
HR ADVISOR

Legal & Practical Guidance

**JANUARY/
FEBRUARY
2 0 0 6
VOL. 12/No. 1**

IN FLSA LITIGATION, IT'S ALL ABOUT THE PLAINTIFF'S ATTORNEY'S FEES **5**

A majority of FLSA actions have centered around one of two alleged violations: misclassification of employees as exempt from FLSA overtime requirements, or failure to compensate for so-called "off-the-clock" work. Some of these actions, particularly the alleged "off-the-clock" violations, only revolve around a few minutes of uncompensated time, yet their popularity has exploded.

Allan H. Weitzman and Elena J. Voss

USING RELEASES IN EMPLOYMENT TERMINATIONS **10**

At a time when employment litigation has almost become a routine part of running a business, it is not surprising that many employers have turned to the use of releases to protect themselves from liability when terminating an employee or groups of employees. Such a practice is advisable under certain circumstances, especially when the employer is providing severance benefits to terminated employees.

Janet G. Payton

NO-SMOKING POLICIES MUST CONTEND WITH STATE LAWS PROTECTING SMOKERS **29**

Tobacco use is a major contributor to a range of illnesses that account for a large percentage of health care costs incurred by employers. As a result, many employers are now considering plans to implement "no smoking" policies for their employees.

Stephanie V. Rosseau

INSTANT MESSAGING: FLEETING BUT FURIOUS **33**

Just as people are starting to get their arms around record retention requirements in general, companies these days have to figure out their obligations to preserve communications transmitted over public or private Instant Messaging systems. Given the uncertainty regarding the preservation of IM traffic, companies should at a minimum set certain guidelines for IM use.

Rodney Satterwhite

COMMENTS FROM THE EDITOR-IN-CHIEF	Allan H. Weitzman	3
TERMINATION OF EMPLOYMENT	Turning Down an Offer You Can't Refuse. Marty Denis, Esq.	38
THE HR TROUBLESHOOTER	Why Soldiers Make Good Employees. Gerard P. Panaro, Esq.	42
THE POLICY CORNER	EEO-1 Gets a Face Lift. Robert J. Nobile, Esq.	49

INSTANT MESSAGING: FLEETING BUT FURIOUS

Rodney A. Satterwhite

First it was paper; then microfiche; then email; then voicemail. Now the newest kid on the record retention block is, you guessed it (presumably from the title): Instant Messaging (“IM”). Just as people are starting to get their arms around record retention requirements in general, companies these days have to figure out their obligations to preserve communications transmitted over public or private IM systems. They are also wrestling with the decision of whether to implement a private

Rodney A. Satterwhite is a partner in the Richmond office of McGuire-Woods LLP. Practicing in the firm’s Labor and Employment Department, he tries cases and counsels clients in equal employment opportunity law, sexual harassment, employment contracts, non-competition agreements, wrongful discharge and employer trade secret protection. As Chief Counsel / Knowledge Management for the firm, he assists clients in the application of technology to litigation management. He participates in the design and development of extranets for improved attorney-client collaboration and communication, in the context of litigation and transactional work.

IM system that is a bit more controlled, or trying to regulate (and in some cases prohibit) employee use of public IM systems, such as AOL and Yahoo!, while on their work computers. Regardless of the answers to these questions, the need for some sort of policy addressing IM is nearly ubiquitous. This article explores some of the legal background giving rise to all this corporate angst.

SAVE OR SHRED: IS THERE AN OBLIGATION TO RETAIN IM TRAFFIC?

Existing IM Records

It would be nice for companies to be able to venture into the IM issue with a clean slate, but most already have a substantial amount of IM baggage in their systems. Sometimes employees will cut and paste an IM conversation into an email, text file or a word processing document and then save it just like any other document. Once this happens, IM loses whatever ethereal waif-like characteristics it might have possessed, and becomes a real live official corporate

document like any other. Thus, if IM traffic is already preserved in any way on Company systems, it should be subject to appropriate corporate record retention policies and guidelines. For obvious reasons, this can pose serious risks if employers don’t know what’s on those IM systems:

Instant Messaging (IM) is a form of electronic communication that involves immediate correspondence between two or more users who are all online simultaneously. Many employees use IM to circumvent their company’s email policy and say things they wouldn’t say in an email. Therefore, IM poses a significant litigation threat for companies and has the potential to be a “smoking gun.” Although the law is not well developed on whether companies must implement technology to capture Instant Messages, if an Instant Message is a record that must be retained by statutory or legal requirement, then, according to some, the company must take affirmative steps to ensure the message is retained.¹

Any record of IM traffic, once stored on a company system, may

be the subject of record retention requirements just as any other document or email might be. For example, Section 404 of the Sarbanes-Oxley Act of 2002², requires that corporate management establish and maintain "an adequate internal control structure and procedures for financial reporting." Final rules from the Securities and Exchange Commission implementing Sarbanes-Oxley require companies to keep appropriate documentation about these internal controls:

Therefore, the final rules do not specify the method or procedures to be performed in an evaluation period. However, in conducting such an evaluation and developing its assessment of the effectiveness of internal control over financial reporting, a company **must maintain evidential matter, including documentation, to provide reasonable support for management's assessment of the effectiveness of the company's internal control over financial reporting.** Developing and maintaining such evidential matter is an inherent element of effective internal controls.³

Because of the rising prevalence of IM in the workplace (Gartner Group forecasts that by 2006 more messages will be exchanged over IM than email), it is reasonable to conclude that some IM traffic will fall within the scope of "evidential material."

Similarly, any IM traffic which has been preserved would also be the subject of litigation holds and discovery requirements. *Zubulake v. UBS Warburg LLC*⁴, addresses a company's duty to preserve and produce, in a litigation context, electronic records. Specifically, the case dealt with emails, but has been interpreted by subsequent com-

mentary to apply to other types of electronic records as well, potentially including IMs. The case consisted of a claim of employment discrimination and retaliation. The employee claimed that the company's failure to preserve certain backup tapes and deleted emails constituted spoliation of evidence. The court held that the company was culpable with regard to the spoliation claims and granted the employee costs involved in further depositions, but denied the request for an adverse inference instruction because the employee failed to show that the lost evidence likely would have supported her claims. In so doing, the court addressed the company's duty to preserve electronic evidence:

Once a party reasonably anticipates litigation, it must suspend its routine document retention/destruction policy and put in place a 'litigation hold' to ensure the preservation of relevant documents. . . . If a company can identify where particular employee documents are stored on backup tapes, then the tapes storing the documents of 'key players' to the existing or threatened litigation should be preserved if the information contained on those tapes is not otherwise available. This exception applies to all backup tapes.⁵

Zubulake does not purport to impose any obligation to preserve electronic records, such as IM's that may not be automatically preserved. However, if these records are preserved, *Zubulake* sets guidelines regarding enforcement of the document retention/destruction policy when litigation is expected. Furthermore, to the extent that company policy is to not preserve IMs, and the company is technically capable of preserving them, a litigant may be able to argue that suspension of the compa-

ny's destruction policy requires preservation of IM's when litigation is expected.

When they Don't Exist: Affirmative Duty to Log IM Conversations

Although existing IM records are likely subject to document retention requirements, there does not appear to be any affirmative obligation for companies to track or log IM traffic on their systems. Although no court has specifically decided the issue, one has come close. *Convolve, Inc. v. Compaq Computer Corp.*⁶, addressed without deciding a company's duty to preserve IMs. However, the court's brief treatment of the IM issue sheds some light on how it would be likely to rule on the issue. There, Convolve claimed that Compaq had engaged in spoliation under *Zubulake* by failing to preserve certain intermediate steps that, Convolve argued, infringed its patent. The intermediate steps (consisting of wave forms that were manipulated en route to preparation of a final product) were, by their nature, transitive and were destroyed when further steps in the process were applied. The court held that *Zubulake's* requirement of a litigation hold did not apply to items such as the wave forms that had no "semi-permanent existence." The court then stated:

A somewhat analogous situation arises in the use of Instant Messenger functions. There the question may be a closer one both because at least some Instant Messenger programs have the capability, like e-mail, of storing messages, and because such information is intended to be transmitted to others. I offer no opinion here on the circumstances under which the failure to preserve Instant Message

communications would be considered spoliation.⁷

The court's indication in *Con-volve* is that it may consider the technological capabilities of preserving IMs as well as a company's policy of IM retention, in deciding a spoliation claim based on failure to preserve such records.

Similarly, some commentators have suggested that the nature of Instant Messaging is more akin to a telephone conversation than an email exchange.

Like a phone conversation, an IM communication is a real-time dialogue between two or more people. ...The text of the entire conversation generally appears in a small user interface window on a user's screen. When a user closes the IM window, the content of the conversation disappears from view. ...Consistent with the treatment of the conversations that IM communication replaces in the corporate environment, it is not necessary to record such IM interactions, unless doing so is the pre-established business practice of the IM user.⁸

Applying this logic, therefore, a company could argue it has no duty to create records by affirmatively tracking or logging IM conversations:

Although a litigant may be required to compile existing data, it generally may not be compelled to create information that is not and has never been in existence. Thus, while tape recordings of conversations may be considered "stored information" subject to preservation if litigation is anticipated, a party is under no affirmative duty to record oral communications that have not otherwise been recorded in the ordinary course of business. The same would seem logically to apply to IM conversations not recorded by

the participants in the conduct of their daily business.⁹

WHAT'S LOOMING ON THE HORIZON: THE FUTURE OF IM RETENTION REQUIREMENTS

Despite the logic of this conclusion, certain actions among courts and regulatory agencies mandate that companies continue to monitor and periodically reevaluate their policies regarding the retention of IM traffic. In the criminal context relating to the prosecution of sexual predators, one court has acknowledged that the mere exchange of words during an IM conversation creates a record—albeit short-lived—of the conversation:

Instant Messaging is a form of computer communication in which individuals hold an online conversation via the Internet. When a person sends an Instant Message to another person online, that message is transmitted instantaneously to the recipient, opening a [chat] window that allows both parties to see the message and to respond immediately. The [chat] window, while open, **contains a complete history of all messages sent and received during the online conversation.**¹⁰

Similarly, another court deciding a motion to suppress evidence in a criminal matter, recognized that Instant Messaging traffic can be stored data by virtue of its receipt of the transmitted message:

While either a computer or a computer Instant Messaging program is capable of being a medium of conversation, each is also simultaneously capable of being used as a recording device.... Like an email message and a message left on an answering machine, the recording of the Instant Message is necessary for the intended recipient of that message to read the message.¹¹

Thus, while the analogy of Instant Messaging to a telephone conversation may be logical and persuasive, these decisions suggest that some courts will view Instant Messaging conversations as a stored record at the time of receipt, regardless of whether they are actually tracked, logged or archived. Should this analysis be adopted in the civil context, corporations may be held accountable for appropriate retention of Instant Messaging conversations when they actually occur.

Additionally, the prevalence of Instant Messaging in certain regulated industries has resulted in requirements that companies affirmatively archive and preserve Instant Message traffic on their systems.

The financial industry enacted regulations regarding the retention of IMs (as well as email). NASD Rule 3110 and SCC Rule 17-A4(b)(4) require that members retain IM's for three years. The NASD further indicated that members should not use IM platforms that do not support archiving and retrieving of IM's. The notice further provided that if a member cannot establish an adequate supervisory program, the member must prohibit the use of Instant Messaging. Similarly, the FDIC suggested that financial institutions use corporate versions of IM that allows for messages to be monitored and logged. They also directed financial institutions to draft written policies regarding IM usage.¹²

Although these regulations do not apply directly to companies outside the reach of NASD rules, the increased use of IM in the workplace, combined with the potential for courts to treat these conversations as corporate records, warrants a close continuing scrutiny of this issue.

WHAT TO DO - WHAT TO DO - REGULATING EXISTING IM USE

Like it or not, most companies have at least some employees who are currently using public IM systems (such as AOL Instant Messenger, MSN Messenger, or Yahoo! Messenger) to communicate with one another, and with the outside world. A company's obligation to preserve this IM traffic is subject to the same analysis discussed above. However, the nature of public IM systems may create additional practical burdens for these companies.

Most importantly, public IM systems give individual users the capability of logging and archiving.

Similar to email and other computer data, Instant Messages do not disappear when the Instant Message window closes. Many of the free and widely-used Instant Message programs have the ability to generate text copies of all incoming and outgoing messages, as long as the archival/logging function is enabled [by the individual user]. For now, however, there is no real way to automate the extraction of these logs. Thus, the process is burdensome and time consuming. This is one reason why some companies are implementing enterprise-wide Instant Message control and logging solutions.¹³

Thus, permitting employees to have unregulated use of public IM systems increases the risk that some employees will turn on (or simply fail to turn off) automatic logging. As discussed above, once those IM conversations reside on company computers, they become corporate documents subject to record retention requirements and discovery requests. Under *Zubulake*, companies and their counsel are obligated to locate all sources of relevant in-

formation, including records retained at individual levels:

Once a "litigation hold" is in place, a party and her counsel must make certain that all sources of potentially relevant information are identified and placed "on hold," to the extent required in *Zubulake*. To do this, counsel must become fully familiar with her client's document retention policies, as well as the client's data retention architecture. This will invariably involve speaking with information technology personnel, who can explain system-wide backup procedures and the actual (as opposed to theoretical) implementation of the firm's recycling policy. It will also involve communicating with the "key players" in the litigation, in order to understand how they stored information. In this case, for example, some UBS employees created separate computer files pertaining to *Zubulake*, while others printed out relevant e-mails and retained them in hard copy only. Unless counsel interviews each employee, it is impossible to determine whether all potential sources of information have been inspected. A brief conversation with counsel, for example, might have revealed that Tong maintained "archive" copies of e-mails concerning *Zubulake*, and that "archive" meant a separate on-line computer file, not a backup tape. Had that conversation taken place, *Zubulake* might have had relevant e-mails from that file two years ago.¹⁴

If employees are permitted to create individual archives of IM conversations, then companies may have a duty to search those archives when they are implicated in discovery requests. This will potentially be more burdensome, and create additional costs, when compared to the ability to extract such material from a central archived system.

INSTANT MESSAGING POLICY

Given the uncertainty regarding the preservation of IM traffic, companies should at a minimum set certain guidelines for IM use. These guidelines can be incorporated into existing Acceptable Use Policies (AUPs) that cover employee email and internet use, but should take into account the following:

- A reminder that employees cannot expect any confidentiality when using any company communication systems, including IM.
- A reminder of any existing policies that govern any of their communications, including avoiding sexual harassment, avoiding discrimination, etc.
- A reminder that employees must be extra vigilant in complying with these policies in the chatty world of IM.
- A statement of the Company's policy on personal use of IM (this should be consistent with the Company's position on personal use of email and other electronic communications).
- Possible prohibition on employees downloading their own IM software from AOL, Microsoft, etc.
- To the extent that the Company can search for any personally downloaded software, the policy should advise employees that it will do so.
- If the Company cannot or does not prohibit employees from downloading IM software (or otherwise using personal IM means for com-

pany business), it should declare whether employees are required to retain messages related to company business.

- A statement whether employees are allowed to use IM to communicate with others outside the Company. This will be difficult to prohibit, given the nature and purpose of IM, but should be squarely addressed by the policy.
- If the Company allows its employees to use IM with outsiders, the policy should emphasize: the dangers that this use poses to the attorney client privilege; intellectual property risks; and statutory, regulatory and other duties of confidentiality.
- A reminder that any IM message cut and pasted into an e

mail or any other form of communication will be governed by that form of communication's rules (including any retention rules).

- If employees are logging IM conversations, the policy should include a reminder that retained IM is subject to the standard corporate document retention rules.
- Advise employees that the technology and law in this area are changing rapidly, and they might eventually be required to retain IM as a result of technological advancements, statutory or regulatory requirements (as in the financial institution world) or other developments (including case law).

NOTES:

1. "The Challenge of Electronic Records," *The Corporate Counselor*, June 2005.
2. 15 U.S.C.A. § 7262.
3. SEC Final Rule Summary, Release No. 33-8238 (www.sec.gov/rules/final/33-8238.htm).
4. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212 (S.D.N.Y. 2003).
5. *Zubulake v. UBS Warburg LLC*, 220 F.R.D. 212, at 218 (S.D.N.Y. 2003).
6. *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162 (S.D.N.Y. 2004).
7. *Convolve, Inc. v. Compaq Computer Corp.*, 223 F.R.D. 162, at 177 n.4 (S.D.N.Y. 2004).
8. "Are Instant Messages Discoverable?" *National Law Journal*, June 7, 2004.
9. "Are Instant Messages Discoverable?" *National Law Journal*, June 7, 2004.
10. *State v. Bouse*, 150 S.W. 3rd 326, 329 n.2 (Mo. Ct. App. 2004) (emphasis added).
11. *See Com. v. Proetto*, 2001 Penn. Sup. Ct. 1995, 771 A. 2nd 823, 830 (Penn. Sup. Ct. 2001) ("sending an email or chat room communication is analogous to leaving a message on an answering machine").
12. "The Challenge of Electronic Records," *The Corporate Counselor*, June 2005.
13. "The Challenge of Electronic Records," *The Corporate Counselor*, June 2005.
14. *Zubulake v. UBS Warburg LLC*, 2004 U.S. Dist. LEXIS 13574, 32-34 (D.N.Y. 2004).