Web Only

The Business Magazine
For The Chief Legal Officer

CORPORATE counsel

corpcounsel.com • November 12, 2009

Calling Up Dangers to Privilege

Edward Cheng and Chris Blazejewski

When attorney-client privilege law first developed, carbon paper was considered cutting-edge technology. Today, technological advances allow lawyers to communicate with their clients in ways that would make Buck Rogers envious.

All that new technology, however, poses some difficult questions about the attorney-client privilege. With everyone e-mailing, texting and talking on mobile devices, in-house counsel may hope that these communications are confidential and privileged in case of litigation. But are they? The answer from the courts to date: It depends.

For the attorney-client privilege to exist, four elements must be present. There must be (1) a communication (2) made between privileged persons, such as an attorney and client, (3) in confidence (4) for the purpose of seeking, obtaining, or providing legal advice or assistance. The privilege, however, can be waived when there is no reasonable expectation that the communication will remain confidential. A waiver of privilege grants litigation opponents access to information they otherwise would not be entitled to during the course of discovery.

Today's fast-changing technology increases the risk of potential waiver. Using mobile phones and PDAs, lawyers and clients can share information instantaneously from virtually anywhere in the world. Memos, letters, charts can be transmitted or stored. Conversations can take place by phone, through e-mail or with instant messaging. As the uses of these devices continues to expand, the courts find themselves looking to rulings on older technologies as they consider the application of the attorney-client privilege law to today's rapidly evolving methods of communication.

Edward S. Cheng

Chris Blazejewski

The good news is that state and federal courts have already held that there is a reasonable expectation of privacy for communication using landline telephones and faxes, which are not easily intercepted inadvertently. Congress and several states have also codified the privacy of e-mails, now widely recognized by the courts. The Electronic Communications Privacy Act of 1986 ("ECPA") criminalized the interception of e-mail transmissions and provides that interception does not result in the loss of the attorney-client privilege. States including New York and California have statutes expressly providing that the interception of e-mail does not vitiate privilege.

Further, cases from federal and state courts around the country—such as *Stafford Trading, Inc. v. Lovely* (2007), *In re Lernout & Hauspie Sec. Litig.* (2004), and *Bovis Lend Lease, LMB, Inc. v. Seasons Contracting Corp.* (2002)—reinforce the protection of privacy and privilege for e-mail. Rulings in these cases have held that e-mailed communication between counsel and client remains privileged.

When it comes to other kinds of technology, however, the expectation of privacy is still developing. The rules governing mobile or cellular telephones are a case in point. Before the introduction of cellular phones, courts held that attorney-client communications over mobile radio phones were not privileged. As a Louisiana federal district court in *Edwards v. Bardwell* wrote, "there is no reasonable expectation of privacy in a communication which is

broadcast by radio in all directions to be overheard by countless people who have purchased and daily use receiving devices." Similarly, the federal appeals court in *U.S. v. Mathis* held that conversations over cordless phones were not deemed to be confidential, so a lawyer would be tempting fate by talking to his client over a cordless phone.

When mobile radio phones gave way to early cell phones, courts such as the Eighth Circuit in 1989's *Tyler v. Berodt* and the Fifth Circuit in 1992's *U.S. v. Smith* continued to maintain that parties had no expectation of privacy and thus confidentiality. These rulings were based on the fact that early cell phones used analog frequencies to transmit calls, making them more easily susceptible to interception through police scanners or other phones using the same frequencies.

More recently, courts such as the Fifth Circuit in 2007's *U.S. v. Finley* and the Ninth Circuit in 1997's *Dunlap v. County of Inyo* recognized increased expectations of privacy and confidentiality for communications and information stored and transmitted on cell phones. In light of the fact that cell phones today broadcast with encrypted digital signals, a court would likely rule that an attorney has a reasonable expectation of privacy in discussions over a digital cell phone. But even that ruling would not protect a lawyer talking loudly over his or her cell phone in a taxi or airport lounge. Clearly transmission is only part of the issue. Also of concern is whether the conversation is being conducted in a way that can be overheard.

Communication technology, however, is evolving rapidly and people are adopting it faster than the courts can decide these issues. That makes it critical for in-house counsel to exercise common sense and due diligence when using an emerging technology to communicate. For example, it appears obvious that communication with clients over social networking services such as Twitter or Facebook will not be privileged because third-party "friends" can see the communications. The same holds true for Internet blogs, where the content of the communication is posted publicly and can be viewed by others. What may be less obvious is that although some of the communications through these public services may appear confidential, they may actually be accessible to others simply through a few strokes of the keyboard.

The next attorney-client privilege frontier: mobile data devices like the Blackberry and the iPhone, which combine telephone and e-mail services with Web browsers, contact databases, and calendars. Many lawyers already entrust volumes of attorney-client communication and work product to these devices. The good news is that in 2009's *S.E.I.U. v. Roselli*, a California federal district court explicitly permitted a party to withhold information stored on a Blackberry or PDA on the basis of privilege.

Mobile data devices, however, are not all the same in terms of data encryption and protection. Concerns about the security features of the initial models of the iPhone, for example, led some companies to insist that their employees use the industry-standard Blackberry to ensure confidentiality and protect attorney-client communications. Aware of those concerns, Apple, Inc., announced several security enhancements for its popular iPhone this summer at the 26th Worldwide Developers Conference. These enhancements reflected Apple's renewed efforts to market the iPhone to businesses by addressing security concerns. While such technical information might at first glance seem to be a matter for the information technology department, savvy in-house counsel should also take notice so that they can properly balance function and versatility when choosing communications devices for their department's contacts with clients.

Today, attorneys and clients can deliver messages instantaneously around the world using cutting edge technologies, some more secure than others. As they adopt these technologies, lawyers and clients alike must exercise vigilance and common sense to protect the confidentiality and privilege of their communications. That means in-house counsel may want to forego the advantages of being an early adapter to make sure that they have first done their homework.

Edward S. Cheng *is a partner specializing in business litigation at Boston-based Sherin and Lodgen LLP.* ***Christopher R. Blazejewski*** *is an associate in the firm's Litigation Department.*