



# Journal of Local Government Law

---

Published by the Local Government Section of the Virginia State Bar

---

Vol. XXI No. 4, Spring 2011

## The Myth of “My Computer, My Email”

Phyllis Katz  
Ruth Griggs

The technological revolution that has occurred in recent years has enabled us to communicate with people at points around the world in micro-seconds. The communication may be written, data bits, images, sounds, and symbols and may be shared through various mediums. Although the clouds may be filled with these pieces of information, we certainly expect our communications to be private.

But is this belief founded? “Privacy in today’s workplace is largely illusory. In this era of open space cubicles, shared desk space, networked computers and teleworkers, it is hard to realistically hold onto a belief in private space . . . . Work is carried out on equipment belonging to employers who have a legal right to the work product of the employees using it.” Ellen Bayer, the American Management Association, as reported on [www.keylogger.org/articles/american\\_management\\_association](http://www.keylogger.org/articles/american_management_association).

As recently reported, “Nearly half of employers . . . track content, keystrokes and time spent at the keyboard. They’re seeking increased productivity but also are watching workers to make sure they’re not spilling trade secrets, sending boss-

slamming e-mails to bloggers who cover their particular industry, sexually harassing co-workers or posting discriminatory remarks on personal blogs.” *USA Today* on March 17, 2011. “In the context of the ‘community norm’ within 21<sup>st</sup> Century computer-dependent businesses . . . the use of computers in the employment context carries with it social norms that effectively diminish the employee’s reasonable expectation of privacy with regard to his use of his employer’s computer.” See *U.S. v Ziegler*, 456 F.3d 1139, 1145 (9<sup>th</sup> Cir. 2006). Yet, “for most people, their computers are their most private spaces” *U.S. v Gourde*, 440 F.3d 1065, 1077 (9<sup>th</sup> Cir. 2006), (observing that an expectation of privacy in employer-provided computers may be misguided). Complicating this issue is that many employees use personal computers that are connected to the employer’s internal network. This interconnectivity makes employer monitoring of the personal, non-work communications of employees possible with the right software equipment.

The monitoring of the computer activities of employees is pervasive and fraught with many legal issues. In the public sector, the monitoring takes on even more risks. This article will provide an introduction to some of the legal issues involved with such monitoring.

### Gaining Access to Communicated Messages

Stemming from the principles of property law, the widespread belief among employers is that any condition on the use of employer-provided equipment

can be imposed, including the right to inspect messages stored on such computer. See e.g. *Muick v Glenayre Electronics*, 280 F. 3<sup>rd</sup> 741, 743 (7<sup>th</sup> Cir. 2002), (upholding under common law a private employer’s search of the messages stored on the employer-provided laptop). Although the common law may recognize such ownership rights, separating the ownership of the communications equipment and systems from the messages transmitted and/or stored on such equipment is pivotal to any present day analysis of the respective employer/employee rights. Since 1986 with the enactment of the Electronic Communications Privacy Act of 1986 (Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U.S.C. §§ 2510-2511 (“ECPA”) and the Stored Communications Act (SCA), 18 U.S.C §§ 2701-2712, the courts have been dealing with the scope of the privacy afforded electronically communications.

### Fourth Amendment

The “Fourth Amendment prohibits ‘unreasonable searches and seizures’ by governmental agents, including governmental employers or supervisors.” *U.S. v Simons*, 206 F.3d 392, 398 (4<sup>th</sup> Cir. 1999) (upholding the FBIS’ search of Simons computer). The FBIS’ Internet policy stated that the employer would “audit, inspect, and/or monitor employees’ use of the Internet, including all file transfers, all websites visited, and all e-mail messages, ‘as it deemed appropriate.’ The court found that the policy placed employees on notice that they could not reasonably expect that their internet activity would be private.” *Id.* In reach-

*Phyllis Katz is a principal at the firm of Sands Anderson and specializes in local government and employment law. Her e-mail is [pkatz@sandsanderson.com](mailto:pkatz@sandsanderson.com). Ruth Griggs is an associate at Sands Anderson and may be reached at [rgriggs@sandsanderson.com](mailto:rgriggs@sandsanderson.com).*