SAN FRANCISCO
Daily Journal
www.dailyjournal.com
WEDNESDAY, SEPTEMBER 14, 2011

Be tech smart: Protecting your client communications

By Alison P. Buchanan

Imagine this scenario: Your client is suing her current employer. During discovery, you travel out of town to depose a witness at opposing counsel's office. You arrive an hour early and go to a nearby café. You use your laptop and the café's WiFi to access your firm's network, conduct legal research, prepare a short memo, and review pertinent documents in preparation for the deposition. At opposing counsel's office you obtain their WiFi password so that you can access confidential documents during the deposition. You obtain helpful testimony and catch the witness making a false statement, which you will expose later using the confidential documents. As you are putting your laptop away, your client emails you about the status of the case, advising she can't talk on the phone because she is at work. You reply via Blackberry. You let your client know about the witness's false testimony and tell your client how you think it will impact the upcoming mediation. You briefly discuss strategy recommendations and potential settlement figures. Unfortunately, you leave your Blackberry in opposing counsel's conference room, but opposing counsel kindly overnights it to you.

Associated Press

Stephanie Axelrod works on her laptop at a Starbucks Corp. store in Seattle.

When using a wireless connection to access your firm's network, only use a network that you know is secure; otherwise, hackers may intercept your confidential communications and data.

This sounds like a typical day for many lawyers, except that you may have unknowingly violated your duties of confidentiality and competence in several ways, potentially disadvantaging your client and exposing you to a malpractice and breach of fiduciary duty claim. For transactional lawyers who think the above scenario doesn't apply, imagine negotiating a deal where the other side obtains access to your confidential client communications.

How could you have violated such important duties to your client by using technology to your advantage and communicating promptly with your client? Both the State Bar's Committee on Professional Responsibility and Conduct (COPRAC) and the American Bar Association have recently addressed the issue.

COPRAC Formal Opinion 2010-179 addresses a situation where an attorney accessed confidential client data from a firm-issued laptop using public WiFi at a café. COPRAC found that in that situation, an attorney risks violating "the duties of confidentiality and competence he or she owes to a client by using technology to transmit or store confidential client information when the technology may be susceptible to unauthorized access by third parties."

COPRAC sets forth six factors for an attorney to consider before using a specific technology, including an evaluation of the attorney's ability to assess the security afforded by a specific technology, the legal ramifications to third-parties intercepting or accessing the electronic information, the degree of sensitivity of the information, the potential impact to the client if inadvertent disclosure occurs, the urgency of the situation, and client instructions and circumstances.

More recently, the ABA's Aug. 4 opinion (ABA Op. 11-459, *"Duty to Protect the Confidentiality of E-mail Communications with One's Client"*) provides that "[a] lawyer sending or receiving substantive communications with a client via e-mail 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 e-mail account, to which

Alison P. Buchanan *is a shareholder based in Hoge Fenton Jones & Appel's San Jose office, where she focuses her practice on business litigation, legal ethics, and professional malpractice defense. She is a frequent lecturer on legal ethics and teaches professional responsibility at San Jose's Lincoln Law School. She was recently appointed to COPRAC, effective Sept. 18.*

a third party may gain access.... Whenever a lawyer communicates with a client by e-mail, the lawyer must first consider whether, given the client's situation, there is a significant risk that third parties will have access to the communications. If so, the lawyer must take reasonable care to protect the confidentiality of the communications by giving appropriately tailored advice..."

Using technology can make you a more effective advocate. But with these recent opinions in mind, how can you use technology without jeopardizing confidential communications and data? Following are a few tips:

First, be conscious of the technology you use. When using a wireless connection to access your firm's network, only use a network that you know is secure; otherwise, hackers may intercept your confidential communications and data. Airport and café networks tend to be unsecured. Hotel networks are often secured, but not always. Your home wireless connection is safe if it is secured (security levels are usually set up at the time of installation). Unsure whether the wireless network at opposing counsel's office or at your mediator's office is secure? Ask. In the opening hypothetical, you used the café's and opposing counsel's wireless networks to access confidential communications and data without questioning the security of either network. The better practice is to find out first whether the wireless network you plan to use is secure. If not, don't use that network to access confidential data or communications.

Second, be aware of the technology your client uses. In the opening hypothetical, the client emails you from her company email address regarding her pending lawsuit against that same company. As one state court recently held, a client whose company policy states that work computers are for work only and subject to inspection by the company has no expectation of privacy and those communications are not privileged. See *Holmes v. Petrovich Development Co.* (2011) 191 Cal.App.4th 1047, 1069-1070. Given the significant risk involved, you should have advised your client to only use a private email address from a non-company computer when communicating with you about the litigation.

Third, protect your devices. Is your smartphone password-protected (with a strong password)? If not, and you leave it unattended, anyone can access confidential communications on the device. Is your laptop password-protected and encrypted? If not, a thief can access your confidential communications and data. In the opening hypothetical, you inadvertently left your phone in opposing counsel's conference room. If this was not password-protected, an unscrupulous opposing counsel could access your confidential email communications.

Worry not. The sky is not falling. You don't have to revert to hard copy documents and non-electronic means of communicating with clients. You can easily implement the above-referenced safeguards. Utilize technology to your advantage. But be safe, be smart, and communicate with your clients about significant risks.