Michael A. Caldwell, L.L.C.
Email: ***Michaelcaldwell@dcbflegal.com***

Writer's Direct Dial: 404-979-3154
Writer's Direct Fax: 404-835-0652

EMPLOYER COMPUTER-PRIVACY POLICIES

Many management clients express concern that their abilities to monitor employees' use of their company information technology are limited by laws regarding employee "privacy rights." They fear that if they take action against an employee whom they learn has been abusing the Company's Internet access and using email programs for personal or even anti-management purposes, they may subject themselves to liability for invasion of employee "privacy rights."

First of all, the right to privacy is a right that is not explicitly stated in the U.S. Constitution. Rather, the Supreme Court has theorized that the protection of individual's privacy from intrusion by the government is one of the "penumbral rights" attendant to the Fourth Amendment's guarantee of protections from a government's "unreasonable search and seizure."

Individuals have no constitutionally protected right of privacy protecting them from intrusions by other private individuals. To obtain such protections against non-governmental parties' trespasses upon their private lives, individuals must look to the rights of privacy developed under statutory and common law.

The common law right to privacy, which state courts enforce and some state legislatures explicitly have enacted into their statutes, generally recognizes and protects individuals' rights against unwanted intrusions into areas of their lives and activities wherein they maintain "legitimate expectations of privacy." Legal theories have developed defining as personal injuries or torts "invasion of privacy" and "public disclosures of private facts." Such torts have a common element: Where an individual has not chosen to disclose facts that generally are not available to the public through normal passive observation, or where an individual otherwise has not invited the public's attention to or interest in such private matters (such as, for example, by a teen-aged girl's Facebook publishing of a picture of herself clad in a skimpy bikini and setting her privacy controls to allow not only her designated Facebook *"friends*" but also, the *"friends of friends"*) the individual has a "reasonable expectation" that unwanted observers will not intrude into, try to learn about, or disclose to others such facts or matters.

The question lately has risen in the workplace environment of whether and to what extent employers can monitor and govern their employees' use of company information technology resources (company computers, internet access, email systems, etc.) made available to employees for company business purposes. There are competing concerns at work here. On one hand, the

employer owns the computers, pays for the Internet access, and purchases and maintains the email software, and it pays employees for the time they are on the job accessing their computers. On the other hand, employees do not generally expect their employer to act as Big Brother looking over their shoulders, spying on every private message or otherwise exercising thought-control over them. Add to the latter concern, the employees rights guaranteed under Section 7 of the National Labor Relations Act to engage in union organizing efforts, discussions of wages, hours and other working conditions or even to advocate "protected concerted activity" without fear of employer interference or coercion by spying on such activities. Thus the question of employer monitoring of employees computer use has even more serious legal implications.

The key to balancing the competing concerns is to create a policy that reasonably sets forth and defines the boundaries of employees' "reasonable expectations of privacy" when they are using the employer's electronic communication technology resources. The employer who provides the technology to the employees reserves to itself and maintains the right to define or even limit employees' privacy expectations—and hence the employees' privacy "rights" so long as it does so on a clear and rational basis that does not discriminate on the basis of the subject matter of the information communicated or accessed by the employee.

For these reasons, employers are well advised to adopt the following rules:

TO: ALL EMPLOYEES, SUPERVISORS, AND MANAGERS

SUBJECT: EMPLOYEE PRIVACY EXPECTATIONS IN THE USE OF COMPANY INFORMATION TECHNOLOGY

Privacy. The [***director of information services or other management official with technological ability to do this***] can override any individual password and thus has access to all e-mail messages in order to ensure compliance with company policy. This means that employees do not have an expectation of privacy in their company e-mail or any other information stored or accessed on company computers.

E-mail review. All e-mail is subject to review by management. Your use of the e-mail system grants consent to the review of any of the messages to or from you in the system whether in printed form or in any other medium. If you don't want management to see the communication, don't use a company computer, company Internet access, or the company's email system to communicate it.

Solicitation. In line with our general policy, e-mail must not be used to solicit for outside business ventures, personal parties, social meetings, charities, membership in any private organization, political causes, religious causes, or other matters not connected to the company's business. This rule is not intended to restrict employees' rights of self-organization or other lawful communications to the extent that they are protected under Section 7 of the National Labor Relations Act, as amended.