



## Avoiding Liability



By Jeffrey P. Lewis

*Jeffrey P. Lewis is a member in the Philadelphia office of the Pittsburgh-based law firm of Eckert Seamans Cherin & Mellott L.L.C. He serves on the PBA Professional Liability Committee.*

# Duty to Warn Client to Protect Confidentiality of Electronic Communications with Counsel

In this day and age counsel and client routinely communicate with each other electronically, whether by email or text messaging, using computers, smartphones and tablet devices. This author has written previously concerning instances where the attorney-client privilege is compromised because clients have not taken reasonable steps to protect their privileged communications from access by third parties. An example would be instances where clients and their lawyers communicate with each other using the email account of the client's employer. The case law is evolving in this area so that it is not clear in each instance whether the client has employed sufficient protection, such as by using a password-protected personal account on the employer's computer, to avoid a waiver of privilege. But it is not just the issue of whether the employer can gain access to such communication and use it, for example, against the employee in an employment dispute. If sufficient protection has not been employed, such communications would also be subject to access by a third party by subpoena. Moreover, this issue is not limited to instances involving an employer's computer; waiver can be found where the client has used someone else's computer to communicate with counsel, whether in a library or hotel, on a borrowed computer or even on a computer at home where other members of the family have access. In many instances the potential for, and consequences of, waiver are not appreciated by the client.

The issue of waiver in this context was addressed in *Parnes v. Parnes*, 915 N.Y.S.2d 345 (Sup. Ct. App. Div. 1011), a case I reported on earlier, wherein the wife in a domestic dispute had found her husband's password to his personal email account on a piece of paper on his desk and used it to gain access to emails between him and his counsel. In that instance, although the court found that husband had been careless to leave his password lying about in a house he shared with his estranged wife, husband still had a reasonable expectation of privacy and therefore had not waived the privilege.

All of the foregoing raise the question: What duty does a lawyer have to advise a client not to engage in conduct that could result in waiver of the attorney-client privilege for failure to secure electronic communication of substantive discussions? The ABA Standing Committee on Ethics and Professional Responsibility recently issued Formal Opinion 11-459, "Duty to Protect the Confidentiality of Email Communications with One's Client." The opinion is based on the ABA Model Rules of Professional Conduct, which are not substantially different from Pennsylvania's Rules of Professional Conduct. Notwithstanding that the preamble of both sets of the rules and case law support the proposition that a violation of these rules does not provide a basis for civil liability, the ABA committee opinion is a suggestion of where case law may lead with respect to such a duty to warn.

In the ABA committee's view, "[a] lawyer sending or receiving substantive communications with a client via email or other electronic means ordinarily must warn the client about the risk of sending or receiving electronic communications using a computer or other device, or email account, where there is a significant risk that a third party may gain access. In the context of representing an employee, this obligation arises, at the very least, when the lawyer knows or reasonably should know that the client is likely to send or receive substantive client-lawyer communications via email or other electronic means, using a business device or system under circumstances where there is a significant risk that the communications will be read by the employer or another third party."



The opinion cites several considerations when determining the existence of "a significant risk" of access by a third party. These include: 1) whether client had either used or

indicated an intention to use electronic communication with counsel; 2) whether client has access to a workplace device or system; 3) whether the client's employer or a third party has the means to access the client's electronic communications; and 4) that "as far as the lawyer knows, the employer's internal policy and the jurisdiction's laws do not clearly protect the privacy of the employee's personal email communications via a business device or system." According to the opinion, a lawyer need not assume that an employer has an internal policy to grant it access to the employee's emails sent or received on a workplace device or system "(u)nless a lawyer has reason to believe otherwise. ..."

Based upon the foregoing criteria, once the lawyer believes there is a risk of compromise of the attorney-client privilege by third-party access to electronic communication, the opinion indicates that the lawyer should take protective measures. These would include cautioning the client not to communicate with counsel under circumstances where an employer or other third party may have access, such as "a business email account or using a personal email account on a workplace computer or device at least for substantive emails with counsel." Protective measures would also include the lawyer refraining from sending electronic communications "to the client's workplace, as distinct from personal, email address."

From the standpoint of potential professional liability, this opinion demonstrates that counsel must exercise vigilance to inform clients of their need to exercise care in the electronic means used to communicate. Moreover, counsel should exercise the same vigilance in communicating with clients.