



## “You’ve Got Mail” – and Other Electronic Data

By *Geoff Boodell*

### Revisiting The Need For Employers To Implement and Enforce Electronic Communication Policies

For many of us, it is hard to remember a time when our waking hours did not consist of surfing the Internet, sifting through an endless sea of emails, hearing the all-to-familiar hum of cell phones and PDA's, and being able to remotely access our office desktops via laptops and other electronic devices. The landscape in which we conduct business is continually changing. Many organizations today transact the majority of their business via some form of electronic medium. One study several years ago found that over 130 million workers are flooding recipients with 2.8 billion email messages each day! Since the study was conducted, that number may have doubled.

Email is one of the most widely used forms of office technology. The widespread use of email, however, raises many legal and practical concerns for employers, including the extent to which email is private, the potential impact of email in harassment and other claims by employees, and the impact it has in litigation generally. A recent decision from the Court of Appeals for the Ninth Circuit provides a timely reminder to employers to implement and enforce electronic communication policies. The Ninth Circuit decision, *U.S. v. Ziegler*, highlights the importance of implementing, disseminating and enforcing policies relating to employees' use of company-owned electronic devices.

**U.S. v. Ziegler.** Ziegler was employed as the Director of Operations for a private company in Bozeman, Montana that services Internet merchants by processing on-line electronic payments. His troubles began when the FBI had received a complaint from the company's Internet provider that someone (Ziegler) had accessed child-pornographic websites from a workplace computer. The FBI pursued the report and contacted the company's Internet Technology ("IT") Administrator whose duty was to monitor employee use of the workplace computers including their Internet access.

The company had in place a firewall that permitted constant monitoring of the employees' Internet activities. The company's employees were also apprised of the company's monitoring efforts through training and an employment manual, and they were told that the computers were company-owned and not to be used for activities of a personal nature. In light of the allegations, the company cooperated with the FBI and company employees entered Ziegler's locked office and copied the hard drive of Ziegler's work computer. Based upon the evidence found, the government charged Ziegler with crimes for downloading obscene materials and child pornography on his work computer from the Internet. Ziegler pled guilty to receipt of obscene material in exchange for the government dismissing the child pornography counts after the federal court denied his motion to suppress evidence obtained from a search of his workplace computer. Ziegler's plea agreement was conditioned on his ability to appeal the denial of his motion to suppress evidence obtained from his work computer to the Ninth Circuit Court of Appeals.

On Appeal, Ziegler sought to suppress the evidence as being an unreasonable search and seizure by a governmental agent. While the legal issues focused on the search powers of a governmental agent, the Ninth Circuit held that *the employer* had the authority to consent to the search because the computer was "workplace property" and the contents of Ziegler's hard drive were work related items that contained business information and which were provided to, or created by, the employee in the context of a business relationship. Ziegler's downloading of personal items (pornography) did not destroy the employer's common authority over the computer given the company's policies that informed employees that electronic devices were company-owned and subject to monitoring.

*U.S. v. Ziegler* highlights the importance of having in place an electronic communications policy and the importance of enforcing it once in place. Had Zeigler believed that his employer was serious about enforcing its policy, he may have thought twice about using his work computer for illegal activity.

**Elements of an Effective Policy.** An electronic communications policy should, at minimum, advise employees that:

- All electronic devices (computers, phones, PDA's, laptops, etc.) are company property and not private; that the device should be used for business purposes only; that all messages, sent or received, are subject to review; and that the email system and all messages distributed on it are the property of the employer, not the employee.
- Company email or other electronic devices or medium is not to be used for the creation or distribution of any offensive or disruptive messages, including messages containing offensive sexual comments, or offensive comments regarding race, gender, age, sexual orientation, political beliefs, disability or national origin.
- Violation of the policy subjects the employee to discipline, up to and including discharge.

Of course, to be effective the policy must be enforced. Recent court decisions make it clear that complaints regarding unsolicited, unwelcome emails with sexual or otherwise offensive overtones are no different than any other type of harassment complaint, and should be taken just as seriously.

\*This Employment Law Note is written to inform our clients and friends of developments in labor and employment relations law. It is not intended nor should it be used as a substitute for specific legal advice or opinions since legal counsel may be given only in response to inquiries regarding particular factual situations. For more information on this subject, please call Sebris Busto James at (425) 454-4233.

© 2007 SEBRIS BUSTO JAMES

---

---