REPORT FROM COUNSEL

AUGUST 2011

DELETING COMPANY E-MAIL AND SOCIAL MEDIA IN THE WORKPLACE

DELETING COMPANY E-MAIL

When a telecommunications company went defunct, almost literally on his way out the door, the former president and CEO of the company allegedly deleted certain e-mails from the company's computers. When the company was placed in receivership, the receiver sued the former executive for a variety of his actions taken in connection with the collapse of the company. Among these claims was an assertion that when he deleted the e-mails, allegedly to cover up some misconduct, the executive violated the federal Computer Fraud and Abuse Act (CFAA).

One of the executive's arguments was that the CFAA only makes it illegal to damage computers, and that the mere deletion of e-mails could not reasonably be regarded as inflicting such damage. The federal district court hearing the case disagreed. To require something like physical harm to a computer, or even some lesser injurious action of the kind, for there to be damage would be to ignore the expansive language that Congress used in drafting the CFAA.

"Damage" is defined in the law as "any impairment to the integrity or availability of data, a program, a system, or information." Given that definition, the court concluded that even the commonplace act of deletion of data from the company computers impaired the availability of computerized data, thereby constituting damage within the meaning of the CFAA.

The executive was unable to have the case against him dismissed on this basis, but it remained for a jury to decide if he had, in fact, both deleted the e-mails and done so without authorization. On those points, an examination of the defendant's e-mail box on the server was enough to allow a jury to find that he had deleted the e-mails in question.

The e-mail box had been reduced in size by about 98%. Moreover, even the previously authorized use of a computer system may become unauthorized when an employee breaches his duty of loyalty to his employer. The executive no doubt at some point had broad authority to deal with his company e-mails as he wished, but the pending litigation against him was replete with claims that he had been disloyal to the company in a number of different ways. If the receiver could prove such disloyalty, whatever authority the defendant had once had over the company computers was gone as quickly as he had left the premises following the deletions.

SOCIAL MEDIA IN THE WORKPLACE

The prevalence of social media, including postings that are meant for employment-related topics in particular, has led to an increase in litigation on the subject between employees and their employers. The scenarios leading the parties to the courtroom are as varied as one might imagine. A company fires a worker over her criticisms of the boss that she posted on Facebook. Repeated attempts by a manager to "friend" a female employee on Facebook eventually leads to allegations of sexual harassment. A disappointed job applicant sues when a job offer is retracted after a hiring manager turns up something about the applicant on Twitter that the manager finds disturbing.

In addition to scenarios in which a worker loses his or her job because of something appearing in social media, litigation may ensue against an employer if its supervisory officials go too far in digging for dirt by this means. For example, two restaurant workers won a monetary settlement after having sued their former employer for gaining access to postings on a password-protected Myspace page set up as a chat group for employees only. What was found on the page eventually led to the workers' termination. The case was settled after a jury found that the employer had violated the federal Stored Communications Act (SCA).

The employees' managers had violated the SCA by knowingly accessing the chat group on Myspace without authorization. Although a fellow employee had provided her log-in information to one of the company's managers, she had not authorized access to the chat group by any of the company's managers. She also felt that she had been coerced into giving her password to her manager, as she felt that she would have been in trouble if she had not done so.

Using the employee's password, the company's managers accessed the chat group on several

occasions, although it was clear on the website that the chat group was intended to be private and accessible only to invited members. Finally, the mangers continued to access the chat group even after realizing that the employee had reservations about having provided her log-in information.

Since e-mail first came on the scene, similar cases have arisen over what was or was not appropriate when employees used their company-provided computers for sending e-mails. One preventative measure for employers has been to create a clear written policy on the subject, followed up by informing and training the employees. Likewise, an employer's best protection against potential liability stemming from social media may be to establish a policy that clearly spells out the ground rules for the use of social media.