



2ND QUARTER *Brief*

100 South Mason Street · Harrisonburg, VA 22801 · Main (540) 434-0316 · Staunton (540) 885-0199 · Fax (540) 434-5502

Electronic Privacy Issue at Work

Frequently, your employees need their computers—including access to the Internet and e-mail accounts—to do their jobs properly. But you may be concerned that their level of personal use has exceeded reasonable bounds. Employees may be “tweeting” or checking their fantasy sports teams when they should be working.

Even worse, it is possible that some employees are exposing proprietary information about your company online. So you want to keep a closer watch on proceedings through electronic means. But are your methods legal?

It is relatively safe to say that the legislation in this area has not kept up with technology. The primary applicable federal statute, the Electronic Communications Privacy Act (ECPA), was enacted back

in 1986 (although it has been modified since then). The law has also been coordinated with the USA PATRIOT Act.

The ECPA was initially intended to govern third-party interceptions of electronic communications. It imposes civil and criminal penalties on anyone who intentionally intercepts, uses or discloses wire, oral or electronic communications. For this purpose, an “electronic communication” is defined as “any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photo optical system that affects interstate or foreign commerce.” Thus, this legislation appears to have a wide application.

On the other hand, state law may provide greater
see Electronic page 2

Backing Out of the Deal

Suppose you were eager to “sign on the dotted line” following a persuasive sales pitch by an aggressive salesperson. But now that you have had a couple of days to mull over the arrangement, you realize it is a mistake. Are you out of luck?

Not necessarily. You still may be able to void the contract if you act quickly enough. Depending on the applicable federal and state law in this area, you may be able to benefit from a legal concept called a right of rescission. In effect, this is the right to call off the deal during a stated period of time.

As a prime example, the Truth in Lending Act of 1968 provides a three-day “cooling-off period” for most consumer credit transactions (other than home purchases) that are secured by your home. For instance, you have three business days to change your mind about taking out a home equity loan.

Within 20 days after the lender receives the notice of rescission, it must return all funds paid as part of the transaction. The lender also must release any interest in the home that was used as security for this purpose.

In addition, many states have laws protecting consumers from impulsive decisions, including the following:

Insurance products: This includes not only life and health insurance sales, but also annuities and income continuation policies. The rescission period varies from state to state, but you can expect a minimum of ten days.

Health and fitness clubs: Some states even allow you to void a membership agreement after the cooling-off period has expired (e.g., if your physician says you can no longer use the facilities).

Real estate developments: Most states require real estate developers to prepare an offering plan or prospectus. The same laws that require a buyer to receive full disclosure from the developer also enable the buyer to cancel within a certain period of time. This period varies under state law, but is generally at least ten days.

Despite these “safety nets,” you are better off doing
see Backing Out page 2

Wharton Aldhizer & Weaver PLC

Electronic from page 1

for employees. Some states recognize a right of privacy that includes the right to be free from physical or electronic intrusions into a person’s private affairs.

However, state law can vary widely in this area. As a result, employers should be cautious and conservative when monitoring employee e-mail. Before an employer begins to conduct surveillance of employees, it should ask these questions:

*Is the surveillance necessary in pursuit of a valid business purpose? If an employee is reasonably suspected of theft or other wrongdoing, the surveillance may be justified. Conversely, indiscriminate surveillance without a business purpose is more difficult to justify and may be illegal.

*Is the type and extent of surveillance the minimum needed to achieve the business purpose? Assuming the surveillance is necessary, it may be considered an invasion of privacy if it is excessive or unnecessarily intrusive.

*Have employees been warned of the possibility of surveillance? If no warnings are provided, a court may determine that the employee had a reasonable expectation of privacy that was invaded by the employer.

The laws relating to electronic communications are still evolving. Consult with a legal adviser regarding your particular circumstances.

Backing Out from page 1

things right in the first place. For example, if you are buying a home, make sure that the contract permits you to rescind the deal if an inspection shows undisclosed damage or if favorable financing does not come through.

Brief's

***Truck Stop**—In a new case, a disabled truck driver quit his job and filed a discrimination lawsuit. He claimed that he was paid less than other drivers even though he had more seniority. But the company manual clearly indicated that salary was not based on length of service. Instead, the company focused on profitability, performance and other factors. Result: The Seventh Circuit Court dismissed the claim.

***Investment Scams**—Bernard Madoff and others have been accused of swindling investors in so-called Ponzi schemes. Now a new IRS ruling says you can deduct such a loss as a theft loss rather than a capital loss. The loss is deductible in the year it is discovered without applying the usual limits. Normally, casualty and theft losses must be reduced by \$100 per event (\$500 in 2009) and 10% of your AGI.

***Asleep on the Job**—Company supervisors suspected that an employee was sleeping in his cubicle. So they set up a surveillance camera that caught the employee in the act. When he was fired, he sued the employer, alleging invasion of privacy. Reason: He never expected to be filmed at the job. But a District Court in Texas ruled that he did not have a reasonable expectation of privacy in an open cubicle.

***One for the Ages**—Be careful what you say about older workers and how you say it. New case: An Ohio manufacturer fired a 55-year-old as part of a reduction in force. But a plant manager had remarked during union negotiations that older workers were driving up health care costs. The ex-employee was allowed to reference the manager’s statement to convince a jury that his firing was motivated by age discrimination.

Questions?

For more information about articles and information contained in the WAW Brief, contact Wharton Aldhizer & Weaver at (540) 434-0316 or send e-mail to info@wawlaw.com.

WAW has been serving our clients' legal needs for nearly 160 years in the areas of business, taxation, employment, health care, litigation, estate planning and administration, and land use.



Keeping Your Eyes on the Road

Can you talk on your cell phone or text while you are driving? Currently, drivers are prohibited from using hand-held cell phones in five states (California, Connecticut, New Jersey, New York and Washington) and the District of Columbia while ten states (Alaska, Arkansas, California, Connecticut, Louisiana, Minnesota, New Jersey, Utah, Virginia and Washington) and the District of Columbia have enacted a ban against texting for drivers.

Even if state law does not prohibit such actions, you may be held liable for a traffic accident caused while you were using your cell phone, not to mention the risks of personal injury to yourself and others. The best approach: Just don't do it.