If Your Company Monitors Employee Email You Still Need to Have Privacy Protocols in Place

March 13, 2017 - Most large corporations, and many smaller firms monitor employee email accounts. And most of the companies that monitor email have written policies in place that their employees have to sign off on. In other words, employees are notified by their employer that their corporate emails belong to the company and that the employees have no reasonable expectation of privacy when they use their corporate account. But that doesn't mean that companies don't have to provide some level of privacy to their employees on email. There is some new case law that companies need to be aware of if they want to stay out of court.

A ruling in the case Brown Jordan Intl, Inc v. Carmicle should have corporate America examining its email privacy policies. The case is really about a former employee - Carmicle - who thought of himself as a whistleblower. In an attempt to dig up dirt on his employer, that employee went snooping through the email accounts of other employees. In that process, he thought he had developed evidence of financial improprieties by his employer.

An investigation of the alleged financial misdeeds found that the company had done nothing wrong but during the investigation Carmicle admitted that he had secretly accessed employee email accounts using a password that granted universal email access. Carmicle was terminated for his actions and the company hired outside computer consultants to assess what, if any damage was done and to ensure that he same type of issues wouldn't arise in the future. Then the company sued Carmicle.

In his arguments to have the suit thrown out, Carmicle said that accessing the email accounts of other employees was permissible under the Stored Communications Act since the company had notified employees of their email policies. Those policies allowed for corporate monitoring of company issued email accounts. But both the lower court and the Eleventh Circuit Court of Appeals disagreed. The appellate court said that it was unreasonable to think that provisions of the law allowing corporate email monitoring would include the use of a universal password by an unauthorized employee.

While the court also reviewed other areas of the law and found for the plaintiffs in each case, the ruling on access to email is what caught our attention because it likely cuts both ways. Employees who gain unauthorized access to email using methods such as a universal password could easily find their employers suing them to recover damages. But we suspect that companies could also be sued by employees for failure to protect their individual email accounts from unauthorized access.

Companies need to have clearly articulated policies with regard to email usage and access. Only employees with an absolute need to know should have access to email accounts other than their own. All employees should be trained on email use and access policies and the consequences for disregarding those policies should be harsh and swift.
byJim Malmberg
Note: When posting a comment, please sign-in first if you want a response. If you are not registered, click here. Registration is easy and free.
Follow me on Twitter:

Follow ACCESS