The Lawyers' Lawyer Newsletter

Recent Developments in Risk Management

December 2011 | Volume 16 | Issue 4

Social Media—Communicating With Represented Parties—Impermissible Use of Subterfuge

San Diego Bar Opinion 2011-2 (May 24, 2011)

Risk Management Issue: What are the limits of permissible social networking conduct by lawyers?

The Opinion: This ethics opinion addressed a hypothetical situation involving an attorney representing a former employee against a company-employer in a wrongful discharge action. The lawyer sent "friend" requests to two high-ranking employees with the client's former company whom the client had identified as being dissatisfied with the employer and thus likely to make disparaging comments about it on their social media pages. The attorney intended to use information gleaned from the social media sites to advance his client's interests in the litigation; the "friend" requests gave only the attorney's name.

The San Diego Bar County Legal Ethics Committee (Committee) stated in the opinion that the lawyer's requests violated both California's no-contact rule and the attorney's duty not to deceive others. A lawyer seeking to obtain access to a represented party on social media sites must either: (1) fully disclose his or her affiliation and the purpose of the "friend" request to a nonpublic account of a represented party, after obtaining consent to that communication by the represented party's attorney; or (2) seek such discovery through formal discovery channels.

Communication with represented parties is regulated by Cal. R. Prof'l Conduct 2-100. The equivalent ABA Model Rule provision is 4.2.

When analyzing whether the attorney's friend request was a communication "about the subject of the representation," the Committee explored the context in which the statement was made, and the lawyer's motive in making it. If the communication to the represented party is motivated by a search for information about the subject of the representation, then the communication with the represented party is "about the subject matter of the representation."

While a "friend" request normally makes no reference to anything other than the sender's name, it is nevertheless objectionable. The subject of the representation need not be directly referenced in the query to be "about" the subject matter of the representation.

The Committee expressly rejected the suggestion that "friending" a represented party is no different from accessing an opposing party's public website. The very reason the friend request is made is to get beyond the restricted access placed on the social media page by the user. The no-contact rule, on the other hand, is designed to avoid disrupting the trust essential to the attorney-client relationship.

The Committee distinguished *U.S. v. Carona*, 630 F.3d 917, 2011 WL 32581 (9th Cir. 2011), where the U.S. Court of Appeals for the Ninth Circuit held that a prosecutor did not violate Cal. R. Prof'l Conduct 2-100 by providing fake subpoena attachments to a cooperating witness to elicit pre-indictment, noncustodial incriminating statements during a conversation with the criminal defendant. The Ninth Circuit held that there was no direct communication between the prosecutor and defendant, and that the use of the fake subpoena attachments did not make the informant the prosecutor's alter ego. The Ninth Circuit further reasoned that even if Rule 2-100 was violated, the district court did not abuse its discretion in not suppressing the statements on the ground that state bar discipline was available to address any misconduct. In *Carona*, the

Social Media—Communicating With Represented Parties, continued on page 2

Hinshaw & Culbertson LLP
222 North LaSalle Street
Suite 300, Chicago, IL 60601
312-704-3000
www.hinshawlaw.com
www.lawyeringlaw.com

Co-Editors: Anthony E. Davis and Victoria L. Orze

Contributors: Wendy Wen Yun Chang, Katie M. Lachter and David A. Sorensen

Ninth Circuit focused on the lack of direct contact between the prosecutor and defendant, whereas the friend request at issue in the Committee's opinion was a direct *ex parte* friend request to a represented party.

Importantly, and following other ethics opinions—including Bar Association of the City of New York Formal Opinion 2010-02 and Philadelphia Bar Association Opinion 2009-02—the Committee concluded that the attorney also violated his ethical duty not to deceive by making the friend request without disclosing why the request was being made. This conclusion is based on extensive case law in California holding that the duty of an attorney not to deceive extends to intentional deception of opposing counsel and the general common law duty not to deceive is a duty that extends to misrepresentation to those other than judges.

The Committee also concluded that if there is a duty not to deceive opposing counsel, who is far better equipped by training than lay witnesses to protect himself or herself against the deception of his or her adversary, then the duty surely precludes an attorney from deceiving a lay witness.

Risk Management Solution: Law firms need to develop clear social networking policies to guide lawyers on what conduct is—and is not—permissible and appropriate, and to provide effective training to help secure compliance.

Attorney-Client Privilege—Duty to Preserve Client Confidences—Electronic Storage of Client Information

New York State Bar Ethics Opinion 842 (Sept. 10, 2010), and *District of Columbia Bar Legal Ethics Committee Opinion No. 357*

Risk Management Issue: What measures do law firms need to take to manage the risks associated with storage of client files and sensitive client information in the "cloud?"

The Opinions: In recent years, lawyers have turned to emerging digital storage solutions such as "cloud" computing to store client files. These tools pose new and different risks than those used for traditional storage of physical files. They likewise raise complicated issues associated with electronic security, maintaining and protecting client confidences and work product privileges, as well as ownership and return of the client's file upon termination of the representation. In its broadest sense, the cloud consists of all the electronic storage resources available using the internet rather than servers owned and wholly controlled by the owner of the information to be stored. The cloud is composed of domains and servers accessible through a network of internet service providers, and includes any service provided online and operated by a third party, such as online data storage, internet-based email and software as a service.

The New York State Bar Association Committee on Professional Ethics (NYSBA Committee) issued Ethics Opinion 842 to explain the ethical questions that attorneys who hire third-party providers to store electronic client files in the cloud need to address. District of Columbia Bar Legal Ethics Committee (DCB Committee) Opinion No. 357 deals with lawyers' obligations regarding former clients' records maintained in electronic form when the client relationship is terminated. Taken together, these two opinions provide guidance to lawyers who seek to uphold their ethical duties to clients while modernizing their practice environment.

The NYSBA Committee concluded that online storage systems are permissible so long as an attorney exercises reasonable care to ensure that confidential information will remain secure. The NYSBA Committee compared the practice with the common practice in the past and present of hiring a third party to store physical copies of client files. Under N.Y. R. Prof'l Conduct 1.6(a) "a lawyer shall not knowingly reveal confidential information" and under N.Y. R. Prof'l Conduct 1.6(c) an attorney must exercise "reasonable care" to ensure that third parties who provide services for the attorney do not divulge or use confidential information. With modern technology however, what constitutes "reasonable care" in the context of third-party storage remains somewhat unclear. Accordingly, the NYSBA Committee suggested four practices that attorneys should consider as part of exercising "reasonable care":

(1) Ensure, and periodically reconfirm, that the storage provider has "an enforceable obligation to preserve confidentiality and security" and "will notify the lawyer if served with process requiring the production of client information."

(2) Investigate the storage provider's "security measures, policies, recoverability methods, and other procedures to determine if they are adequate under the circumstances."

(3) Utilize "available technology to guard against reasonably foreseeable attempts to infiltrate the data that is stored" and notify affected clients in the event of a breach.

(4) Review the provider's ability to purge, wipe and transfer the data if the attorney decides to use another provider.

Bar committees in at least four other jurisdictions (Alabama, Arizona, Nevada and New Jersey) have also reviewed ethical issues associated with cloud computing and have found the practice permissible. All appear to concur that attorney obligations have not fundamentally changed in the face of these new technologies, and lawyers are advised to maintain appropriate competence to understand and keep current with technological developments and their effect on security measures in order to protect confidential information.

The DCB Committee opinion discussed lawyers' continuing duty to protect client interests when the attorney-client relationship ends where all or part of client files are maintained electronically. Following its Opinion 357 that the entire file unequivocally belongs to the client, the DCB Committee also reaffirmed the rule that in terminating representation under D.C. Rule 1.16 a lawyer must take appropriate steps to protect client interests in surrendering papers and property to which they are entitled, regardless of the media in which they are stored.

On the related issues of when electronic files must be converted to paper, and who should bear such costs, the DCB Committee rejected a "bright-line" test. While a lawyer in most cases must comply with a reasonable request from a client to convert electronic files to paper, the client should in most cases bear the conversion cost. However, the attorney should bear the cost if neither the client nor substitute counsel can access the records "without undue cost or burden" and the former client's need for the file in paper form outweighs the burden to the lawyer to furnish the file in that manner.

Risk Management Solution: In fulfilling their duties of confidentiality and competence to their clients, attorneys must make reasonable efforts to ensure that technology they employ does not place confidential client information at undue risk of unauthorized disclosure. Technology is continually evolving and available products may differ significantly in security features offered. As well as ensuring and regularly monitoring the security of technology being used, lawyers should also address issues of file retention, maintenance and security in their engagement letters with clients when the representation begins. Where practical, attorneys should consider client input in making technology decisions such as the use of cloud service providers. In the exercise of due diligence and reasonable care, lawyers should be competent to evaluate their use of online technologies and be prepared to interview service providers, particularly with respect to security, backup and service continuity issues.

Duty of Candor—Client Communications

McCollough v. Johnson, Rodenburg & Lauinger, LLC, 637 F.3d 939 (9th Cir. 2011)

Risk Management Issue: What is required in order for lawyers to fulfill their obligation to verify representations provided by the client before relying on those representations?

The Case: Plaintiff debtor sued defendant debt collection law firm in the U.S. District Court for the District of Montana, claiming a violation of the federal Fair Debt Collection Practices Act (FDCPA) and the Montana Unfair Trade Practices and Consumer Protection Act (MCPA), and alleging state torts of malicious prosecution and abuse of process. The court granted summary judgment in part for the debtor and the jury rendered a verdict on behalf of him on the remaining counts. The U.S. Court of Appeals for the Ninth Circuit affirmed.

In 1999, the debtor fell behind on his bank credit card bill of $3,000. The bank "charged off" the debt in 2000 and sold it to a collection agency. The collection agency sued the debtor on the debt in 2005 and the debtor, acting *pro se*, responded that the statute of limitations had run. The collection agency dismissed the case two weeks later, but documented service of the complaint and the debtor's response in its electronic files.

Duty of Candor—Client Communications, continued on page 4

In 2006, the collection agency retained the law firm to pursue collection of the debtor's outstanding debt. The client's retainer agreement with the firm contained a disclaimer stating that: "[the collection agency] makes no warranty as to the accuracy or validity of data provided," and made the law firm "responsible to determine [its] legal and ethical ability to collect these accounts."

After the law firm's screening procedures flagged a statute of limitations problem with the debt, the law firm asked its client whether there was any writing that extended the limitations period. The client erroneously responded that the debtor had made a $75 partial payment in June 2004, (which would have extended the limitations period to 2009).

In April 2007, the law firm filed suit against the debtor to collect the debt. The debtor retained counsel and responded, again, that the statute of limitations had run. In August 2007, the collection agency informed the law firm by email that the debtor had not made any payments. The client's email was scanned into the debtor's file, but the attorney prosecuting the case did not review it until later. In December 2007, in response to a call from the law firm seeking documentation, the collection agency called the law firm and informed it again that there was no June 2004 payment and that the statute of limitations had indeed expired, and instructed the law firm to dismiss the suit.

The debtor then sued the law firm directly for malicious prosecution, abuse of process, and violations of the FDCPA. On cross-motions for summary judgment, the district court found that the law firm had filed a time-barred lawsuit against the debtor in April 2007, that by August 2007 the firm had information from the client demonstrating that the lawsuit was time-barred, and that the law firm nonetheless continued to prosecute the time-barred lawsuit until December 2007. A jury then awarded the debtor $1,000 in statutory damages, $250,000 for emotional distress, and $60,000 in punitive damages.

The attorney prosecuting the debtor testified that he made no independent inquiry into whether the debtor had actually made the June 2004 payment to extend the statute of limitations. Rather, he relied on the information provided by the collection agency. With respect to the August email from the client informing the law firm that the debtor had not in fact made any payments, the attorney said he did not review it in the file until later.

The court found that the law firm had erred by relying without verification on the client's representation about the June 2004 payment and by overlooking contrary information in its electronic file. Because of multiple pieces of contradictory evidence available to the firm, its reliance on the client's original, erroneous email was unreasonable as a matter of law. The court upheld the jury's finding that the law firm could not have reasonably believed that a June 2004 partial payment had been made in light of all the evidence in its file; it knowingly filed a baseless action and acted with malice by disregarding the true facts concerning the timeliness of the lawsuit. The law firm's problems were compounded by the fact that it had served the debtor with requests for admission, including one that asked him to admit that he had made the 2004 payment. The discovery failed to inform the debtor that his failure to timely respond would result in the requests being deemed "admitted."

Comment: In addition to liability to adversaries, a lawyer may be liable to his or her own client for malpractice for allowing that client to pursue frivolous litigation. In *Ashby & Geddes, P.A. v. Brandt*, --- F. Supp. 2d ---, 2011 WL 3290329 (D.Del. Aug. 1, 2011), a malpractice claim against a law firm survived a motion to dismiss on the theory that the law firm failed to review its client's claims and to advise the client on the viability of those claims. The law firm attempted to rely on the existence of co-counsel in another state, which was tasked with taking the lead on the client's matters, but the court was not persuaded, commenting that the law firm had an independent duty to advise the client of the viability of its claims and litigation strategy.

Risk Management Solution: These cases serve as a reminder that lawyers have an obligation to verify the accuracy of the information on which they rely. At the very least, they are required to review the information available to them and may not rely blindly on client representations that are contradicted by other evidence. Law firms should develop practice management policies and procedures that require attorneys to undertake independent investigation of statements made by clients before taking action based on those statements. It is also wise to incorporate into the firm's management practices a process whereby new matters are reviewed by someone other than the lawyer handling a case before undertaking the representation and commencing litigation. Such policies and procedures ultimately benefit clients, as well as protecting firms from attacks—whether to their pocketbook, or their reputation, or both.