
Managing Your Workplace in an Electronic Age

**Internet, E-Mail,
Cell Phones, and More**

Julie Athey

Attorney

M. LEE SMITH PUBLISHERS LLC
Brentwood, Tennessee

This special report provides practical information concerning the subject matters covered. It is sold with the understanding that neither the publisher nor the writer is rendering legal advice or other professional service. Some of the information provided in this special report contains a broad overview of federal law. The law changes regularly, and the law may vary from state to state and from one locality to another. You should consult a competent attorney in your state if you are in need of specific legal advice concerning any of the subjects addressed in this special report.

© 2007 M. Lee Smith Publishers LLC
5201 Virginia Way
P.O. Box 5094
Brentwood, Tennessee 37024-5094
ISBN 1-60029-027-2

All rights reserved. No part of this book may be reproduced or transmitted in any form or by any means without permission in writing from the publisher.

Printed in the United States of America

Contents

INTRODUCTION	1
1 — ELECTRONIC COMMUNICATIONS	3
E-mail Decorum	3
Confidential Information	5
Pornography	6
Gone, but Not Forgotten	7
Computer Viruses	8
2 — INTERNET USAGE	9
Pornography	9
Copyright Violations	10
Loose Lips	11
Final Thoughts About Productivity	13
3 — ELECTRONIC SECURITY	15
Online Security Threats	15
Laptops and Personal Digital Assistants	18
Identity Theft	20
4 — CELL PHONES AND OTHER ELECTRONIC DEVICES	23
Driving While Distracted	23
Other Misuse of Cell Phones	26

5 — MONITORING EMPLOYEES	29
Deciding Whether to Monitor	29
Applicable Laws	31
6 — THE ELECTRONIC COMMUNICATIONS PRIVACY ACT	35
Scope and Coverage	35
Monitoring Telephone Conversations	36
E-mail and Internet Usage	38
Voice Mail Communications	39
Video and Audio Surveillance	40
7 — A MONITORING POLICY: YOUR BEST DEFENSE	41
Drafting Your Policy	42
After Drafting Your Policy	43
8 — THE PLUSES AND PITFALLS OF E-RECRUITING	45
Is E-Recruiting the Right Tool for You?	45
Potential Liabilities	46
Disparate Impact Discrimination	46
Other Concerns	47
Dangers of Resume-Screening Software	47
9 — WHEN THE UNION COMES SURFING	49
No-Solicitation Rules Apply to E-mail	49
What Can You Do to Limit Online Organizing?	50
A FINAL WORD	51
Notes	51

Introduction

Computers, e-mail, the Internet, and other technological advances have brought a new age of ease and efficiency to the workplace. Just think about the many changes that have occurred in the last 15 years alone. In 1993, the vast majority of people hadn't even heard of the Internet, and there was no such thing as e-mail. Nowadays, most employees who work in an office have a computer and Internet and e-mail access. And increasing numbers of employees rely on a host of other technological goodies such as laptops, personal digital assistants (such as BlackBerries or Palm Pilots), and cell phones that offer an ever-expanding array of features.

If you think about it, the benefits that these advances in technology offer are truly remarkable. The advent of increasingly powerful laptops, PDAs, and cell phones has made it possible for many employees to work almost anywhere they want to — and to take a “virtual” office with them. The answer to practically any question can be found on the Internet . . . most of it for free. Vast amounts of information can be gathered, stored, and exchanged with a few clicks of the mouse.

But along with all those benefits comes new and often unexpected risks. As new technologies continue to be developed and introduced into the workplace, too many employers find themselves the unwitting subject of technology-related missteps and litigation. For example:

- Can you guarantee that your employees aren't using their computers to access and distribute inappropriate material (such as pornography or racist jokes) to other employees?
- Have you protected yourself from their failure to observe trademark laws in accessing and sharing files or software on the Internet?
- How can you protect confidential company and employee information from being technologically hijacked?
- Do you have a policy that takes into account all the latest cell phone features — such as the ability to take pictures and video clips, access the Internet, send and receive text messages, and so on?
- Do you have policies in place to legally monitor employee e-mails and Internet use without violating their privacy or running afoul of the Electronic Communications Privacy Act (ECPA)?
- If you use computer-based hiring techniques, are you sure they won't result in inadvertent discrimination against job applicants that fall into a particular protected class?

On top of the potential legal hassles and liabilities, most employers find themselves confronted with the question of how to make sure employees are

Too many employers find themselves the unwitting subject of technology-related missteps and litigation.

using their work computers in an appropriate and productive manner. For example:

- How do you make sure employees aren't spending hours unproductively surfing the Internet, blogging, sending personal e-mails, text messaging, instant messaging, and so on?
- How can you legally prevent them from using your e-mail system to organize a union campaign when they should be working?

These issues are just the tip of the iceberg! In order to increase employee productivity and decrease the chances of litigation, it is worth your time and effort to develop well-thought-out policies and procedures regarding your organization's and employees' use of technology. This report is designed to help you do just that.

Electronic Communications

1

We live in the age of real-time electronic communications, but unfortunately not everyone has figured out how best to handle this brave new world. Not only must employers and their employees develop a sense of e-mail etiquette, many must also learn how to navigate the fast-paced world of e-mail's younger cousins, the instant message (IM) and text message (TM).

For the uninitiated, IMs are typed messages sent from and to a personal computer in real time. In other words, it's like you're talking on the phone, only you're typing back and forth instead of talking. Text messages are the same, except that they are sent and received by phone — usually a cell phone — or PDA.

As the use of e-mail, IMs, and TMs has become so prevalent, so also have the practical and legal problems associated with them. Just a few years ago, not many companies were worrying about the potential for harassing, discriminatory, or otherwise damaging electronic communications. Today, most employers have implemented — or are in the process of implementing — policies to guard against liability or other damage from what their employees say in or attach to their electronic communications.

E-MAIL DECORUM

Electronic communications can be dangerous in ways that don't have anything to do with legal troubles. Most of the problems arise out of the fact that people tend to treat them more as friendly (or not so friendly) conversations than as formal business communications. Electronic "conversations" are not typically reviewed or edited carefully and may not be "spoken" with the same sense of purpose as a letter or memo. It is also extremely easy for the recipient to misinterpret the sender's "tone of voice," leading to misunderstandings and conflicts. Some of those conflicts may be the kinds of things that can lead to a lawsuit, but most are simply bad for business.

And don't we all have an e-mail horror story in which a totally inappropriate message has fallen into the hands of just the person who was never supposed to see it? You know what I'm talking about . . . like the time you carelessly posted something to everyone on a listserv instead of only to the person you intended to respond to. Or when the supposed-to-be-helpful-but-is-really-more-annoying "auto-complete" feature on your e-mail software filled in the name you started to type with the name of a different person entirely.

Or you sent a snappy reply to a forwarded message thinking that you were replying to the person who forwarded it.

These types of mistakes are so easy to make, you have to take them seriously. They may usually be humorous and harmless, but companies have been known to lose customers and clients because an employee accidentally sent them a snarky comment. It's just one reason why employees should be trained to always use restraint in drafting their e-mails, even when they think they're "talking" to someone they can trust.



POLICY POINTER

Employees should be trained to always use restraint in drafting their e-mails.

Train your managers and staff to treat their electronic communications with the same care as any other business communication:

- Remind them that carelessly worded messages, discriminatory comments, and thoughtless criticisms of employees or clients have no place in the workplace.
- Impress upon them the importance of reviewing every e-mail carefully before it's sent. Professionalism is important, even in e-mails, and that includes using good grammar and correct spelling and punctuation.
- Suggest that they "sleep on" any message they might draft in anger or frustration before sending it — even to a friend or coworker. You never know when the recipient might forward it on to someone else — whether intentionally or not.

The E-mail Express

A related concern is the ease with which employees can copy and forward e-mail to countless people. If an employee says or puts something inappropriate in an e-mail, even he doesn't know where that e-mail may eventually wind up. E-mail recipients can easily save, print, and forward them to 100 people worldwide, who can forward them on to another 100 people, and so on.

In this way, one inappropriate joke or image can literally make its way around the world — and, more importantly, around your company! The more employees who receive the inappropriate message, the more likely it is that one of them will be offended enough to raise a stink, quit, or sue.

Communicating in Code

IMs and, in particular, TMs have taken on a life of their own — especially among the younger generation. Because IMs and TMs take place in "real time," people have had to find ways to communicate more quickly in writing. Literally thousands of abbreviations have popped up to replace the phrases that would normally be used in an oral dialogue. For example, "BF" stands for "best friend" and "my DH" means "my dear husband" (or a different adjective,

depending on your mood). Some of the other most common abbreviations include B/C (for “because”), B4 (for “before”), and IMO or IMHO (for “in my opinion” or “in my humble opinion”).

In addition, acronyms are frequently used to convey the intended tone of the message or as a less blatant form of a profanity. For example, LOL is short for “laughing out loud” (used to let the reader know you’re kidding) and LMAO is short for “laughing my” Oh, you can figure it out.

Another way to let people know your intent in an electronic communication is to add an “emoticon” — which is just a big word for the little smiley faces that appear in e-mails or web postings to let people know the writer’s mood. For example, the phrase “Well, that’s just swell!” could have very different meanings depending on whether there’s a smiley face next to it or an “angry” emoticon.



POLICY POINTER

Although abbreviations, acronyms, and emoticons can be fun, your employees should be instructed not to use them in an attempt to ensure clarity in their work-related electronic communications. In other words, if an employee cannot express herself clearly in writing, then maybe she needs to be working on her communication skills instead of downloading all the latest emoticons from smileyface.com.

Time’s a Wastin’

Some employees send and receive so many e-mails, IMs, and TMs that you have to wonder where they find time to do their jobs. It may not take long to send an individual message, but the cumulative effect can greatly impede an employee’s productivity.

One way to deal with this is to set limits on employees’ personal use of e-mail and other electronic communications in the workplace. If you don’t want them to send or receive any personal messages at all, then you should have a policy clearly stating that. It’s a pretty hard-line approach to take, but it may be warranted in some cases.

For most employers, it’s better to prohibit excessive personal e-mail, IMs, and TMs. Anything more than that is probably not worth the ill will it will cause among your employees.

CONFIDENTIAL INFORMATION

Most employers have trade secrets or confidential information they would rather not see in the hands of their competitors. E-mail can pose a serious risk to

those types of information. Employees have been known to attach trade secrets, customer lists, and other sensitive information to their outgoing e-mails.

This is not a safe practice even when the employee means no harm or the intended recipient is an appropriate one. There are too many ways for e-mail to be intercepted or accessed by — or forwarded to — the wrong people. Make sure employees understand that e-mail should not be considered a secure means of communication, and that they should not say or write anything in an e-mail that they would not want someone other than the intended receiver to hear or read.

Of course, there is also the danger of a disgruntled employee who e-mails confidential information to a competitor, or a fired employee who takes time to e-mail his customer list to his home computer on his way out the door. Employers need to have comprehensive security measures to prevent that from happening — for example, by preventing employees who are being fired from accessing their work computers.

PORNOGRAPHY

Want to hear a statistic that will turn your hair gray? An April 2007 survey found pornographic or other inappropriate images on more than 25 percent of 10,000 corporate and public sector computers audited in a nine-month study.¹ A few of the study's most worrisome findings include:

- More than 46 percent of the images were found to show full nudity or sexual activity. A small percentage of the images were actually illegal.
- Forty-five percent of the images were traced to e-mails (35 percent were downloaded from the Internet).
- Of the images that were traced to e-mails, almost 20 percent were contained in outbound e-mails.

Just think about that last statistic for a minute. Twenty percent of the e-mailed pornography found was contained in *outgoing e-mail*.² Given the fact that most companies' names are part of their employees' e-mail addresses, those e-mails were probably identifiable as coming from a specific employer. So the question is, does your company want its name to appear in a pornographic e-mail? Not to mention that you don't want other employees to be exposed to the pornography, whether intentionally or not.



POLICY POINTER

Employers that want to prevent employees from receiving pornography attached to e-mails have several options. First, you should have a policy specifically prohibiting pornography in the workplace. Second, you should consult with your IT department

to discuss possible methods of blocking the receipt of pornographic e-mails. Finally, you should consider implementing a monitoring policy if you don't already have one. Monitoring policies are discussed in more detail in Section 7.

GONE, BUT NOT FORGOTTEN

When lawyers proclaim the hazards of e-mail and other electronic communications, they are usually referring to the fact that such messages are likely to exist in some form long after they are sent, received, and deleted. So if an e-mail, TM, or IM contains things that it shouldn't — such as racist jokes, pornographic images, or harassing statements — chances are that it will show up as evidence in any subsequent litigation.

That's because e-mail messages and other electronic communications or records can be used as evidence in court, just as paper documents are used. Lawyers are becoming more aware of the need to uncover this type of evidence . . . and more sophisticated in doing so. If your company is involved in litigation, the other side's attorney might be able to uncover incriminating evidence on your computer systems that everyone involved had thought was long banished to that big electronic landfill in the sky.³

In addition, if there are electronic records that *should* exist but you can't produce them, a judge or jury may assume they contained information that would have been damaging to your case. For example, let's say you're sued for sexual harassment and part of the case involves harassing e-mails and Internet pornography. If you tossed out the accused employee's computer and don't have any backup tapes to show his computer usage during the time in question, it's possible that will be used against you at trial.

Don't ever dispose of electronic (or other) records that relate to a pending investigation, complaint, or lawsuit.



POLICY POINTER

Don't *ever* dispose of electronic (or other) records that relate to a pending investigation, complaint, or lawsuit — even if they are scheduled to be legitimately disposed of under a records retention policy.

If you don't yet have a record retention policy that specifies when and how certain types of records are to be disposed of or destroyed, then now is the time to get one. Consult with your computer and security personnel to tailor a plan to safely dispose of old hard drives (especially old servers), disks, and backup media that is suited to your particular business operations. In general, you will want to find a solution that is both dependable and cost-effective.⁴

COMPUTER VIRUSES

When you hear about a particularly nasty computer “virus,” chances are it may not be a virus at all, but a “worm” or “Trojan horse.” These malicious programs gain access to your computer systems in different ways, but the most common way is as an apparently harmless attachment to an e-mail. They have been known to cause Web servers, network servers, and individual computers to shut down, delete files, steal or destroy information on your computer, and allow malicious users to control it remotely.

By now, most employers should have technology-based protections in place to prevent their computer systems from becoming infected by these malicious forms of software. Because new viruses are always being created, however, no virus detection software can be effective 100 percent of the time. The best way to protect your company from viruses is to have strong policies and training in place to ensure that employees know how to avoid infecting your network.



POLICY POINTER

Make sure your IT department has initiated adequate measures to protect your company’s computers from viruses. You might also want to seek their help in educating employees. Your e-mail policy should:

Prohibit employees from opening e-mail from unknown sources or e-mail attachments.

- Prohibit employees from opening e-mail from unknown sources or e-mail attachments — at least not without taking certain precautions;
- Prohibit employees from forwarding any inappropriate e-mails they may receive; and
- Instruct employees to notify the HR or IT departments of any computer problems, including unexplained computer glitches or excessive amounts of e-mail or spam.

You might also want to:

- Prohibit employees from opening spam and require them to notify you if they have a spam problem.
- Talk to your computer systems employees to see if they recommend using filters to screen out incoming spam.

Note that viruses and other forms of malicious software can infect your systems in ways other than e-mail, such as if they are attached to documents or software that an employee loads onto his computer from a CD or the Internet. Malicious software that is unknowingly downloaded from the Internet is called “malware,” and it seems to have taken over from viruses and spam as Computer Enemy Number One. More about this type of threat in Section 4.

ORDER FORM

If you would like additional copies of this special report or any other of our **HR Executive Special Reports** for your supervisory or managerial staff, please use the convenient order form below. *Discounts available on multiple copies of individual titles. Please call 800-274-6774 for more information.* Please add \$6 to your total order for shipping and handling.

	Quantity	Unit Cost	Price
<input type="checkbox"/> Employee Privacy Rights & Wrongs	_____	x \$97	= \$_____
<input type="checkbox"/> Workplace Violence & Employer Liability	_____	x \$97	= \$_____
<input type="checkbox"/> How to Conduct Internal Investigations	_____	x \$97	= \$_____
<input type="checkbox"/> How to Manage Problem Employees	_____	x \$97	= \$_____
<input type="checkbox"/> FMLA, ADA & Workers' Comp: Navigating the Treacherous Triangle	_____	x \$97	= \$_____
<input type="checkbox"/> How to Fire Employees Without Getting Burned	_____	x \$97	= \$_____
<input type="checkbox"/> The Company You Keep: Four Key Tools for Employee Retention	_____	x \$97	= \$_____
<input type="checkbox"/> A Legal Guide to Successful Hiring	_____	x \$97	= \$_____
<input type="checkbox"/> The H in OSHA Stands for Health	_____	x \$97	= \$_____
<input type="checkbox"/> Workplace Harassment Trail Guide: Avoiding the Avalanche Zone	_____	x \$97	= \$_____
<input type="checkbox"/> FMLA Leave: A Walk Through the Legal Labyrinth	_____	x \$97	= \$_____
<input type="checkbox"/> Ten Commandments for Avoiding Religious Harassment and Discrimination Claims	_____	x \$97	= \$_____
<input type="checkbox"/> ADA from A to Z	_____	x \$97	= \$_____
<input type="checkbox"/> How to Manage Your Aging Workforce	_____	x \$97	= \$_____
<input type="checkbox"/> How to Discipline & Document Employee Behavior	_____	x \$97	= \$_____
<input type="checkbox"/> How to Make Background Checks Part of Your Hiring Process	_____	x \$97	= \$_____
<input type="checkbox"/> Know Your Responsibilities: Ethics & Fiduciary Duties for HR	_____	x \$97	= \$_____
<input type="checkbox"/> How to Manage & Minimize Absenteeism	_____	x \$97	= \$_____
<input type="checkbox"/> Overtime Ins and Outs: How to Comply with the FLSA	_____	x \$97	= \$_____
<input type="checkbox"/> How to Comply with COBRA Without Getting Bit	_____	x \$97	= \$_____
<input type="checkbox"/> How to Evaluate & Manage Employee Health Plans	_____	x \$97	= \$_____
<input type="checkbox"/> How to Make Telecommuting Work for Your Company	_____	x \$97	= \$_____
<input type="checkbox"/> Defamation in the Workplace	_____	x \$97	= \$_____
<input type="checkbox"/> Stop It Before It Starts: The HR Manager's Guide to Preventing Sexual Harassment	_____	x \$97	= \$_____
<input type="checkbox"/> Reducing Risk for Reductions in Force	_____	x \$97	= \$_____
<input type="checkbox"/> Managing Your Workplace in an Electronic Age	_____	x \$97	= \$_____

Subtotal \$_____

plus shipping and handling \$ 6.00

Grand Total \$_____

Bill me My check is enclosed VISA MasterCard American Express

Card # _____ exp. _____

Signature _____

Name _____

Company/Title _____

Address _____

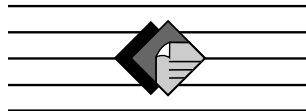
City/State/Zip _____

Phone _____ Fax _____ E-mail _____

HRBKPG

For faster service call toll-free 800-274-6774 or fax this form to 800-785-9212
Mail this form to: M. Lee Smith Publishers LLC • 5201 Virginia Way • P.O. Box 5094 •
Brentwood, TN 37024-5094 • <http://www.mleesmith.com> • E-mail: custserv@mleesmith.com

**If you would like more information on our many products
and services for human resource professionals,
please call our customer service department at
800-274-6774 and request a copy of our Product Guide.
You may also E-mail us — custserv@mleesmith.com**



**M. Lee Smith
Publishers LLC**