tcarroll@vedderprice.com with questions about this article.