

KEEPING UP WITH YOUR TECHNOLOGY
By Christopher P. Gabriel
Campbell Durrant Beatty Palombo & Miller, P.C.

(As prepared for and published in the
Pennsylvania County News
for the County Commissioners Association of Pennsylvania)

E-mail and the Internet are an essential part of the American workplace. These technologies are relatively inexpensive, easy to use, provide an efficient means of facilitating communication between workers and increase access to information. However, abuse of such technology can result in significant loss of productivity and/or potential liability for employers. Furthermore, when faced with litigation, an employer who is not prepared to preserve electronically stored information will face significant consequences.

E-mail and Internet Use: Workplace Management v. Employee Privacy

E-mail has increased business efficiency by enabling information to be disseminated with a keystroke instead of distributing multiple copies of written memos and holding lengthy meetings. However, the same keystroke can pass on not only work-related information but totally inappropriate materials. Many users consider e-mail less formal and potentially more personal, and therefore, senders devote less attention to what is written. However, that e-mail can be forwarded to and read by countless people without the sender's knowledge once he hits the "send" button. Many employees operate under the false perception that e-mail messages may be "deleted," when in fact, the message is stored on the network system. As such, e-mail has exposed employers to problems ranging from sexual harassment liability to the disclosure of confidential personal, financial or medical information.

Employers have many legitimate reasons to monitor their employees' computer usage, including: maintaining professionalism, preventing a decrease in workplace efficiency caused by excessive personal use of E-mails or the Internet, preventing workplace harassment, and preventing the disclosure of confidential information. These business reasons are convincing; however, the goal is to address these concerns without violating an individual's right of privacy.

Potential Sources of Privacy Issues Related to E-mail and Internet Monitoring

Employer monitoring of electronic communications must be consistent with federal and state law. Public employees enjoy a degree of privacy, granted to them by way of the Fourth and Fourteenth Amendment; however, the degree of privacy that each particular workplace receives is determined on a case by case basis. Similarly, the Electronic Communications Privacy Act of 1986 or the "ECPA", (18 U.S.C. § 2510 *et. seq.*) and the Pennsylvania Wiretapping and Electronic Surveillance Control Act (18 Pa.C.S. § 5701, *et. seq.*) provides potential protection for employees against employer monitoring of electronic communications. Employers, however, should avoid any transgressions by having clear policies that address appropriate business use, monitoring, and consent. As explained below, public employers have the ability to define and

even eliminate reasonable expectations of privacy. Because this area of the law is constantly developing employers should seek legal advice if unsure about monitoring, or what use to make of the information obtained.

How to Protect Yourself

An updated e-mail and Internet policy is essential for all employers. Employees must be informed that the work computer/e-mail system is the property of the employer and that the employee has no privacy rights as to the contents of the employer's computer system, including E-mails and all Internet usage. Employees should be required to review the policy and acknowledge in writing these core principles.

Employers can control the privacy expectations of their employees through an explicit and updated electronic communications policy. There are many comprehensive and model policies in circulation that may be utilized if you do not have an updated policy in place. Your policy should address privacy and other issues, including the following points:

- All aspects/apparatus of the computer network, including usage such as E-mail and access to the Internet, are the property of the employer and should be used for business purposes.
- E-mail, voicemail and Internet usage will be monitored in order to assure that they are being used for proper purposes only.
- Employees do not have a privacy right in any matter created, received or sent on the employer's computer, e-mail and voicemail systems.
- E-mail communications that include intimidating, hostile or offensive material based on sex, race, religion, national origin, age or disability are strictly prohibited.
- Discrimination, harassment and other conduct-related policies and prohibitions of the employer are extended to apply to all forms of electronic communication.
- Any employee who is found to have misused the electronic communications devices of the employer and/or violated any policies shall be subject to discipline, up to, and including, discharge.
- Employees should be educated as to the irreversible nature of Internet, e-mail and voicemail use and the fact that these uses are traceable and retrievable even if someone attempts to "delete."
- Employees should be notified of the obligation to preserve evidence, including electronically stored information, upon notification of a claim and/or notice that a claim is reasonably likely to be filed.

The goal for employers is to advance its legitimate business interest by enacting rules regarding electronic workplace usage so as to avoid creating unnecessary expectations of privacy and protect against liability resulting from an employee's abuse of its computer system. Any policy is worthless unless the employer consistently enforces the policy. A policy not enforced will never prevent abuse and is likely to result in liability. Every employer should be proactive

in addressing the issues raised by electronic communications systems and establish or update policies governing the operation of e-mail, voicemail, and the Internet.

Plan now for “E-Discovery”

Nothing highlights the importance of managing your technology more than the prospect of litigation and the discovery of electronically stored information. Once you are on notice of a claim or reasonably expect that a claim will be filed, you must take steps to ensure that evidence is preserved. The primary measure is a “litigation hold” that is implemented to stop any procedures or actions that would result in the destruction or loss of evidence. For electronic evidence, the litigation hold must include the suspension of otherwise routine and systematic procedures like the deletion of emails or files that often occur in accordance with a system-wide schedule. It also should include specific instructions to those supervisors and employees who have the ability to delete or destroy (intentionally or unintentionally) electronic evidence.

In practice, compliance with the obligation to preserve electronic evidence requires collaborative effort that should include the director(s) responsible for human resources or personnel, the director or contractor responsible for your Information Technology, the department head or supervisor(s) most involved with the case, and your legal counsel. The critical first step is to thoroughly review and identify each location for electronically stored information. You need to identify the people, apparatus and types of electronic information in play. To meet those obligations, you must have good electronic management systems and practices in the first place. If so, you will be in a position to identify where electronic information is stored. Do the people involved utilize PDA’s, lap tops or zip drives? Do employees simply save files to a hard drive or in other places of which you are not aware? If you are not in a position to identify these and other sources of electronically stored information now, it will be too late when you are served with a lawsuit. In this regard, you should know that the penalties can be severe¹ and costly² for failing to preserve electronic evidence.

Preparing for the inevitable (e-discovery) will not only enable you to comply with applicable law, but also should serve as a forceful reminder that every electronic communication is evidence that will be found and produced! When these steps are taken in conjunction with updating policies (if necessary) and training, this process should reinforce the reality that supervisors and employees should communicate with the clear understanding that their words will be read by litigants, attorneys, judges and perhaps a jury. Viewed in this context, those involved in personnel matters are more likely to act in conformance with your expectations and policies. The only and best way to avoid the pitfalls of e-discovery is to act now to ensure that you are managing your technology.

¹ In Mosaid Technologies Inc. v. Samsung Electronic Co., 348 F.Supp.2d 348 (D. N.J. 2004), the plaintiff moved for sanctions after the defendant destroyed significant evidence by failing to place a litigation hold on company e-mail even though litigation was foreseeable. The court instructed the jury that it could conclude that the destroyed evidence would have been harmful to the defendant. Monetary sanctions were imposed, which included the plaintiff’s attorneys’ fees and costs related to the motion for sanctions and attempts to obtain the discovery.

² In United States v. Phillip Morris USA, Inc., 327 F.Supp.2d 21 (D. D.C. 2004), the defendants’ noncompliance with a court order addressing evidence preservation and with the company’s document retention policies, resulted in the loss of e-mail records, warranted evidentiary sanctions at trial, as well as a monetary sanction of \$2,995,000.