CVK
COSGRAVE VERGEER KESTER LLP
ATTORNEYS

LABOR & EMPLOYMENT NEWSLETTER – JANUARY 2007

EMAIL TRAFFIC – DRIVE CAREFULLY!

A former employee sued his employer alleging, among other things, disability and Title VII discrimination, and whistleblower retaliation. When asked at deposition what had become of 2,200 documents and emails missing from his company laptop, he answered that he had deleted the files. Not only that, but he had effectively thwarted the company's attempts to retrieve the data by writing a program to "wipe" the deleted files from the hard drive.

Shari L. Lane

The court was not pleased. The case was dismissed, and the former employee was fined $65,000, the amount the employer had spent defending the case thus far. The Ninth Circuit confirmed the dismissal and the fine. *Leon v. IDX Systems Corp.*, 464 F.3d 951 (9th Cir. 2006).

In lawyer-speak, destroying electronic information that is or may be relevant to a pending lawsuit is referred to as "spoliation of evidence." Sanctions have always been available for spoliation of evidence, although the extreme sanctions imposed in Leon are rare.

The case is significant not only because the court slapped the hand of a litigant who intentionally impeded the course of the lawsuit, but also because it highlights the changing face of business operations, and the resultant necessary changes in our legal system.

For instance, there was a time when a discussion between an employee and her supervisor took place orally, in the supervisor's office. If the employee later filed suit, the key evidence would be the parties' recollection of that conversation, bolstered perhaps by any notes the supervisor jotted down during the conversation. The parties' attempt to gather evidence during litigation would then be limited to requesting copies of the notes, and eliciting testimony about the conversation as the parties remembered it. Fast-forward to 2007, and the conversation is almost certain to take place at least in part via email. Throw in the fact that most companies have a program that automatically purges email from the system periodically, along with the fact that some people mistakenly believe they can permanently eliminate potentially incriminating electronic documents simply by deleting the documents, and suddenly the potential for spoliation of evidence—intentional or inadvertent—is enormous.

This problem was recognized—though certainly not eliminated—in the amendments to the Federal Rules of Civil Procedure (fondly known as the FRCP), which went into effect December 1, 2006. The FRCP mandate that early in litigation, the parties must meet to discuss the kinds of evidence each side will produce, and one of the amendments specifically mandates a discussion of "any issues relating to disclosure or discovery of electronically stored information, including the form or forms in which it should be produced." FRCP 26(f).

The Judicial Committee on Rules of Practice and Procedure recommending these changes noted that such discussion is crucial because "[t]he volume and dynamic nature of electronically stored information may complicate preservation obligations. The ordinary operations of computers involves . . . the automatic deletion or overwriting of certain information." The Committee also noted it is important to "pay particular attention to the balance between the competing needs to preserve relevant evidence and to continue routine operations critical to ongoing activities [because] [c]omplete cessation of a party's routine computer operations could paralyze the party's activities." Report of the Judicial Conference at p. 31-32 (September 2005).

The amendments to the FRCP recognize this tension, and include this savings provision: "Absent exceptional circumstances, a court may not impose sanctions under these rules on a party for failing to provide electronically stored information lost as a result of routine, good-faith operation of an electronic information system." FRCP 37(f). [1.]

While the amendments provide some protection to companies utilizing reasonable data storage and destruction policies, there has been a simultaneous move to more consistently penalize deliberate destruction of electronic data, as seen in the *Leon* case. The Third Circuit took this one step further recently in *In re Grand Jury Investigation*, 445 F.3d 266 (3rd Cir. 2006), where the court held that merely discussing the need for preservation of electronic documents with clients eliminated the attorney-client privilege, when the client later destroyed electronic documents in spite of the attorney's advice to the contrary. The court remarked, "In this era, when communications between leaders of business organizations are transmitted to their employees by email rather than by phone or mail, examination of those emails is the method most commonly used by government investigators . . . . It should therefore come as no surprise that efforts to forestall such investigations frequently take the form of deletion of past emails." (The court cited as an example the infamous Arthur Andersen case).

These rules and cases address the issues related to preservation of electronic evidence for litigation purposes. Of course, the issues for today's businesses are not limited to problems arising in litigation. Employee use and misuse of electronic media ranks high on the list of concerns facing today's employers.

The Computer Fraud and Abuse Act addresses some of these broader issues. The Act provides penalties for anyone who "exceeds authorized access," defined as "access[ing] a computer with authorization and . . . us[ing] such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter." The Act provides some recourse to employers when employees steal client contact or other information that may not be protected by other laws, or when employees share, alter, or

destroy company documents without authorization

All of this highlights the need to have ongoing discussions with employees, especially supervisory and human resources personnel, about electronic communication and documentation. Every company (regardless of size) should have a written policy, routinely reviewed and updated, regarding:

1) **The use of company computers for personal purposes.** This policy may include prohibitions on viewing pornographic sites, making internet purchases, doing online banking, drafting and printing personal documents on company computers, and/or using company email for personal communications. There is no "correct" policy in this regard. Every company is made up of human beings who have personal lives that intersect with their workday, and there is no evidence a strict policy prohibiting all personal use is a guarantee against misuse. The key is establishing a clear policy and communicating that policy to all employees.

2) **The use of computer-generated information that may be proprietary.** The policy should indicate what information the company considers "proprietary." If you don't want your salespeople obtaining a client's phone number to invite the client to a (non-work sponsored) game of golf, the policy should say so.

3) **Supervisory communication.** Silence really is golden, in some cases. Supervisors should be advised to say as little as possible in email, when the communication relates to discipline or other supervisory functions. The casual nature of email lends itself to statements that may seem merely tactless at the time, but may later be used against the company as proof of bias or intent. On the other hand, as noted below, supervisors should be advised to create a hard copy or a permanent electronic copy of all supervisory emails, in case such communications become relevant to litigation. As indicated above, intentional deletion may give rise to a claim of spoliation of evidence, and may even destroy attorney-client privilege.

4) **Document retention and storage.** All employees should be advised of the company schedule for automatic deletion of emails and other data, and should be simultaneously advised of the importance of saving important email and other data apart from the format in which it is slated for automatic destruction.

5) **Sharing electronic documents.** All employees should also be trained to save documents in a format that will not allow recipients outside the company to alter the document, or view the document history. This goes beyond the scope of this article, but businesses that routinely relay documents in draft form to individuals outside the company are advised to become savvy about hidden data and metadata.

Summary

As the cases, laws, and rules of civil procedure demonstrate, there are both benefits and dangers inherent in the way we do business in this electronic information age. At the risk of abusing the metaphor, the lesson to be learned is this: businesses must drive the superhighway of electronic communications and data with care, to avoid a collision in the workplace or in court.

---

1. *This rule would not have helped the plaintiff in Leon, of course, because the data was not "lost as a result of routine, good faith operation of an electronic information system." In addition, the court in Leon did not impose sanctions under the FRCP, but rather under its "inherent" power to impose sanctions for what amounts to bad behavior in litigation.*

CVK
COSGRAVE VERGEER KESTER LLP
ATTORNEYS