



## **From E-Mail & IM to Social Networking & Texting... *How to Communicate Online Without Getting Fired, Sued, or Publicly Humiliated***

### **Tip #1: Big Brother Is Reading Over Your Electronic Shoulder**

There simply is no privacy in cyberspace. Employers, law enforcement agencies, courts, regulators, the media, and the public are likely to access your online transmissions, posts, and history one day—if they haven't done so already.

When it comes to workplace computer monitoring, North American employers are primarily concerned about inappropriate web surfing, with 66 percent of bosses watching workers' Internet connections, and another 45 percent tracking content, keystrokes, and time spent at the keyboard. An additional 43 percent of employers monitor employee e-mail, either taking advantage of software to accomplish the job automatically (73 percent) or assigning an individual to manually read and review workers' messages (40 percent), according to the **2007 Electronic Monitoring and Surveillance Survey from American Management Association (AMA) and The ePolicy Institute.**

Employee use of new and emerging technologies is under scrutiny at work, too. Twelve percent of bosses regularly monitor the blogosphere, and another 10 percent keep an eye on social networking sites to determine what type of content employees, disgruntled ex-employees, competitors, customers, critics, fans, and others are posting about the company, its people, products, and services.

### **Tip #2: North American Employees Have No Reasonable Expectation of Privacy When Using Company Computer Systems**

In the United States, the federal Electronic Communications Privacy Act (ECPA) makes it clear that a company-provided computer system is the property of the employer. Employees, therefore, have absolutely no reasonable expectation of privacy when using the system to transmit e-mail, surf the web, or engage in any other form of electronic communication.

U.S. courts have consistently ruled that employees should assume that their workplace computer activity is being watched—even if they have not been formally notified of monitoring. While only two states, Delaware and Connecticut, legally require employers to notify staff that their online activity is being monitored, the court system generally supports the position that informed employees neither would nor should assume that their e-mail transmissions are their own. Even in cases in which employers have told workers that incoming and outgoing e-mail is *not* being monitored, the courts have ruled that employees still should not expect privacy when using a company-provided e-mail system.

Private employers in employment-at-will states (which most states are) have the right to fire employees for just about any reason—including accidental and intentional e-mail violations and inappropriate Internet use. So, if you are thinking about filing an invasion of privacy lawsuit to protest computer monitoring or a wrongful termination claim in response to your e-mail or Internet-related termination, think again. It's unlikely you will have much luck making your case in court.

**Tip #3: European/International Law Looks More Favorably on Employee Privacy**

In the United Kingdom, Germany, Australia, and many other countries, a premium is placed on employee privacy. English law, for example, allows organizations to monitor web surfing and e-mail transmissions, but employers are legally required to alert employees to monitoring and must use the least intrusive surveillance methods possible, according to Attorney Tamzin Matthew of U.K.-based Blake Lapthorn Tarlo Lyons. Before implementing domestic monitoring procedures and privacy policies abroad, U.S. employers are advised to seek the counsel of a lawyer who is familiar with the legal, regulatory, and privacy requirements of each country in which your organization operates.

**Tip #4: Your Boss Isn't the Only One Monitoring Your Electronic Transmissions**

Every time you send an e-mail message, your intended recipient's employer and the employers of any unintended readers to whom your message is forwarded or copied gain access to your e-mail. Consequently, your business and personal e-mail could be archived (possibly forever) and (in the event of a lawsuit, regulatory investigation, or Freedom of Information Act request) turned over to courts, regulators, and reporters, along with the company's own business record e-mail and other electronically stored information. If you engage in instant messaging, and your company or your IM buddy's organization is among the 13 percent of businesses that retain instant messenger chat, according to AMA/ePolicy Institute research, then those brief, real-time conversations also are subject to review by unintended readers.

**Tip #5: E-Mail Creates the Electronic Equivalent of DNA Evidence**

Fully 24 percent of U.S. employers have had e-mail subpoenaed by courts, and another 15 percent have gone to court to battle lawsuits triggered by employee e-mail, according to the **2006 Workplace E-Mail, Instant Messaging & Blog Survey from American Management Association and The ePolicy Institute**. If you use a company e-mail system to transmit personal messages, there's a good chance that your private (potentially embarrassing and career-altering) e-mail has been saved and stored right along with business-critical e-mail. Should a lawsuit or other investigation hit, expect to see your personal e-mail messages, IM chat, and history of web surfing subpoenaed and made available to judges, lawyers, forensic investigators, jurors, expert witnesses, the media, and the public. To prevent potential embarrassment, save your personal correspondence and surfing for your home computer.

### **Tip #6: Writing or Posting Videos about Your Job, Boss, or Coworkers May Get You Fired**

Whether working on company equipment during business hours or on personal technology tools at home after work, posting text, photos, or videos about your company, its people, products, and services can be an express route to the unemployment line—regardless of whether your postings are negative or positive.

Whether blogging on the company's business blog, social networking on Facebook, sharing videos on YouTube, or operating your own personal web site, never write about or otherwise reference your employer or job without formal authorization from management. That means no mentions of your company, boss, or colleagues. No references to your job title or work assignments. No photos of yourself or other staff in company uniforms. No videos of company facilities, products, or people. No posting of your business card, corporate e-mail address, or company letterhead. No use of trademarks, logos, or other visual identifiers. No links to company-operated web sites or blogs. Violate this rule today, and you may find yourself out of work tomorrow.

### **Tip #7: Anonymous Posts Do Not Guarantee Protection from Detection**

Anonymity creates an atmosphere in which some people might be tempted to post content that may be irresponsible, offensive, harassing, defamatory, or otherwise inappropriate. At the end of the day, however, there is no guarantee that anonymous blogging or other nameless postings will protect closeted writers from detection.

Consider the case of Heather Armstrong, the blogger who is credited with coining the term "dooced," which means to lose your job for blogging. According to *The New York Times*, Armstrong used her blog Dooce.com to complain "colorfully about everything from her boss to obnoxious coworkers." While she kept the name of her employer a secret, never revealing the name of the software company that employed her, one reader did not share her sense of discretion. That reader not only figured out where Armstrong worked, but also followed up with an e-mail to Armstrong's employer, detailing the nature of the blogger's rants. Armstrong was fired immediately.

### **Tip #8: Familiarize Yourself with Your Employer's Rules and Policies First; Log On Second**

Don't communicate online until you have read (and understand) all of your organization's employment policies, including e-mail, Internet, IM, blog, cell phone, text messaging, and social networking rules. Familiarize yourself with the company's electronic communication guidelines, code of conduct, confidentiality rules and policies, sexual harassment and discrimination guidelines, and any other rules and policies your employer may impose. Watch your language and adhere to all employment policies—unless you want to lose your job over an e-mail gaffe or thoughtless text message!

### **Tip #9: The First Amendment Does Not Protect Bloggers or Social Networkers**

Do you believe that, under the First Amendment, you have a right to say whatever you want on a personal blog, social networking site, or video sharing site? Many U.S. bloggers and social networkers mistakenly believe that the First Amendment protects their jobs. It doesn't. The First Amendment only restricts government control of speech; it says nothing about private employers. Until recently, government employees had some First Amendment protections not available to private sector employees. No longer. The U.S. Supreme Court recently ruled that government entities are free to fire employees if their comments—online posts included—are harmful to the mission and function of the workplace.

**Tip #10: Don't Be Lulled Into a False Sense of Security by Personal E-Mail Accounts or Public IM Tools**

Depending on the type of technology your employer uses, it is possible for the IT department to track e-mail messages that are sent via personal e-mail accounts like Gmail, Hotmail, or AOL. Scanning technology also enables employers to search the company system for the presence of unauthorized IM downloads from the web (Yahoo! Messenger and AOL AIM, for example). E-mail messages and IM chat transmitted via personal e-mail accounts and free web-based IM tools travel outside the organization's firewall and across the public Internet, where they can be intercepted by data thieves, business competitors, foreign governments, and other malicious third-parties. Consequently, the use of private e-mail accounts and IM tools may trigger a security breach—and the loss of your job.

**Tip #11: The Easiest Way to Control Electronic Risks Is to Control Your Written Content**

In other words, watch your language. Monitoring and filtering technology typically works hand-in-hand with written policy to seek out e-mail transmissions and links to web sites that violate the company's language and content rules. That means no obscene, pornographic, sexual, harassing, discriminatory, defamatory, menacing, or threatening language. Don't transmit gossip, rumors, jokes, disparaging, or defamatory remarks. Don't violate confidentiality rules or expose trade secrets. If you are surfing the web, steer clear of any sites—pornography, gambling, auctions, sports, news, games—that your employer has ruled off-limits.

**Tip #12: Employment-at-Will Means You Can Be Fired for Any Reason—including Writing and Surfing, Talking and Texting**

Are you a U.S. employee working in an employment-at-will state? If so, watch it! Private employers operating in employment-at-will states (which most are) may fire employees for just about any reason, as long as it is not discriminatory or in retaliation for whistle-blowing or union organizing.

Laws prevent employers from terminating employees on the basis of race, ethnicity, sex, age, religion, disability, and sexual orientation in some places. But when it comes to online communication, even keeping your personal blog or social networking page clean of work-related material won't necessarily protect you from termination. As Attorney Daniel M. Klein of Atlanta-based Buckley & Klein told *The New York Times*: "It doesn't matter if you blog about skydiving or pornography. If your employer feels the blog makes you a poor representative of their corporate values, the executives have the freedom to disassociate themselves from you."

**Tip #13: Don't Use Your E-Mail Inbox as an Ad Hoc Filing System**

If—in spite of these warnings—you still insist on using your employer's e-mail system for personal reasons, be sure to empty your inbox of all non-business-related mail at the end of each day. Either forward personal mail to your home account or simply delete it from your mailbox. While it's true that e-mail never disappears completely, there's no point making it any easier than necessary for your company's chief information officer or an external computer forensic investigator to locate and read your private, non-business-related electronic correspondence in the event of an employment review, civil lawsuit, criminal investigation, regulatory audit, or Freedom of Information Act request.

**Tip #14: Beware: Prospective Employers Screen Job Applicants' Blogs, Social Networking Profiles, and Video Posts**

With 70 million Facebook members alone, it's no surprise that interviewers are now scrutinizing job candidates' social networking profiles and video site postings—for an unfiltered look at the real person behind the resume. In the course of job interviews, one Missouri school superintendent, for example, asks potential teachers if they have a Facebook or MySpace page. If the candidate says yes, then the superintendent suggests taking an immediate look at the would-be teacher's profile, according to the Missouri State Teachers Association, as reported by the *Washington Post*. This example should serve as a wake-up call to all current job candidates—and any employee who may one day want (or need) to make a job change.

Do you really want to give a prospective employer one more reason to reject you? If you're in the job market, consider deactivating your personal blog, discontinuing your social networking page, or editing your posts to focus solely on content that is certain to appeal to prospective employers by highlighting your expertise, experience, or eagerness to fulfill your career goal.

© 2008, Nancy Flynn, Executive Director, The ePolicy Institute, [www.ePolicyInstitute.com](http://www.ePolicyInstitute.com). **Tips** excerpted from **THE e-POLICY HANDBOOK, Second Edition** by Nancy Flynn (AMACOM, December 2008). For informational purposes only. No reliance should be placed on this without the advice of legal counsel. Individual electronic business communication rules and policies should be developed with assistance from competent legal counsel.