December 5, 2013

Attorney-Client Emails: Not Always Privileged

Lawyers and their clients may have a nasty surprise in store if a party in litigation seeks to compel production of the emails between them, if the client uses an employer's corporate email account that is subject to monitoring by the employer. Depending on the circumstances, a court may hold that the attorney-client privilege does not protect these communications. And, if such communications are not protected, have they waived the privilege for all of their communications? Fortunately, there is an easy solution for those who are diligent.

In the case of *In re Information Management Services, Inc.*[1], the Delaware Chancery Court held that the numerous emails sent by two company executives to and from the corporate email account of their employer to their attorney were not privileged because the employer maintained an express policy of monitoring such communications, thus destroying the required reasonable expectation of privacy.

In this case, the plaintiff was a shareholder who brought a derivative action against the two executives. Thus, the corporation was named as a plaintiff, being the real party in interest. The discovery request for the emails thus came from the corporation, although the plaintiff-shareholder and his lawyers did not have access to the emails other than through discovery. The court applied a traditional 4-part test to determine if the executives had a reasonable expectation of privacy at the time the emails were sent. In summary, the factors are: (1) whether the employer either advises employees of a policy restricting personal use of the company's email account, or informs them that they do not have a privacy right in such emails, or advised employees that it reserves the right to monitor emails; (2) the extent to which the company enforces its policies and informs employees of the policy; (3) whether any third parties may access the company's emails; and (4) whether the company had duly notified employees of the use and monitoring policies.

The Delaware Chancery Court considered these four factors, and noted that no single factor is dispositive or required, and concluded that the executives did not have a reasonable expectation of privacy due to the company's policy that it monitored emails, that it so notified employees, and that the executives knew it. The executives' and their lawyers' practice of placing a legend on the emails "Privileged Attorney Client Communication" did not cure the loss of the privilege.

The particular circumstances in the Information Management Services case are atypical because when the company seeks the emails, it already has access to them, even though counsel for the shareholder does not. However, it is not difficult to imagine a number of scenarios when third parties seek emails of employees to their counsel that are transmitted on the company account. It can readily be argued that the loss of any expectation of privacy applies regardless of who is making the request. The Delaware court noted that a different result might obtain when the requestor is a third party, but did not answer that question. Indeed, the 4-factor test could well produce different and inconsistent rulings.

The issue of losing a valuable privilege is important to both the requesting party and the requested party. Perhaps a lawsuit is a purely private one not involving the employer, but the employee has used the employer's account to communicate with counsel. In such case also, there is a risk that the privilege has been lost.

---

[1] 2013 WL 5426157 (Del. Sept. 5, 2013)

The best safeguard is the use of the employee's private email account. The Delaware court, without deciding, stated that the outcome may well be different when a private account is used from the workplace, because the expectation of privacy is probably greater. Even then, however, if the employer has a policy prohibiting the use of private accounts from the workplace, an adverse party has an argument that the privilege is lost, especially if the employer's policy gives it the right to monitor workplace use of private accounts. However, the use of a private cell phone or pad to transmit an email via a private account would seem likely to be insulated from a claimed loss of privilege.

The most fail-safe means to communicate with counsel is to use a private account outside of the workplace, not on company time, and outside the scope of a company's monitoring policy. If counsel for the employee wants to be sure of the outcome, this should be advised from the outset.

Often, a former employee will bring suit against the employer, but has used company email to communicate with counsel prior to termination. There is unlikely to be any expectation of privacy as to those emails that could shield them from the company, or possibly from third parties. Company counsel should therefore ensure that there is a policy in place that the company may monitor all emails, either from the company site or a private site, transmitted to and from the workplace, if the company may seek to obtain the private-site emails in litigation against the employee.

Thomas Earl Patton
202 454 2840
pattont@butzel.com