TECHNOLOGY RELATED ETHICS ISSUES

William J. Cobb [1]
Assistant General Counsel, State Bar of Georgia
wjcobb@gabar.org

[1] Opinions and suggestions in this paper are informal, are not binding on the Office of the General Counsel, the State Disciplinary Board or the Supreme Court of Georgia, and do not necessarily represent official positions of the Office of the General Counsel.

TABLE OF CONTENTS

I. INTRODUCTION

It will surprise no one that the rapid and thorough integration of technology, the Internet and the practice of law has outpaced straightforward application of ethics rules written earlier without a crystal ball. Clarifications, interpretations and revisions have begun to appear in recent years – though not in Georgia – with different jurisdictions sometimes reaching different conclusions. In Georgia, only the advertising rules explicitly encompass the use of electronic media. Georgia Rules of Professional Conduct (GRPC) Rules 7.1(a)("A lawyer may advertise through all forms of public media . . .") and 7.2(a)(4)(". . . a lawyer may advertise services through: . . . electronic . . . communication."). The recent explosion of lawyer-focused web sites and use of social media by lawyers and clients raises some especially challenging issues.

We should not overstate the problem, however. Most provisions of the GRPC adapt quite easily to this new environment. For example, "communication" inherently includes communication by electronic means; "writing" is writing regardless of the medium; and most GRPC statements of obligation and prohibition are not media dependent. Even so, neither explicit GRPC text nor Formal Advisory Opinions (FAO) dictate answers to some of the ethics questions created or magnified by today's pervasive use of technology. In fact, there are no FAOs in Georgia on this subject.

This paper briefly addresses some of the most common ethics issues associated with the use of technology and the Internet in a law practice. Some are old news but still important, while others have emerged rapidly in recent years and remain without explicit interpretive guidance.

II. EMAIL, TEXTS, AND DIGITAL DOCUMENTS

A. Stop – and Think – Before You Click

Email is no longer new by any means, but it continues to present most of the same concerns it always has. Texting is not much different. Foremost among those concerns is a lawyer's duty to protect the confidentiality of client related information. GRPC 1.6(a).[2]

Despite or perhaps because of today's ubiquitous preference for professional communication by email (and to a lesser extent texting), the duty of confidentiality inherently requires that when communicating through these means, just as with any means, a lawyer must be cognizant of the risks, and if necessary take protective measures. Interpreting its Model Rule from which GRPC 1.6 is derived, ABA Formal Advisory Opinion 11 (August 4, 2011)[3] concluded:

> 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, *where there is a significant risk that a third party may gain access*. (italics added)

As demonstrated by the near universal use of email by commercial sites, including banks, for retrieving lost usernames and passwords, email is generally quite

[2] Most of the Georgia ethics rules referenced in this paper are appended in full, along with their official comments. However, **the rules should always be reviewed on the State Bar's web site to assure reference to the most up to date versions.** www.gabar.org>Bar Rules>Ethics & Professionalism>Georgia Rules of Professional Conduct.

[3] Because ABA Formal Advisory Opinions are copyrighted, they are not reproduced with these materials. However, they should be accessible via Google.

safe and secure. However, there are a number of sources of potential risk. In general and without pretending to be comprehensive, consider first that email and texts have fundamental characteristics not shared by oral or even paper communications. One is that, once created, their existence may well be permanent regardless of deletion efforts, because of such things as backup procedures, archiving and automated third party data collection. Those processes are often beyond the control or even awareness of the sender or recipient of the email or text. In addition, widespread duplication and dissemination is fast and easy. That, too, is not necessarily controllable.

The ABA opinion makes special note of the inherent increased risk of inadvertent disclosure and unintended access when the client is an employee using the employee's work computer, particularly if the representation relates to the employment. Other noted risks include increased opportunities for third party access when using a public computer (such as a library or hotel computer), a borrowed computer, or a device available to other family members. And unsecured public and retail Wi-Fi and Wi-Fi hotspots are an increasingly ubiquitous source of risk for unauthorized disclosure.

As a practical matter, the nature and extent of reasonably necessary protective measures vary with (i) the degree the risk, (ii) the sensitivity of the information being communicated, and (iii) the difficulty and expense of applying particular protective measures. *See* ABA Opinion 99-413 (1999), "Protecting the Confidentiality of Unencrypted E-Mail" (concluding that, as a general proposition subject to factors like those stated above, a lawyer may ethically use unencrypted e-mail, because it affords a reasonable expectation of privacy by virtue of technological and legal protections). Encryption, or limiting or specially configuring the physical devices through which

communications will occur, might nevertheless be appropriate in some circumstances. Similarly, where encryption is warranted, the type and extent that are reasonable will vary. Military grade encryption may be neither warranted nor practicable, for example, but a lawyer may decide that an off the shelf encryption product is simple and inexpensive enough that its use is desirable, either routinely or in certain cases.[4]

The now well-known NSA data collection and analysis programs have obvious potential relevance here, but the uncertainties they present do not mean lawyers must routinely communicate only using methods that ensure against NSA interception or worse (which may or may not even be possible as a practical matter). As is evident from the earlier discussion, Rule 1.6 does not require elimination of all risk of inadvertent or unauthorized disclosure. That was impossible even in the ink and paper world. Rather, the rule requires attention to the potential problem, and reasonable balancing of risks and protective measures appropriate to the parties, the subject matter and the circumstances of the representation. In certain cases, of course – perhaps defending clients accused of certain criminal or terrorist activity, for example – that balancing could call for extraordinary measures to protect client information from disclosure. In most cases, though, Rule 1.6 compliance will require less.

[4] The ABA has an on-line CLE on encryption, Product Code CET13EMSOLC, and a related book, *The ABA Cybersecurity Handbook: A Resource for Attorneys, Law Firms, and Business Professionals*, Product Code 3550023.

You can head off problems in the use of emails and texts by:

- Raising and discussing these issues with the client at the outset,
- Reaching an understanding about establishing protocols for email and text use, and
- Addressing the above in the representation agreement.

Though not traditionally applied in this context, one might argue that GRPC Rule 1.4(a)(2) at least counsels that conversation: "A lawyer shall . . . reasonably consult with the client about the means by which the client's objectives are to be accomplished."

B. Inadvertent Disclosure: Email and Texting

Email has made it much easier for a lawyer to inadvertently disclose protected information to inappropriate recipients. Two of the most common and most preventable sources of inadvertent disclosure are by now well known to all lawyers, Reply All and Auto-fill.

1. Reply All

No explanation of this hazard is really necessary. All of us have direct experience, whether in a work or personal environment, or both. "Reply All" is for many people the reflexive default for responding to email. For lawyers especially, that is a big mistake. It is a Rule 1.6 violation waiting all but inevitably to happen, and the danger extends beyond disclosure of confidential client information. In July 2014, for example, multiple media outlets reported that a Fulton County ADA in the Atlanta schools

cheating case mistakenly used Reply All to reply "surprise, surprise" to a notification that defendant Beverly Hall was too ill to attend trial or assist her lawyers, sending the comment to dozens of lawyers and others associated with the case. The ADA was suspended without pay for three days and removed from the case. F.C.D.R. (July 10, 2014).

Do whatever you reasonably can to *make "Reply" the rule* and *"Reply All" the exception that requires an affirmative decision.* You can always resend the response to other recipients. You cannot unsend it.

This problem is a prime candidate for a software solution. If your email program allows moving "Reply All" to a drop-down list that does not include "Reply," that would all but insure that "Reply All" is always a purposeful choice. Even just moving the "Reply All" button away from the "Reply" button would help a little. In MS Outlook, implementing such a fix is not straightforward. Attachment 1 to this paper presents possible ways to do it, but this author has not tested any of them and cannot vouch for their efficacy or speak to possible problems or side effects.

2. Auto-fill

Bet you've done this, too. You think you entered, say, the client's or opposing counsel's e-mail address, but you were moving too fast and did not notice that auto-fill actually inserted someone else's address because of their similarities. The resulting disclosure could be relatively benign in practical effect and voluntarily correctable depending on the recipient, but obviously it could also be disastrous. There are at least two solutions for this problem, each with its own downsides.

One is to *turn off or disable the auto-fill function*. That eliminates the problem by definition, but it is inconvenient, increases your expenditure of time, and increases the odds of typographical errors.

The other solution is "just" to remain at all times mindful, to pay attention, and to *look and verify before you click*. While the advantages of auto-fill are thereby retained, this solution does require constant mental discipline. As with any repetitive task, though, it can through sustained effort become more automatic.

C. Inadvertent Disclosure: Digital Documents

Metadata presents the greatest risk of unauthorized access/inadvertent disclosure apart from the transmission of the document.[5] Metadata is information embedded in electronically created documents, though hidden from view during routine use. The hidden information may be embedded automatically in the background, or it can be intentionally embedded for purposes of identification, organization, tracking changes, collaboration, etc. It often includes such things as text deleted from or added to earlier drafts, dates and sequence of edits, and identification of authors, editors and recipients. A determined recipient, or sometimes even just a curious one, can expose metadata and thereby learn things the sender assumed would not be learned and under GRPC Rule 1.6 perhaps should not be learned.

[5] The plethora of potential issues arising from e-discovery is beyond the scope of this paper. Note, however, that disclosures required by court order or by discovery rules are explicit exceptions to the GRPC non-disclosure obligations. Rule 1.6(a)(". . . , except for disclosures that . . . are required by these Rules or other law, or by order of the Court.")

Therefore, with the caveat discussed below, a lawyer should establish policies and practices designed to ensure that metadata not intended to be disclosed is not disclosed. At least one state has decided that removing metadata before distribution is obligatory under its Rule 1.6. W. Va. Ethics Op. 2009-01 (2009).

There are two basic approaches to this metadata problem. Some document creation/processing software includes settings or features through which creation of metadata during drafting and editing is minimized. It may well be, though, that a given program will always save some metadata regardless of those choices.

Alternatively, removing metadata after completion but before sending the document to its ultimate recipients is likely to be more comprehensive. MS Word, for example, has a function for inspecting metadata in the document and selectively removing it. In Word 2010, that function is located at File>Info>Check for Issues>Inspect document. There are many dedicated off-the-shelf programs, too, with varying capabilities.

One important caveat must be noted. In some circumstances the law may impose an affirmative obligation *not* to alter documents, and/or to retain at least copies in their original or "native" state. In such instances, removing metadata could constitute spoliation of evidence, which in turn could implicate GRPC Rule 8.4(a)(4)(Misconduct) ("engag[ing] in professional conduct involving dishonesty, fraud, deceit or misrepresentation"), or Rule 3.4(a)("A lawyer shall not unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value."). GRPC Rule 1.6(a) anticipates such

situations, by stating the exception to the confidentiality obligation noted above, i.e., where "required by these Rules or other law, or by order of the Court."

The overriding point, as it was with email, is to be aware of what is happening. Think before you click.

D. Inadvertent Disclosure: Potential Consequences

It should not be necessary to dwell on why avoiding inadvertent disclosure of confidential client information is important. This confidentiality is at the very core of the attorney-client relationship and the proper functioning of the justice system. Thus GRPC 1.6 presumptively mandates it, and the maximum punishment for violation is disbarment. As additional incentive for implementing protective measures like those suggested above, though, a brief pause may be useful to consider the ethical obligations of a lawyer who inadvertently receives confidential information, say from opposing counsel.

Simply stated, a lawyer who inadvertently receives confidential information that should not have been disclosed has *no obligation under the GRPC to refrain from reading it, to return it, or to refrain from using it*. Georgia does not even require notice of receipt to the disclosing lawyer, as the second paragraph of ABA Model Rule 4.4 does, though it ordinarily may be good form and consistent with professionalism aspirations to do so.

In fact, the ethical obligation to communicate with clients, GRPC Rule 1.4(a)(2), (3) & (4), and to consult with them concerning the means by which their objectives will be pursued, Rule 1.2(a), could require the receiving lawyer to inform her client and

share the information. Similarly, scenarios making it problematic for the receiving lawyer *not* to use the information to advance the client's case are not hard to imagine.

However, there is no *per se* obligation in the Georgia Rules of Professional Conduct to inform the client and/or use otherwise protected information inadvertently received. For example, if the receiving lawyer already knew the information, or if it could not affect the conduct or outcome of the case, it may be difficult to then conclude that the lawyer must share the information with the client.

In short, inadvertent disclosure of information protected under GRPC Rule 1.6 can have serious consequences for the disclosing and the receiving lawyers, and for their clients. It can directly affect the conduct and even the outcome of the case itself.

E. Email, Computer Literacy and Professional Competence

Not every lawyer has jumped on the email bandwagon. Some use it only reluctantly or sporadically. Some are self-confessed, even proud "computer illiterates," including a dwindling number who have never bothered to master e-mail and rely on staff for that. But the march of time – including such changes as mandatory e-filing and rules requiring attention to e-discovery – is making computer illiteracy and e-mail aversion increasingly problematic for lawyers.

At present, GRPC 1.1 (Competence) has not been interpreted to require computer literacy. Rule 1.1 begins by defining "competent representation" as requiring a "level of competence" or association with a lawyer who is "competent." The rule then adds this: "Competence requires the *legal* knowledge, skill, thoroughness and preparation

reasonably necessary for the representation." (italics added) The official comments seem to confirm that "skill" as used in the rule refers to traditional notions of legal skill.

Nevertheless, consider an extreme hypothetical. What if a lawyer had adopted essentially no modern technology? No fax, no internet, no email, no photocopier, no computer, just a landline phone and manual typewriters. Would a client be justified in questioning that lawyer's competence, as the term is commonly understood?

The ABA Model Rules now link competence and computer literacy, though not in those exact terms and not in the text of the rule itself. In 2012, an amendment to what is now Comment [8] to Model Rule 1.1 added the language shown here in italics: "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, *including the benefits and risks associated with relevant technology, . . .*"

Some courts are showing intolerance of technological illiteracy as well. For example, a trial court in Pennsylvania recently denied a lawyer the opportunity to arbitrate a fee dispute, because he did not attend to his email while responsible staff was ill and unable to do so, causing him to miss a scheduling notice. Attachment 2 (*Knox v. Patterson*).

F. These Problems Are Not Yours Alone

Lawyers not only have to abide by the Georgia Rules of Professional Conduct, they also must try to ensure that lawyers and staff working for them do, too. A lawyer's obligations with respect to conduct of staff are governed by GRPC Rule 5.3:

> (a) a partner, and a lawyer who individually or together with other lawyers possesses managerial authority in a law firm, shall make reasonable efforts to ensure that **the firm** has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
>
> (b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that **the person's** conduct is compatible with the professional obligations of the lawyer . . .

Rule 5.1 states essentially the same obligations to ensure ethical conduct by a firm's non-managerial lawyers, and by direct lawyer supervisees.

In addition, under parallel provisions in Rules 5.1(c) and 5.3(c), conduct by a subordinate lawyer or staff, respectively, can be attributed to and itself constitute an ethical violation by the managing or supervising lawyer himself. As stated in Rule 5.3(c), that liability attaches where:

> 1. the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> 2. the lawyer is a partner in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time

when its consequences can be avoided or mitigated but fails to take reasonable remedial action.[6]

Establishing and enforcing clear policies to address these issues is essential. All of these responsibilities apply equally to the matters discussed in Part III, below.

III. THE INTERNET, SOCIAL MEDIA & THE CLOUD

A. The Ethics Landscape of Cyberspace

My colleague Christina Petrig has compiled an excellent, concise and practical overview of the ethics issues most often encountered in this brave new world. Following that, a couple of problems will be discussed in somewhat more detail.

LAWYERS, SOCIAL MEDIA & COMMON SENSE

Christina Petrig
Assistant General Counsel
State Bar of Georgia

THE SAME RULES APPLY

All the Rules of Professional Conduct apply to things lawyers do as lawyers on social media and other Internet platforms. Pay particular attention to Rules 6.1 (confidentiality), 3.6 (trial publicity), and 7.1 through 7.5 (communications concerning a lawyer's services/lawyer advertising). Consider your social media and other postings as billboards. Think carefully about everything you post. Then think again before it's too late. Do not post impulsively.

[6] The Rule 5.1(c)(2) iteration for lawyer subordinates applies where "the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action."

NO FALSE OR MISLEADING STATEMENTS: RULE 7.1

Social media and similar postings are subject to the same rules as public communications in "old media." Your communications cannot be false, fraudulent, deceptive or misleading. Rule 7.1(a)(1)-(5) provides an illustrative list of communications that would violate this rule. All communications must contain your name. Note that disbarment is the maximum penalty for a violation of this rule.

CONFIDENTIALITY: RULE 1.6

Georgia's confidentiality rule is very broad: a lawyer shall maintain in confidence **all information gained in the professional relationship with a client.** All means all. The fact that pleadings are filed does not mean that you are free to discuss your client's legal matter in cyberspace. Do not blog, post, tweet, etc. about your clients or their cases unless you have informed consent from your client. Informed consent involves at the very least advising your client of what you propose to say about their matter, and how and when you propose to say it.

TRIAL PUBLICITY: RULE 3.6

Even if you have your client's informed consent to publicly comment on a matter, remember your duties under Rule 3.6: public communications that will have a substantial likelihood of prejudicing an adjudicative proceeding are prohibited.

DISHONESTY, FRAUD, DECEIT, MISREPRESENTATION: RULE 8.4

Do not use social media or other public internet platforms to engage in communication with an opposing party. Rules 4.2 and 4.3. While you can certainly view any

information that a party or witness has publically posted, never use a false identity or pretext to communicate with anyone related to a legal matter. Nor can you do this by having someone else do it for you. Rule 8.4(a)(1).

JUDGES

Judges are responsible for their social media conduct under the Judicial Canon of Ethics. It is unwise at best for judges and lawyers to communicate as "friends" on Facebook, particularly when the lawyer has a matter pending before the judge and/or regularly has cases with that judge.

As a matter of professionalism if nothing else, do not post rants about a judge. Consider the impact on the interests of your current and future clients.

BEWARE OF FORMING UNINTENDED ATTORNEY-CLIENT RELATIONSHIP

If you choose to answer questions from potential clients or participate in online forums, be careful to use cautionary language and disclaimers. Keep your answers generic and avoid specific facts. Remember also that social media communications with strangers can result in conflicts of interest. If someone is providing you with specific facts, you need to know his/her real name for your conflicts database.

BEWARE OF UNAUTHORIZED PRACTICE

Your communications online know no state line boundaries. Be clear about where you are licensed and disclaim any advice as to residents of other states.

RECOMMENDATIONS & ENDORSEMENTS: RULE 7.3(c)

Do not offer any *quid pro quo* for an endorsement or recommendation on LinkedIn, Avvo, Facebook, etc. If someone posts an endorsement or recommendation that contains inaccurate information (for example, regarding your expertise or experience), you need to either have it removed or post corrective information.

HAVE AND ENFORCE AN OFFICE POLICY ON SOCIAL MEDIA

Rules 5.1 and 5.3 impose a duty to supervise subordinate attorneys and non-attorney staff to ensure that their conduct is compatible with your professional obligations. Have a clear policy to ensure that your staff understands the ethical implications of use of social media.

CONCLUSION: *DON'T LET THE INTERNET MAKE YOU STUPID OR STEAL YOUR LICENSE*!

B. Privacy Does Not Exist in Social Media or the Internet In General

1. Full Control of Your Online Information Is Not Possible

While many Internet sites enable users to place some limitations on who may view or post content, the exact effect of such measures is not always easily predictable. As just one example, many web browsers have introduced an "anonymous" or "incognito" setting which disables the capture and retention of at least some information otherwise routinely preserved by the browser software in the course of using it to search the web. However, such settings typically affect only what is preserved on the user's local computer (the one on which the web browser is installed), and have no effect at all

on what information is available to the browser company or is captured by visited sites or by web bots systematically scouring the internet for personal information about you.

In addition, one can no longer ignore the fact that social media, search engines and other web sites capture for advertising and other uses huge amounts of information about anyone who uses or even just visits the sites. Take a look, as just one example, at the scope and detail of information routinely captured by Facebook (and that is what's accessible to the Facebook account user, not necessarily everything that Facebook captures). Attachment 3. Web sites are "free" essentially because of advertising, which employs ever more refined targeting of ads for products and services selectively to particular individuals deemed specifically amenable to purchasing them. And the only way to accomplish that is to capture ever more, and ever more specific, information about that individual, i.e., you, the user.

If you have any doubt that this fully applies to you, personally, try this: Run the exact same Google search on your computer and on a friend's or co-worker's computer, and compare the results. They will not be identical.

Admonishing users to read the privacy policies of utilized and visited sites has thus become something of a mantra. But apart from learning about and using privacy settings, if available, how useful is that admonition as a practical matter? Modifying or creating exceptions to anything in a given privacy policy is not an option. All one can do is use the application's privacy settings, if they exist. The choice as to the privacy policy itself, which always goes way beyond just settings, is simply to accept it or not, meaning use the site or avoid it altogether. Anyone who has downloaded an app to a smart phone

has seen this in action, and most people just capitulate, since it's either that or don't use the app.

In addition, comprehending privacy policies is not a quick and simple undertaking. Virtually all applications and web sites have the equivalent of a Privacy Policy and a separate User Agreement, both of which are triggered by creating an account and often just by using a site. Using LinkedIn as an example – a "social" media variant designed for professionals and used by vast numbers of lawyers – the User Agreement states (as of December 5, 2014):

> When you use our Services . . . , you are entering into a legal agreement and you agree to all of these terms. You also agree to our Privacy Policy, which covers how we collect, use, share, and store your personal information.

It goes on for 7 pages of mostly very small text. The Privacy Policy is 10 pages more. LinkedIn is one of the more transparent and user friendly sites in this regard. No two user agreements or privacy policies are exactly the same. And at the end of all that effort, of course, lies the reality that these provisions, along with available settings and how they function, can change at any time and often do.

2. Dangers from Posting and Removing Information

Given the above realities and those described below, it is this author's opinion that lawyers should assume that there is no such thing as full, predictable privacy for anything the lawyer posts or even just finds on the Internet. The same is true, of course, for clients. Cases are already being reported where clients have defeated their own cases by posting on social media activities irreconcilable with claims being asserted in pending litigation. In 2013, a judge set aside one of the largest loss of consortium awards in

Georgia history because of that plaintiff's Facebook postings. *Bowbliss v. Quick-Med Inc.*, Fulton County Superior Court File No. 10EV009640; *FCDR* at 1-2 (August 28, 2013). FCDR quotes one post by a plaintiff as stating that he "can not go to a gym til lawsuit over . . . due to it not looking right for me to be working out . . . and saying I have a bad arm." Other posts apparently indicated the marriage had already become very strained. And there was this reported gem: "Judge is f[***]ing on my case . . . dee and I aren't divorced yet because of piece of s[***] judge and case."

Lawyers should strongly caution clients against putting anything about a pending case out on the Internet in any form. Putting that advice in writing is always a good idea. So is reminding the client from time to time.

On the flip side, removing already posted content can create big problems. Remember, first, that removal does not equal disappearance in the Internet world. Worse, taking down content can constitute spoliation of evidence. *The Katiroll Company, Inc. v. Kati Roll And Platters, Inc. et al.*, Civil Action No. 10-3620 (GEB), 2011 U.S. Dist. LEXIS 85212 (U.S.D.C., D.N.J. August 3, 2011). A lawyer who advises a client to do so can face spoliation sanctions as well, *Allied Concrete v. Lester*, 285 Va. 295 (2013), and a lawyer's involvement in such conduct may also raise serious issues under GRPC Rules 3.3 (Candor Toward The Tribunal), 3.4 (Fairness to opposing party and counsel), 4.1 (Truthfulness In Statements to Others), 4.4 (Respect for Rights of Third Persons) and 8.4 (Misconduct)(especially subpart (a)(4)).

3. Merely Finding and Viewing On-line Information Has Ethics Implications

Another new reality is that merely *viewing* someone's information on-line can have unintended consequences, such as notifying the person that you have done so. ABA Formal Opinion 466 (April 23, 2014) addresses that fact in the context of lawyers who obtain on-line information about jurors or potential jurors before and/or during trial. Its conclusions:

- Unless limited by law or court order, it is permissible so long as the lawyer does not communicate with the person directly or through another.
- Sending an access request to the person's social media is not permitted. (That is defined as a communication (i) requesting access to information the person has not made public, and (ii) that would be the type of *ex parte* communication prohibited by Model Rule 3.5(b) [same rule number in the GRPC].)
- Rule 3.5(b) is not violated by the fact that the person is made aware by a network setting of internet viewing by a lawyer.
- If the information viewed reveals criminal or fraudulent misconduct, the lawyer must take reasonable remedial measures including, if necessary, disclosure to the tribunal.

C. Self-Promotion and Self-Defense on the Internet

1. A Closer Look at GRPC Rule 1.6

Unauthorized disclosure is a recurrent, central problem in both of these arenas. Rule 1.6(a) states the lawyer's affirmative obligation:

> A lawyer shall maintain in confidence **all information gained in the professional relationship** with a client, including information which the client has requested to be held inviolate **or** the disclosure of which would be embarrassing **or** would likely be detrimental to the client, **unless** the client gives informed consent, **except** for disclosures that are impliedly authorized in order to carry out the representation, or are required by these Rules or other law, or by order of the Court.

Note first that the language Ms. Petrig emphasized earlier – "all information gained in the professional relationship with a client" – presumptively extends the confidentiality obligation beyond information protected by the evidentiary attorney-client privilege, and beyond information the client has specifically identified as confidential. *See* Comment [5] to GRPC Rule 1.6. Common sense notions of what would be considered "confidential" are thus not reliable guides. For example, information may be confidential for Rule 1.6 purposes even though it might also be lawfully obtained by others, outside of the attorney-client relationship or discovery rules. **Your default presumption should be that if you got the information as part of representing a client, it is confidential regardless of source;** then you can think about whether one of the rule's exceptions applies.

Second, information may be confidential because of the potential effect of disclosure, rather than because of the source of the information. If disclosure would be

"embarrassing" or likely "detrimental" to the client, it is protected. Thus, though perhaps initially counterintuitive, the mere fact that information may be in the public domain in some fashion does *not* automatically mean it can be disclosed without client consent, if a lawyer has learned it in the course of representing the client.

2. Publicizing Successful Results

Whether on a lawyer's web site, a social media post, a blog, a discussion group, a comments thread or any of the myriad opportunities for on-line promotion, letting peers and potential clients know about a lawyer's successes has obvious value for building reputations, attracting new clients and increasing revenues. It is easy to think, why would a client object to publicizing a great outcome? It means they "won" or at least attained their goal, and if it was litigation, it is highly likely to be a matter of public record already. So what's the problem?

The answer becomes clear when one remembers that (1) confidentiality includes an "effects test," and (2) the audiences of public records of court proceedings are highly likely to be not only different than, but often infinitesimal in number compared to the potential recipients of the same information posted on the Internet. What if the success was acquittal of a client charged with aggravated sexual battery of a child? The truth of that result, and its existence in the "public record," perhaps even in the news media, does not diminish the fact that for most such clients it would be both embarrassing and highly likely to be detrimental in any number of ways. Such disclosure without client informed consent would almost certainly violate the ethical obligation imposed by Rule 1.6.

Many situations will be far less black and white than that example. The simple, foolproof (if there is such a thing) solution is explicit in Rule 1.6(a) itself: disclosure is prohibited "unless the client gives informed consent." Informed consent is a defined term which "denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct." GRPC Rule 1.0(h). **Always obtain informed consent before posting <u>any</u> information about a client's case or matter anywhere.**

What the client needs to know in order to make an informed decision will vary according to what is to be posted and where. It is impossible to list all possible considerations, but here are a few examples: Will the post be in the form of a client testimonial, or just be about the client's case? Will the client be named or remain anonymous (beware the possibility of revealing identity from the facts)? Will it appear on the lawyer's web site, intended to be seen only by those who choose to explore the site? (If so, will it appear prominently on the home page? Under a testimonials tab? As part of a slide show?) Or will the post be actively disseminated via Facebook, blog, tweet, discussion group or other "push" platform? In the latter case, who is the potential audience?

In addition, think about possible unintended consequences. For example, it may not be possible to limit posted information to a lawyer's web site, and it is likely impossible to assure that only someone browsing that web site will see it. Google and others use automated web crawlers to constantly amass, archive, package and redistribute information in various ways for various purposes. So one simple question

that perhaps the client should always be asked is this: Are you comfortable with the possibility that the posted information may pop up in a Google or Yahoo! search, say by a relative or a potential employer?

All such questions interact closely with what information, exactly, a client is willing after informed consent to disclose. You will have greater protection if the client consents to the verbatim content and exact location of the posting, and to the details and context of the posting within that location to the extent that is reasonably practicable. And while Rule 1.6 does not require it, written consent signed by the client is good prophylactic practice.

The Pennsylvania Bar Association recently issues formal advisory opinion discussing at length several aspects of the ethics issues implicated in lawyers use of social media. It is appended as Attachment 4. The opinion "addresses social media profiles and websites used by lawyers for business purposes, but does not address the issues relating to attorney advertising and marketing on social networking websites." It is not binding even in Pennsylvania, but does provide a primer on how to think about the application of the ethics rules in this realm.

3. Defending Yourself Against On-line Criticism By Clients: Can You? *Should* You?

Web sites like AVVO and Facebook present positive opportunities for lawyers, but the reverse is also true. What can you ethically do if an unreasonable, irate client or former client attacks you on-line with false statements and accusations, apart from a defamation action? Can you respond on-line using truthful information that otherwise

would be protected from disclosure by GRPC Rule 1.6, without obtaining client consent?

> Rule 1.6(b)(1)(iii) states:
>
> A lawyer may reveal information covered by paragraph (a) which the lawyer reasonably believes necessary . . . to establish a claim or defense on behalf of the lawyer in a **controversy** between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, **or** to respond to allegations in any proceeding concerning the lawyer's representation of the client;

An on-line attack obviously is not a criminal charge or civil claim, nor is it in a proceeding. Is it a "controversy"?

The best answer in Georgia at this time is that **in these circumstances disclosure not explicitly authorized by the client is very risky**. In 2014, the Georgia Supreme Court for the first time imposed discipline on a lawyer for disclosing confidential client information online, in response to negative comments about the lawyer posted by a former client on three consumer web sites. *In the Matter of Skinner*, 295 Ga. 217 (2014)(appended at Attachment 5). That case involved an uncontested divorce with long delays, increasing client dissatisfaction, and eventually a fee dispute and change of counsel. After the former client posted "negative reviews" with unspecified content, the lawyer responded by posting the client's name and employer, the amount paid to the lawyer, the county in which the divorce was filed, and a statement that the former client had a boyfriend. The Court had no difficulty concluding that those disclosures violated Rule 1.6, without need for any analysis or explanation.

The *Skinner* case should give lawyers great pause before disclosing any client information in response to client criticism, though it may not definitively resolve the issue in all circumstances. The unauthorized disclosures in *Skinner* were apparently so out of bounds in relation to the client reviews that the "controversy" exception of Rule 1.6 never came up. However, there is good reason to doubt that the exception will be recognized in this context if the Court does address it, not least because the legal definition of "controversy" simply does not fit online disputes like this:

> A litigated question; adversary proceeding in a court of law; a civil action or suit, either at law or in equity. . . . It differs from "case," which includes all suits, criminal as well as civil; whereas "controversy" is a civil and not a criminal proceeding.

Black's Law Dictionary Free On-line 2d Ed. (accessed October 9, 2013)(internal citations omitted). The few ethics decisions on point in other jurisdictions are mixed, and the summary in the *ABA Annotated Model Rules* at pp. 109-110 (2011)(quoted at appended Attachment 6) includes the statement that "[m]ere criticism of the lawyer, however, may be insufficient to warrant disclosures in self defense, even when the criticisms appear in the press."

For anyone willing to risk violating Rule 1.6 in these circumstances, the question still remains: *Should* you defend with disclosure of information about the client or case, or even defend at all? One school of thought is that, as professionals, lawyers should just accept this sort of thing as an occupational hazard and ignore it. (If it is a recurrent problem, that may well suggest that the lawyer has an actual underlying problem.) Most on-line denizens recognize by now that over-the-top criticisms are ubiquitous on the Internet, and would not expect lawyers to be immune from them. One libelous rant, this

thinking goes, is therefore unlikely to drive away droves of potential clients, and if it cannot be taken down it will eventually drop off, become submerged and/or be an obvious outlier.

Others suggest that if a response is deemed essential, it should be extremely limited and *disclose no client information* at all. Something like, "I respectfully disagree." Period. The end.

This author's view is that pragmatic considerations counsel against responding even to false and malicious attacks, at least as a long term strategy. Even "I respectfully disagree" is virtually certain to generate additional vitriol, and each increment of additional content is likely to add fuel to the fire and bulk to an exchange that could easily be regarded as unseemly. In addition, put yourself in the position of a potential client who sees this back and forth. Might not he or she naturally wonder if this publicly played out dispute portends undesirable conflict if the lawyer and potential client come to be at odds about the conduct or outcome of a case?

Note, however, that GRPC Rule 1.6 does not preclude lawyers from pursuing civil remedies for wrongful criticism or accusations posted by clients. A lawsuit is without doubt a controversy excepted from the Rule 1.6 prohibitions (at least if the claims are colorably meritorious; *see* GRPC Rule 3.1), and last year a Georgia lawyer prevailed rather dramatically against a former client's baseless criticisms, based on theories of fraud, libel *per se*, and false light invasion of privacy. *Pampattiwar v. Hinson*, 326 Ga.App. 163 (2014) (appended at Attachment 7).

Finally, a word about Better Business Bureaus. Through the ethics advice hot-line, the Office of the General Counsel has seen some instances where standard BBB practices, which apparently vary from place to place, directly conflict with lawyers' ethical obligations to their clients. For example, the BBB may forward a client complaint to the lawyer and ask for a substantive response before the BBB decides how to take the complaint into account in its "scoring" of the lawyer or firm as a business. To respond as requested would certainly violate GRPC Rule 1.6, but in one instance that caused a firm to get an "F" rating on the local BBB site. If you receive such a request, this author advises a strong response pointing out the ethical obligation of confidentiality about clients and their cases, the lawyer's refusal to breach that ethical duty, the disciplinary consequences of breach even if the lawyer was so inclined, and taking the bureau to task for even considering imposing a ratings penalty for doing what is ethically both required and right. There is at present no data regarding the effectiveness of that approach.

C. Ethics Implications Of "Cloud" Computing

Use of the "cloud" in legal practice is rapidly expanding and already commonplace. It brings significant benefits ranging from back-up unaffected by local conditions, to document and data access not confined to a particular physical computer or mobile device, to enabling easy collaboration with colleagues and clients, to use in courtroom presentations, and more. Volumes have been written on this subject, but there is no Georgia case or Formal Advisory Opinion. A recent Pennsylvania ethics opinion (appended as Attachment 8) thoroughly details most considerations as well as practical protective measures; this is only one bar association's view and of course it is

not binding in Georgia. Only a couple of general considerations are presented here, and they presume the reader knows what the "cloud" is (hint: it's the Internet).

The principle ethics implications of cloud computing are obvious and mirror those discussed above in other contexts, namely the risks of inadvertent disclosure of and unauthorized access to information protected by GRPC Rule 1.6. To that we should add the pragmatic concern for the preservation and integrity of the information stored in the cloud.

Thus, before utilizing a cloud service a lawyer should make sufficient inquires to be satisfied that there will be reasonable measures in place to guard against improper disclosure, such as password and related access security, encryption, policies regarding access of employees of the service itself, policies controlling requests for access by law enforcement, and the like. Admittedly, that generic sampling begs many potential questions. As a practical matter, negligence concepts may often suggest clearer answers than the ethics rules do.

In addition to Rule 1.6 concerns, use of the cloud presents a risk of loss or corruption of files, data and information entrusted to the cloud provider. Potential causes include technological failure, business failure (provider or lawyer), response to non-payment of service fees, malware, miscreant hackers, etc., etc. Hardware, software, systems and business policies and practices all have a role in planning for such contingencies. In this context, the inherent ease of duplicating digital information can be a positive benefit if appropriately controlled. And here, too, negligence concepts may be at least as useful as ethics rules in fashioning preventive solutions, although GRPC Rules 1.16(d)(obligation to return original client file upon termination of representation)

and 1.15(I)(obligation to segregate and preserve client property) cannot be ignored. The latter could apply, for example, to original documents that have intrinsic potential value to the case that is not equally true of copies.

TABLE OF CONTENTS OF APPENDED DOCUMENTS

ATTACHMENT 1

MOVING/REMOVING "REPLY ALL" IN MS OUTLOOK

CAVEAT: The following was received by the author of this CLE paper in response to comments posted after an on-line ABA Journal article. Since my reflexive default is Reply, I have not tried the following fixes and cannot vouch for their success or possible side-effects.

Try this. There are also several downloadable programs that will perform this function.

Click File tab, choose Options, and select Customize Ribbon.

Choose Respond in the right pane and click Remove.

Click New Group twice. Rename the first New Group (Custom) as "Respond (Custom)" and the second as "Reply all (Custom)."

At the top of the left pane, click Main Tabs from "Choose commands from."

In the left pane, expand Home (Mail) and Respond.

In the right pane, select Respond (Custom).

Add the commands "Post reply," "Reply," "Forward," "Meeting,"

"IM," and "More" from left frame to Respond (Custom) in the right pane one by one.

In the right pane, choose "Reply all (Custom)."

Add the command Reply All to "Reply all (Custom)."

Select "Reply all (Custom)" and use the Down button to move it under "Send/Receive (IMAP/POP)."

Click OK.

You can alter the steps above to eliminate the Reply All button altogether by creating only one New Group named Respond (Custom) that lacks the Reply All option. In all three versions of Outlook, you can still reply to all by pressing Ctrl-Shift-R, or by clicking Actions > Reply to All in Outlook 2003 and 2007.

Last December, CNET's Rob Lightner described Microsoft's free NoReplyAll add-on for Outlook 2010 that lets the sender of a message disable the Reply to All and Forward functions for the message. As Rob explains, the program includes a feature that lets you disable reply all for all the messages you receive.

ATTACHMENT 2

RICHARD H. KNOX, Plaintiff v. BISHOP ANTHONEE PATTERSON, Defendant

No. 2421

COMMON PLEAS COURT OF PHILADELPHIA COUNTY, PENNSYLVANIA

2011 Phila. Ct. Com. Pl. LEXIS 299; 21 Pa. D. & C.5th 149

January 11, 2011, Decided
January 13, 2011, Filed

CASE SUMMARY:

PROCEDURAL POSTURE: The court set forth its opinion in support of its order denying petitioner attorney's motion open/strike judgment. Petitioner had brought a breach of contract action against defendant former client. A judgment of non pros was entered, pursuant to *Pa.R.C.P. No. 1303*, after petitioner failed to appear twice for arbitration.

OVERVIEW: The court noted that the first time petitioner failed to appear for the arbitration scheduled in the matter, he insisted to the court that he would be more careful and had never made a mistake in all of his years practicing law. However, a new arbitration date was set and electronic notice was sent, which petitioner claimed he did not receive because he had not checked his e-mail for over four months and his legal secretary, his wife, was temporarily disabled and had not checked his electronic communications either. The court found that petitioner's excuses lacked merit as the court had a mandatory electronic e-filing notification system, which was required of all attorneys to comply. Further, petitioner knew that his wife was temporarily disabled and could not check his electronic notices, yet he failed to ensure he checked his electronic communications somehow during that time period.

OUTCOME: The court recommended that its order denying the petition to open/strike judgment be affirmed.

LexisNexis(R) Headnotes

Civil Procedure > Judgments > Relief From Judgment > Extraordinary Circumstances
Civil Procedure > Judgments > Relief From Judgment > Motions to Vacate
[HN1] A petition to open a judgment is addressed to the equitable powers of the court and is a matter of judicial discretion. The court will only exercise this discretion when (1) the petition has been promptly filed; (2) a meritorious defense can be shown; and (3) the failure to appear can be excused.

Civil Procedure > Pretrial Judgments > Default > Entry of Default Judgments
Civil Procedure > Pretrial Judgments > Default > Relief From Default
Civil Procedure > Appeals > Standards of Review > Abuse of Discretion
[HN2] A lower court's ruling refusing to open a default judgment will not be reversed unless there has been an error of law or a clear, manifest abuse of discretion.

Civil Procedure > Judgments > Relief From Judgment > Extraordinary Circumstances
Civil Procedure > Judgments > Relief From Judgment > Motions to Alter & Amend
Civil Procedure > Judgments > Relief From Judgment > Motions to Vacate
[HN3] A petition to open judgment must be filed within 10 days after the judgment is entered on the docket. *Pa.R.C.P. No. 237.3(b).*

Civil Procedure > Judgments > Relief From Judgment > Extraordinary Circumstances
Civil Procedure > Judgments > Relief From Judgment > Motions to Alter & Amend
Civil Procedure > Judgments > Relief From Judgment > Motions to Vacate
[HN4] Post-trial relief may be granted if a satisfactory excuse is given. An excuse is satisfactory if it would constitute a valid ground for a continuance. Examples include illness of counsel, a party, or a witness. Lack of notice after the paper mailing of an arbitration notice has been deemed an unsatisfactory excuse for post-trial relief.

COUNSEL: [*1] For Plaintiff: Mr. Richard H. Knox, Philadelphia, PA.

For Defendant: Mr. Willie Pollins, Philadelphia, PA.

JUDGES: Sandra Mazer Moss, J.

OPINION BY: Sandra Mazer Moss

OPINION

[**151] Sandra Mazer Moss, J.

The issue is whether the Petition to Open/Strike Judgment of May 24, 2010 should have been granted. For the foregoing reasons, We denied said Petition.

Facts and Procedural History

Petitioner Richard H. Knox ("Knox") is an octogenarian attorney representing himself, who on January 22, 2009 filed a Complaint alleging breach of contract against Defendant Bishop Anthonee Patterson ("Patterson") for alleged non-payment of his legal fees. Knox was retained in 2008 for a matter dealing with the transfer of money from a decedent's estate. Whether Patterson was retained as a principal or an agent of the Church is disputed.

Originally, a Judgment of Non Pros was entered, pursuant to *Pa. R. C. P. 1303(b)(2)*, when all parties failed to appear for the September 15, 2010 arbitration. This Judgment was later stricken on February 27, 2010 when Knox filed a Motion to Vacate judgment after admitting to having made a scheduling error. In that Petition Knox claimed this was the first time he made such an error in an arbitration hearing or in [*2] a regular trial case. *See* Knox's First Petition of Relief from Non-Pros, 09/29/09, ¶ 3. Moreover, Knox promised to be more careful and to not make the same [**152] error again. *Id.*

A new arbitration date was set for May 24, 2010. All parties were electronically noticed on March 2, 2010. Knox *again* failed to appear for arbitration. A second Judgment of Non Pros was entered that day. Subsequently, Knox filed a Petition to Strike/Open Judgment on June 17, 2010. While this Petition was originally granted, a subsequent reconsideration motion and oral argument led the Court on September 28, 2010 to deny Knox's Petition. Knox now appeals.

Knox originally argued that he had not received notice of the arbitration. *See* Knox's Second Petition of Relief from Non-Pros, 06/17/10, ¶¶ 3, 7. However, Patterson denied that Knox lacked notice and attached the electronic filing notifying the parties of the arbitration date. *See* Patterson Answer to Second Petition of Relief from Non-Pros, 07/07/10, ¶2, Ex. A. Subsequently, Knox argued while he has been practicing law for over fifty (50) years, he is not proficient in electronic communication and not familiar with e-mail. *See* Knox Supplemental Petition, Nunc Pro [*3] Tunc To Open/Strike Judgment, 07/13/10, ¶¶ 8-10. He stated when he became aware of the second Non Pros Judgment, he had not checked his e-mail for four (4) months, despite the mandatory e-filing system in Philadelphia,[1] of which he claims to have not been aware. *See generally id.* Knox's wife was his legal secretary for [**153] thirty-six (36) years and performed all the electronic work. *Id.* ¶ *4.* However, during the relevant period, he claims she was absent from work because of a temporary disabling injury. *See id.* ¶¶5-6. Therefore, P argues he never received notice of the second arbitration on May 24, 2010. *Id.* ¶9.

1 The Court implemented the electronic filing system in 2008. It became a mandatory requirement on January 5, 2009 at 9:00 AM, pursuant to Philadelphia Local Rule No. *205.4.

Discussion

The Petition to Open/Strike Judgment of May 24, 2010 should be denied. [HN1] "A petition to open a judgment is addressed to the equitable powers of the court and is a matter of judicial discretion. *Schultz v. Erie Ins. Exchange, 505 Pa. 90, 477 A.2d 471, 472 (Pa. 1984)* (internal citations omitted). "The court will *only* exercise this discretion when (1) the petition has been promptly filed; (2) a meritorious defense can [*4] be shown; *and* (3) the failure to appear can be excused." *Id.* (first emphasis added; second emphasis in original). [HN2] "A lower court's ruling refusing to open a default judgment will not be reversed unless there has been an error of law or a clear, manifest abuse of discretion." *Id.* (citing *Balk v. Ford Motor Co., 446 Pa. 137, 285 A.2d 128, 131 (1971)*).

This Court did not abuse its discretion and did not make a clear error of law. There are at least two strong reasons why this Court properly exercised its discretion

to deny Knox's Petition. First, Knox's Petition was not timely and fails the first prong of the three part test. [HN3] A Petition to Open Judgment must be filed within ten days after the judgment is entered on the docket. *See Pa. R.C.P. 237.3(b)*. The [**154] second Judgment of Non-Pros was entered and docketed May 24, 2010. Electronic notice of this Judgment was given June 1, 2010. Knox filed his Petition June 17, 2010. This was seventeen days after he received electronic notice and well past the ten day deadline. Therefore, Knox's Petition was untimely. Under the conjunctive three pronged test, Knox's Petition failed the first prong.

Second, Knox failed the third prong in providing a valid excuse for [*5] his failure to appear. [HN4] Post-trial relief may be granted if a *satisfactory excuse* is given. *Breza v. Don Farr Moving & Storage Co., 2003 PA Super 252, 828 A.2d 1131,1134 (Pa. Super. 2003)* (citing *Pa. R. C. P. 218*). An excuse is satisfactory if it would constitute a valid ground for a continuance. *Id.* Examples include illness of counsel, a party, or a witness, etc. *Id. at 1135* (internal citations omitted). Lack of notice after the paper mailing of an arbitration notice has been deemed an unsatisfactory excuse for post-trial relief. *Id.*

While *Farr* can technically be distinguished because it dealt with a mailed, hard-copy, the case is nevertheless analogous. Considering e-filing and electronic noticing is now the mandatory system in Philadelphia County, e-mail notification is analogous to the *Farr* paper mailing. Moreover, Knox does not allege he didn't receive the Court's email notification. Rather, he asserts lack of notice because he did not know how to retrieve this email.

Digging deeper, Knox's negligence is even more apparent. First, Knox he knew his wife (i.e. secretary) was temporarily disabled and could not check electronic [**155] notices. Knox, a very experienced attorney with an active caseload, knowing [*6] he was computer illiterate, should have ensured any important communication was discovered during her absence. First, he could have learned Philadelphia's e-filing notification system. Second, he could have hired a temporary secretary to fill the gap.. Knox, however, did nothing. He just let his electronic communications pile up until his wife returned.

What makes Knox's nonfeasance more egregious is that it was the second time it happened. Moreover, he promised to be "more careful" after his first Petition to Open was granted February 27, 2010. Knox knew to expect notification of a new arbitration date. Yet he never bothered to inquire after a hard-copy notification did not arrive. At the very least, an individual embarrassed about missing an earlier arbitration date and given a second chance should have followed through on his promise to be "more careful" by taking extra precautions to appear at a second arbitration. A simple telephone call to the Court during the almost three month period from March 2, 2010 to May 24, 2010 might have avoided this whole predicament. Therefore, Knox did not provide a satisfactory excuse for missing the second arbitration date and thus fails the third [*7] prong.

Knox may or may not have a meritorious claim for the alleged non-payment of his legal fees. However, we do not [**156] have to reach that question because Petitioner has failed to satisfy two of the three required prongs.

Conclusion

For the reasons stated above, Our Order denying the Petitioner's Petition to Open/Strike Judgment of May 24, 2010 should not be disturbed.

BY THE COURT:

/s/ Sandra Mazer Moss

Sandra Mazer Moss, J.

ATTACHMENT 3

where can I find my facebook data

Accessing Your Facebook Data

Where can I find my Facebook data?

- **Your Facebook Account**: Most of your data is available to you simply by logging into your account. For example, your Timeline contains posts you have shared on Facebook, along with comments and other interactions from people. Additionally, you can find your message and chat conversations by going to your inbox, or photos and videos you have added or been tagged in by going to those sections of your Timeline.
- **Activity Log**: Within your account, your activity log is a history of your activity on Facebook, from posts you have commented on or liked, to apps you have used, to anything you have searched for. Learn more.
- **Download Your Info**: This includes a lot of the same information available to you in your account and activity log, including your Timeline info, posts you have shared, messages, photos and more. Additionally, it includes information that is not available simply by logging into your account, like the ads you have clicked on, data like the IP addresses that are logged when you log into or out of Facebook, and more. To download your information, go to your Settings and click **Download a copy of your Facebook data**. Learn more.

What categories of my Facebook data are available to me?

These are the categories of Facebook data that are available to you either in your activity log or your downloaded data, or in both places. We have provided a short explanation of what each data category is and where you can find it. We store different categories of data for different time periods, so you may not find all of your data since you joined Facebook. You will not find information or content that you have deleted because this is deleted from Facebook servers.

Remember, most of your Facebook data is available to you simply by logging into your account (ex: all of your messages and chats are available in your inbox.) Also note that the categories of data that we receive, collect, and save may change over time. When this happens, this list will be updated.

What info is available?	**What is it?**	**Where can I find it?**
About Me	Information you added to the **About** section of your Timeline like relationships, work, education, where you live and more. It includes any updates or changes you made in the past and what is currently in the **About** section of your Timeline.	Activity Log Downloaded Info
Account Status History	The dates when your account was reactivated, deactivated, disabled or deleted.	Downloaded Info
Active Sessions	All stored active sessions, including date, time, device, IP address, machine cookie and browser information.	Downloaded Info
Ads Clicked	Dates, times and titles of ads clicked (limited retention period).	Downloaded Info
Address	Your current address or any past addresses you had on your account.	Downloaded Info
Ad Topics	A list of topics that you may be targeted against based on your stated likes, interests and other data you put in your Timeline.	Downloaded Info
	Any alternate names you have on your account (ex:	

Alternate Name	a maiden name or a nickname).	Downloaded Info
Apps	All of the apps you have added.	Downloaded Info
Birthday Visibility	How your birthday appears on your Timeline.	Downloaded Info
Chat	A history of the conversations you've had on Facebook Chat (a complete history is available directly from your messages inbox).	Downloaded Info
Check-ins	The places you've checked into.	Activity Log Downloaded Info Activity Log
Connections	The people who have liked your Page or Place, RSVPed to your event, installed your app or checked in to your advertised place within 24 hours of viewing or clicking on an ad or Sponsored Story.	Activity Log
Credit Cards	If you make purchases on Facebook (ex: in apps) and have given Facebook your credit card number.	Account Settings
Currency	Your preferred currency on Facebook. If you use Facebook Payments, this will be used to display prices and charge your credit cards.	Downloaded Info
Current City	The city you added to the **About** section of your Timeline.	Downloaded Info
Date of Birth	The date you added to Birthday in the **About** section of your Timeline.	Downloaded Info
Deleted Friends	People you've removed as friends.	Downloaded Info
Education	Any information you added to Education field in the About section of your Timeline.	Downloaded Info
Emails	Email addresses added to your account (even those you may have removed).	Downloaded Info
Events	Events you've joined or been invited to.	Activity Log Downloaded Info
Facial Recognition Data	A unique number based on a comparison of the photos you're tagged in. We use this data to help others tag you in photos.	Downloaded Info
Family	Friends you've indicated are family members.	Downloaded Info
Favorite Quotes	Information you've added to the Favorite Quotes section of the **About** section of your Timeline.	Downloaded Info
Followers	A list of people who follow you.	Downloaded Info
Following	A list of people you follow.	Activity Log
Friend Requests	Pending sent and received friend requests.	Downloaded Info
Friends	A list of your friends.	Downloaded Info
Gender	The gender you added to the **About** section of your Timeline.	Downloaded Info
Groups	A list of groups you belong to on Facebook.	Downloaded Info
Hidden from News Feed	Any friends, apps or pages you've hidden from your News Feed.	Downloaded Info
Hometown	The place you added to hometown in the **About** section of your Timeline.	Downloaded Info

IP Addresses	A list of IP addresses where you've logged into your Facebook account (won't include all historical IP addresses as they are deleted according to a retention schedule).	Downloaded Info
Last Location	The last location associated with an update.	Activity Log
Likes on Others' Posts	Posts, photos or other content you've liked.	Activity Log
Likes on Your Posts from others	Likes on your own posts, photos or other content.	Activity Log
Likes on Other Sites	Likes you've made on sites off of Facebook.	Activity Log
Linked Accounts	A list of the accounts you've linked to your Facebook account	Account Settings
Locale	The language you've selected to use Facebook in.	Downloaded Info
Logins	IP address, date and time associated with logins to your Facebook account.	Downloaded Info
Logouts	IP address, date and time associated with logouts from your Facebook account.	Downloaded Info
Messages	Messages you've sent and received on Facebook. Note, if you've deleted a message it won't be included in your download as it has been deleted from your account.	Downloaded Info
Name	The name on your Facebook account.	Downloaded Info
Name Changes	Any changes you've made to the original name you used when you signed up for Facebook.	Downloaded Info
Networks	Networks (affiliations with schools or workplaces) that you belong to on Facebook.	Downloaded Info
Notes	Any notes you've written and published to your account.	Activity Log
Notification Settings	A list of all your notification preferences and whether you have email and text enabled or disabled for each.	Downloaded Info
Pages You Admin	A list of pages you admin.	Downloaded Info
Pending Friend Requests	Pending sent and received friend requests.	Downloaded Info
Phone Numbers	Mobile phone numbers you've added to your account, including verified mobile numbers you've added for security purposes.	Downloaded Info
Photos	Photos you've uploaded to your account.	Downloaded Info
Photos Metadata	Any metadata that is transmitted with your uploaded photos.	Downloaded Info
Physical Tokens	Badges you've added to your account.	Downloaded Info
Pokes	A list of who's poked you and who you've poked. Poke content from our mobile poke app is not included because it's only available for a brief period of time. After the recipient has viewed the content it's permanently deleted from our systems.	Downloaded Info
Political Views	Any information you added to Political Views in the About section of Timeline.	Downloaded Info
	Anything you posted to your own Timeline, like	

Posts by You	photos, videos and status updates.	Activity Log
Posts by Others	Anything posted to your Timeline by someone else, like wall posts or links shared on your Timeline by friends.	Activity Log Downloaded Info
Posts to Others	Anything you posted to someone else's Timeline, like photos, videos and status updates.	Activity Log
Privacy Settings	Your privacy settings.	Privacy Settings Downloaded Info
Recent Activities	Actions you've taken and interactions you've recently had.	Activity Log Downloaded Info
Registration Date	The date you joined Facebook.	Activity Log Downloaded Info
Religious Views	The current information you added to Religious Views in the **About** section of your Timeline.	Downloaded Info
Removed Friends	People you've removed as friends.	Activity Log Downloaded Info
Screen Names	The screen names you've added to your account, and the service they're associated with. You can also see if they're hidden or visible on your account.	Downloaded Info
Searches	Searches you've made on Facebook.	Activity Log
Shares	Content (ex: a news article) you've shared with others on Facebook using the **Share** button or link.	Activity Log
Spoken Languages	The languages you added to Spoken Languages in the **About** section of your Timeline.	Downloaded Info
Status Updates	Any status updates you've posted.	Activity Log Downloaded Info
Work	Any current information you've added to Work in the About section of your Timeline.	Downloaded Info
Vanity URL	Your Facebook URL (ex: username or vanity for your account).	Visible in your Timeline URL
Videos	Videos you've posted to your Timeline.	Activity Log Downloaded Info

Was the content on this page helpful to you? Yes · No

Permalink · Share

English (US)

ATTACHMENT 4

FORMAL OPINION 2014-300

ETHICAL OBLIGATIONS FOR ATTORNEYS USING SOCIAL MEDIA

I. Introduction and Summary

"Social media" or "social networking" websites permit users to join online communities where they can share information, ideas, messages, and other content using words, photographs, videos and other methods of communication. There are thousands of these websites, which vary in form and content. Most of these sites, such as Facebook, LinkedIn, and Twitter, are designed to permit users to share information about their personal and professional activities and interests. As of January 2014, an estimated 74 percent of adults age 18 and over use these sites.[1]

Attorneys and clients use these websites for both business and personal reasons, and their use raises ethical concerns, both in how attorneys use the sites and in the advice attorneys provide to clients who use them. The Rules of Professional Conduct apply to all of these uses.

The issues raised by the use of social networking websites are highly fact-specific, although certain general principles apply. This Opinion reiterates the guidance provided in several previous ethics opinions in this developing area and provides a broad overview of the ethical concerns raised by social media, including the following:

1. Whether attorneys may advise clients about the content of the clients' social networking websites, including removing or adding information.
2. Whether attorneys may connect with a client or former client on a social networking website.
3. Whether attorneys may contact a represented person through a social networking website.
4. Whether attorneys may contact an unrepresented person through a social networking website, or use a pretextual basis for viewing information on a social networking site that would otherwise be private/unavailable to the public.
5. Whether attorneys may use information on a social networking website in client-related matters.
6. Whether a client who asks to write a review of an attorney, or who writes a review of an attorney, has caused the attorney to violate any Rule of Professional Conduct.
7. Whether attorneys may comment on or respond to reviews or endorsements.
8. Whether attorneys may endorse other attorneys on a social networking website.
9. Whether attorneys may review a juror's Internet presence.

[1] http://www.pewinternet.org/fact-sheets/social-networking-fact-sheet/

10. Whether attorneys may connect with judges on social networking websites.

This Committee concludes that:

1. Attorneys may advise clients about the content of their social networking websites, including the removal or addition of information.
2. Attorneys may connect with clients and former clients.
3. Attorneys may not contact a represented person through social networking websites.
4. Although attorneys may contact an unrepresented person through social networking websites, they may not use a pretextual basis for viewing otherwise private information on social networking websites.
5. Attorneys may use information on social networking websites in a dispute.
6. Attorneys may accept client reviews but must monitor those reviews for accuracy.
7. Attorneys may generally comment or respond to reviews or endorsements, and may solicit such endorsements.
8. Attorneys may generally endorse other attorneys on social networking websites.
9. Attorneys may review a juror's Internet presence.
10. Attorneys may connect with judges on social networking websites provided the purpose is not to influence the judge in carrying out his or her official duties.

This Opinion addresses social media profiles and websites used by lawyers for business purposes, but does not address the issues relating to attorney advertising and marketing on social networking websites. While a social media profile that is used exclusively for personal purposes (*i.e.,* to maintain relationships with friends and family) may not be subject to the Rules of Professional Conduct relating to advertising and soliciting, the Committee emphasizes that attorneys should be conscious that clients and others may discover those websites, and that information contained on those websites is likely to be subject to the Rules of Professional Conduct. Any social media activities or websites that promote, mention or otherwise bring attention to any law firm or to an attorney in his or her role as an attorney are subject to and must comply with the Rules.

II. Background

A social networking website provides a virtual community for people to share their daily activities with family, friends and the public, to share their interest in a particular topic, or to increase their circle of acquaintances. There are dating sites, friendship sites, sites with business purposes, and hybrids that offer numerous combinations of these characteristics. Facebook is currently the leading personal site, and LinkedIn is currently the leading business site. Other social networking sites include, but are not limited to, Twitter, Myspace, Google+, Instagram, AVVO, Vine, YouTube, Pinterest, BlogSpot, and Foursquare. On these sites, members create their own online "profiles," which may include biographical data, pictures and any other information they choose to post.

Members of social networking websites often communicate with each other by making their latest thoughts public in a blog-like format or via e-mail, instant messaging, photographs, videos, voice or videoconferencing to selected members or to the public at large. These services permit members to locate and invite other members into their personal networks (to "friend" them) as well as to invite friends of friends or others.

Social networking websites have varying levels of privacy settings. Some sites allow users to restrict who may see what types of content, or to limit different information to certain defined groups, such as the "public," "friends," and "others." For example, on Facebook, a user may make all posts available only to friends who have requested access. A less restrictive privacy setting allows "friends of friends" to see content posted by a specific user. A still more publicly-accessible setting allows anyone with an account to view all of a person's posts and other items.

These are just a few of the main features of social networking websites. This Opinion does not address every feature of every social networking website, which change frequently. Instead, this Opinion gives a broad overview of the main ethical issues that lawyers may face when using social media and when advising clients who use social media.

III. Discussion

A. Pennsylvania Rules of Professional Conduct: Mandatory and Prohibited Conduct

Each of the issues raised in this Opinion implicates various Rules of Professional Conduct that affect an attorney's responsibilities towards clients, potential clients, and other parties. Although no Pennsylvania Rule of Professional Conduct specifically addresses social networking websites, this Committee's conclusions are based upon the existing rules. The Rules implicated by these issues include:

- Rule 1.1 ("Competence")
- Rule 1.6 ("Confidentiality of Information")
- Rule 3.3 ("Candor Toward the Tribunal")
- Rule 3.4 ("Fairness to Opposing Party and Counsel")
- Rule 3.5 ("Impartiality and Decorum of the Tribunal")
- Rule 3.6 ("Trial Publicity")
- Rule 4.1 ("Truthfulness in Statements to Others")
- Rule 4.2 ("Communication with Person Represented by Counsel")
- Rule 4.3 ("Dealing with Unrepresented Person")
- Rule 8.2 ("Statements Concerning Judges and Other Adjudicatory Officers")
- Rule 8.4 ("Misconduct")

The Rules define the requirements and limitations on an attorney's conduct that may subject the attorney to disciplinary sanctions. While the Comments may assist an attorney in understanding or arguing the intention of the Rules, they are not enforceable in disciplinary proceedings.

B. General Rules for Attorneys Using Social Media and Advising Clients About Social Media

Lawyers must be aware of how these websites operate and the issues they raise in order to represent clients whose matters may be impacted by content posted on social media websites. Lawyers should also understand the manner in which postings are either public or private. A few Rules of

Professional Conduct are particularly important in this context and can be generally applied throughout this Opinion.

Rule 1.1 provides:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

As a general rule, in order to provide competent representation under Rule 1.1, a lawyer should advise clients about the content of their social media accounts, including privacy issues, as well as their clients' obligation to preserve information that may be relevant to their legal disputes.

Comment [8] to Rule 1.1 further explains that, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…." Thus, in order to provide competent representation in accordance with Rule 1.1, a lawyer should (1) have a basic knowledge of how social media websites work, and (2) advise clients about the issues that may arise as a result of their use of these websites.

Another Rule applicable in almost every context, and particularly relevant when social media is involved, is Rule 8.4 ("Misconduct"), which states in relevant part:

> It is professional misconduct for a lawyer to:
> …
> (c) engage in conduct involving dishonesty, fraud, deceit or misrepresentation;

This Rule prohibits "dishonesty, fraud, deceit or misrepresentation." Social networking easily lends itself to dishonesty and misrepresentation because of how simple it is to create a false profile or to post information that is either inaccurate or exaggerated. This Opinion frequently refers to Rule 8.4, because its basic premise permeates much of the discussion surrounding a lawyer's ethical use of social media.

C. Advising Clients on the Content of their Social Media Accounts

As the use of social media expands, so does its place in legal disputes. This is based on the fact that many clients seeking legal advice have at least one account on a social networking site. While an attorney is not responsible for the information posted by a client on the client's social media profile, an attorney may and often should advise a client about the content on the client's profile.

Against this background, this Opinion now addresses the series of questions raised above.

1. Attorneys May, Subject to Certain Limitations, Advise Clients About The Content Of Their Social Networking Websites

Tracking a client's activity on social media may be appropriate for an attorney to remain informed about developments bearing on the client's legal dispute. An attorney can reasonably expect that opposing counsel will monitor a client's social media account.

For example, in a Miami, Florida case, a man received an $80,000.00 confidential settlement payment for his age discrimination claim against his former employer.[2] However, he forfeited that settlement after his daughter posted on her Facebook page "Mama and Papa Snay won the case against Gulliver. Gulliver is now officially paying for my vacation to Europe this summer. SUCK IT." The Facebook post violated the confidentiality agreement in the settlement and, therefore, cost the Plaintiff $80,000.00.

The Virginia State Bar Disciplinary Board[3] suspended an attorney for five years for (1) instructing his client to delete certain damaging photographs from his Facebook account, (2) withholding the photographs from opposing counsel, and (3) withholding from the trial court the emails discussing the plan to delete the information from the client's Facebook page. The Virginia State Bar Disciplinary Board based the suspension upon the attorney's violations of Virginia's rules on candor toward the tribunal, fairness to opposing counsel, and misconduct. In addition, the trial court imposed $722,000 in sanctions ($542,000 upon the lawyer and $180,000 upon his client) to compensate opposing counsel for their legal fees.[4]

While these may appear to be extreme cases, they are indicative of the activity that occur involving social media. As a result, lawyers should be certain that their clients are aware of the ramifications of their social media actions. Lawyers should also be aware of the consequences of their own actions and instructions when dealing with a client's social media account.

Three Rules of Professional Conduct are particularly important when addressing a lawyer's duties relating to a client's use of social media.

Rule 3.3 states:

> (a) A lawyer shall not knowingly:
>
> (1) make a false statement of material fact or law to a tribunal or fail to correct a false statement of material fact or law previously made to the tribunal by the lawyer; …
>
> (3) offer evidence that the lawyer knows to be false. If a lawyer, the lawyer's client, or a witness called by the lawyer, has offered material evidence before a tribunal or in an ancillary proceeding conducted pursuant to a tribunal's adjudicative authority, such as a deposition, and the lawyer comes to know of its falsity, the lawyer shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal. A lawyer may refuse to offer evidence, other than the testimony of a defendant in a criminal matter, that the lawyer reasonably believes is false.
>
> (b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal

[2] "Girl costs father $80,000 with 'SUCK IT' Facebook Post, March 4, 2014: http://www.cnn.com/2014/03/02/us/facebook-post-costs-father/

[3] *In the Matter of Matthew B. Murray*, VSB Nos. 11-070-088405 and 11-070-088422 (June 9, 2013)

[4] *Lester v. Allied Concrete Co.,* Nos. CL08-150 and CL09-223 (Charlotte, VA Circuit Court, October 21, 2011)

or fraudulent conduct related to the proceeding shall take reasonable remedial measures, including, if necessary, disclosure to the tribunal.

(c) The duties stated in paragraphs (a) and (b) continue to the conclusion of the proceeding, and apply even if compliance requires disclosure of information otherwise protected by Rule 1.6.

Rule 3.4 states:

> A lawyer shall not:
>
> (a) unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value or assist another person to do any such act;

Rule 4.1 states:

> In the course of representing a client a lawyer shall not knowingly:
> (a) make a false statement of material fact or law to a third person; or
> (b) fail to disclose a material fact to a third person when disclosure is necessary to avoid aiding and abetting a criminal or fraudulent act by a client, unless disclosure is prohibited by Rule 1.6.

The Rules do not prohibit an attorney from advising clients about their social networking websites. In fact, and to the contrary, a competent lawyer should advise clients about the content that they post publicly online and how it can affect a case or other legal dispute.

The Philadelphia Bar Association Professional Guidance Committee issued Opinion 2014-5, concluding that a lawyer may advise a client to change the privacy settings on the client's social media page but may not instruct a client to destroy any relevant content on the page. Additionally, a lawyer must respond to a discovery request with any relevant social media content posted by the client. The Committee found that changing a client's profile to "private" simply restricts access to the content of the page but does not completely prevent the opposing party from accessing the information. This Committee agrees with and adopts the guidance provided in the Philadelphia Bar Association Opinion.

The Philadelphia Committee also cited the Commercial and Federal Litigation Section of the New York State Bar Association and its "Social Media Guidelines," which concluded that a lawyer may advise a client about the content of the client's social media page, to wit:

- A lawyer may advise a client as to what content may be maintained or made private on her social media account, as well as to what content may be "taken down" or removed, whether posted by the client or someone else, as long as there is no violation of common law or any statute, rule, or regulation relating to the preservation of information.
- Unless an appropriate record of the social media information or data is preserved, a party or nonparty may not delete information from a social media profile that is subject

> to a duty to preserve. This duty arises when the potential for litigation or other conflicts arises [5]

In 2014 Formal Ethics Opinion 5, the North Carolina State Bar concluded that a lawyer may advise a client to remove information on social media if not spoliation or otherwise illegal.[6]

This Committee agrees with and adopts these recommendations, which are consistent with Rule 3.4(a)'s prohibition against "unlawfully alter[ing], destroy[ing] or conceal[ing] a document or other material having potential evidentiary value." Thus, a lawyer may not instruct a client to alter, destroy, or conceal any relevant information, regardless whether that information is in paper or digital form. A lawyer may, however, instruct a client to delete information that may be damaging from the client's page, provided the conduct does not constitute spoliation or is otherwise illegal, but must take appropriate action to preserve the information in the event it is discoverable or becomes relevant to the client's matter.

Similarly, an attorney may not advise a client to post false or misleading information on a social networking website; nor may an attorney offer evidence from a social networking website that the attorney knows is false. Rule 4.1(a) prohibits an attorney from making "a false statement of material fact or law." If an attorney knows that information on a social networking site is false, the attorney may not present that as truthful information. It has become common practice for lawyers to advise clients to refrain from posting any information relevant to a case on any website, and to refrain from using these websites until the case concludes.

2. Attorneys May Ethically Connect with Clients or Former Clients on Social Media

Social media provides many opportunities for attorneys to contact and connect with clients and other relevant persons. While the mode of communication has changed, the Rules that generally address an attorney's communications with others still apply.

There is no *per se* prohibition on an attorney connecting with a client or former client on social media. However, an attorney must continue to adhere to the Rules and maintain a professional relationship with clients. If an attorney connects with clients or former clients on social networking sites, the attorney should be aware that his posts may be viewed by clients and former clients.

Although this Committee does not recommend doing so, if an attorney uses social media to communicate with a client relating to representation of the client, the attorney should retain records of those communications containing legal advice. As outlined below, an attorney must not reveal confidential client information on social media. While the Rules do not prohibit connecting with clients on social media, social media may not be the best platform to connect with clients, particularly in light of the difficulties that often occur when individuals attempt to adjust their privacy settings.

---

[5] *Social Media Ethics Guidelines*, The Commercial and Federal Litigation Section of the New York State Bar Association, March 18, 2014 at 11 (footnote omitted).

[6] http://www.ncbar.com/ethics/printopinion.asp?id=894

3. Attorneys May Not Ethically Contact a Represented Person Through a Social Networking Website

Attorneys may also use social media to contact relevant persons in a conflict, but within limitations. As a general rule, if contacting a party using other forms of communication would be prohibited,[7] it would also be prohibited while using social networking websites.

Rule 4.2 states:

> In representing a client, a lawyer shall not communicate about the subject of the representation with a person the lawyer knows to be represented by another lawyer in the matter, unless the lawyer has the consent of the other lawyer or is authorized to do so by law or a court order.

Regardless of the method of communication, Rule 4.2 clearly states that an attorney may not communicate with a represented party without the permission of that party's lawyer. Social networking websites increase the number of ways to connect with another person but the essence of that connection is still a communication. Contacting a represented party on social media, even without any pretext, is limited by the Rules.

The Philadelphia Bar Association Professional Guidance Committee concluded in Opinion 2009-02,[8] that an attorney may not use an intermediary to access a witness' social media profiles. The inquirer sought access to a witness' social media account for impeachment purposes. The inquirer wanted to ask a third person, *i.e.*, "someone whose name the witness will not recognize," to go to Facebook and Myspace and attempt to "friend" the witness to gain access to the information on the pages. The Committee found that this type of pretextual "friending" violates Rule 8.4(c), which prohibits the use of deception. The action also would violate Rule 4.1 (discussed below) because such conduct amounts to a false statement of material fact to the witness.

The San Diego County Bar Legal Ethics Committee issued similar guidance in Ethics Opinion 2011-2,[9] concluding that an attorney is prohibited from making an *ex parte* "friend" request of a represented party to view the non-public portions of a social networking website. Even if the attorney clearly states his name and purpose for the request, the conduct violates the Rule against communication with a represented party. Consistent with this Opinion, this Committee also finds that "friending" a represented party violates Rule 4.2.

While it would be forbidden for a lawyer to "friend" a represented party, it would be permissible for the lawyer to access the public portions of the represented person's social networking site, just as it would be permissible to review any other public statements the person makes. The New York State

---

[7] *See, e.g.,* Formal Opinion 90-142 (updated by 2005-200), in which this Committee concluded that, unless a lawyer has the consent of opposing counsel or is authorized by law to do so, in representing a client, a lawyer shall not conduct ex parte communications about the matter of the representation with present managerial employees of an opposing party, and with any other employee whose acts or omissions may be imputed to the corporation for purposes of civil or criminal liability.

[8] Philadelphia Bar Assn., Prof'l Guidance Comm., Op. 2009-02 (2009).

[9] San Diego County Bar Assn., Legal Ethics Comm., Op. 2011-2 (2011).

Bar Association Committee on Professional Ethics issued Opinion 843,[10] concluded that lawyers may access the public portions of other parties' social media accounts for use in litigation, particularly impeachment. The Committee found that there is no deception in accessing a public website; it also cautioned, however, that a lawyer should not request additional access to the social networking website nor have someone else do so.

This Committee agrees that accessing the public portion of a represented party's social media site does not involve an improper contact with the represented party because the page is publicly accessible under Rule 4.2. However, a request to access the represented party's private page is a prohibited communication under Rule 4.2

4. Attorneys May Generally Contact an Unrepresented Person Through a Social Networking Website But May Not Use a Pretextual Basis For Viewing Otherwise Private Information[11]

Communication with an unrepresented party through a social networking website is governed by the same general rule that, if the contact is prohibited using other forms of communication, then it is also prohibited using social media.

Rule 4.3 states in relevant part:

> (a) In dealing on behalf of a client with a person who is not represented by counsel, a lawyer shall not state or imply that the lawyer is disinterested. …
> (c) When the lawyer knows or reasonably should know that the unrepresented person misunderstands the lawyer's role in the matter, the lawyer should make reasonable efforts to correct the misunderstanding.

Connecting with an unrepresented person through a social networking website may be ethical if the attorney clearly identifies his or her identity and purpose. Particularly when using social networking websites, an attorney may not use a pretextual basis when attempting to contact the unrepresented person. Rule 4.3(a) instructs that "a lawyer shall not state or imply that the lawyer is disinterested." Additionally, Rule 8.4(c) (discussed above) prohibits a lawyer from using deception. For example, an attorney may not use another person's name or online identity to contact an unrepresented person; rather, the attorney must use his or her own name and state the purpose for contacting the individual.

In Ohio, a former prosecutor was fired after he posed as a woman on a fake Facebook account in order to influence an accused killer's alibi witnesses to change their testimony[12]. He was fired for "unethical behavior," which is also consistent with the Pennsylvania Rules. Contacting witnesses under false pretenses constitutes deception.

---

[10] New York State Bar Assn., Comm. on Prof'l Ethics, Op. 843 (2010).

[11] Attorneys may be prohibited from contacting certain persons, despite their lack of representation. This portion of this Opinion only addresses communication and contact with persons with whom such contact is not otherwise prohibited by the Rules, statute or some other basis.

[12] "Aaron Brockler, Former Prosecutor, Fired for Posing as Accused Killer's Ex-Girlfriend on Facebook," June 7, 2013. http://www.cnn.com/2014/03/02/us/facebook-post-costs-father/

Many Ethics Committees have addressed whether an attorney may contact an unrepresented person on social media. The Kentucky Bar Association Ethics Committee[13] concluded that a lawyer may access the social networking site of a third person to benefit a client within the limits of the Rules. The Committee noted that even though social networking sites are a new medium of communication, "[t]he underlying principles of fairness and honesty are the same, regardless of context."[14] The Committee found that the Rules would not permit a lawyer to communicate through social media with a represented party. But, the Rules do not prohibit social media communication with an unrepresented party provided the lawyer is not deceitful or dishonest in the communication.

As noted above, in Opinion 2009-02,[15] the Philadelphia Bar Association Professional Guidance Committee concluded that an attorney may not access a witness' social media profiles by deceptively using a third party intermediary. Use of an alias or other deceptive conduct violates the Rules as well, regardless whether it is permissible to contact a particular person.

The New Hampshire Bar Association Ethics Committee agreed with the Philadelphia Opinion in Advisory Opinion 2012-13/05,[16] concluding that a lawyer may not use deception to access the private portions of an unrepresented person's social networking account. The Committee noted, "A lawyer has a duty to investigate but also a duty to do so openly and honestly, rather than through subterfuge."

The Oregon State Bar Legal Ethics Committee concurred with these opinions as well in Opinion 2013-189,[17] concluding that a lawyer may request access to an unrepresented party's social networking website if the lawyer is truthful and does not employ deception.

These Committees consistently conclude that a lawyer may not use deception to gain access to an unrepresented party's page, but a lawyer may request access using his or her real name. There is, however, a split of authority among these Committees. The Philadelphia and New Hampshire Committees would further require the lawyer to state the purpose for the request, a conclusion with which this Committee agrees. These Committees found that omitting the purpose of the contact implies that the lawyer is disinterested, in violation of Rule 4.3(a).

This Committee agrees with the Philadelphia Opinion (2009-02) and concludes that a lawyer may not use deception to gain access to an unrepresented person's social networking site. A lawyer may ethically request access to the site, however, by using the lawyer's real name and by stating the lawyer's purpose for the request. Omitting the purpose would imply that the lawyer is disinterested, contrary to Rule 4.3(a).

5. Attorneys May Use Information Discovered on a Social Networking Website in a Dispute

If a lawyer obtains information from a social networking website, that information may be used in a legal dispute provided the information was obtained ethically and consistent with other portions of

[13] Kentucky Bar Assn., Ethics Comm., Formal Op. KBA E-434 (2012).
[14] *Id.* at 2.
[15] Philadelphia Bar Assn., Prof'l Guidance Comm., Op. 2009-02 (2009).
[16] New Hampshire Bar Assn., Ethics Comm., Op. 2012-13/05 (2012).
[17] Oregon State Bar, Legal Ethics Comm., Op. 2013-189 (2013).

this Opinion. As mentioned previously, a competent lawyer has the duty to understand how social media works and how it may be used in a dispute. Because social networking websites allow users to instantaneously post information about anything the user desires in many different formats, a client's postings on social media may potentially be used against the client's interests. Moreover, because of the ease with which individuals can post information on social media websites, there may be an abundance of information about the user that may be discoverable if the user is ever involved in a legal dispute.

For example, in 2011, a New York[18] court ruled against a wife's claim for support in a matrimonial matter based upon evidence from her blog that contradicted her testimony that she was totally disabled, unable to work in any capacity, and rarely left home because she was in too much pain. The posts confirmed that the wife had started belly dancing in 2007, and the Court learned of this activity in 2009 when the husband attached the posts to his motion papers. The Court concluded that the wife's postings were relevant and could be deemed as admissions by the wife that contradicted her claims.

Courts have, with increasing frequency, permitted information from social media sites to be used in litigation, and have granted motions to compel discovery of information on private social networking websites when the public profile shows relevant evidence may be found.

For example, in *McMillen v. Hummingbird Speedway, Inc.,*[19] the Court of Common Pleas of Jefferson County, Pennsylvania granted a motion to compel discovery of the private portions of a litigant's Facebook profile after the opposing party produced evidence that the litigant may have misrepresented the extent of his injuries. In a New York case, *Romano v. Steelcase Inc.,*[20] the Court similarly granted a defendant's request for access to a plaintiff's social media accounts because the Court believed, based on the public portions of plaintiff's account, that the information may be inconsistent with plaintiff's claims of loss of enjoyment of life and physical injuries, thus making the social media accounts relevant.

In *Largent v. Reed,*[21] a Pennsylvania Court of Common Pleas granted a discovery request for access to a personal injury plaintiff's social media accounts. The Court engaged in a lengthy discussion of Facebook's privacy policy and Facebook's ability to produce subpoenaed information. The Court also ordered that plaintiff produce her login information for opposing counsel and required that she make no changes to her Facebook for thirty-five days while the defendant had access to the account.

Conversely, in *McCann v. Harleysville Insurance Co.,*[22] a New York court denied a defendant access to a plaintiff's social media account because there was no evidence on the public portion of the profile to suggest that there was relevant evidence on the private portion. The court characterized this request as a "fishing expedition" that was too broad to be granted. Similarly, in *Trail v. Lesko,*[23] Judge R. Stanton Wettick, Jr. of the Court of Common Pleas of Allegheny County denied a party access to a

[18] *B.M. v D.M.,* 31 Misc. 3d 1211(A) (N.Y. Sup. Ct. 2011).
[19] *McMillen v. Hummingbird Speedway, Inc.,* 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. County Ct. 2010).
[20] *Romano v Steelcase Inc.,* 30 Misc. 3d 426 (N.Y. Sup. Ct. 2010).
[21] *Largent v. Reed*, No. 2009-1823 (Pa.Ct.Com.Pl. Franklin Cty. 2011).
[22] *McCann v. Harleysville Ins. Co. of N.Y.,* 78 A.D.3d 1524 (N.Y. App. Div. 4th Dep't 2010).
[23] *Trail v. Lesko,* 2012 Pa. Dist. & Cnty. Dec. LEXIS 194 (Pa. County Ct. 2012).

plaintiff's social media accounts, concluding that, under Pa. R.Civ.P. 4011(b), the defendant did not produce any relevant evidence to support its request; therefore, granting access to the plaintiff's Facebook account would have been needlessly intrusive.

6. Attorneys May Generally Comment or Respond to Reviews or Endorsements, and May Solicit Such Endorsements Provided the Reviews Are Monitored for Accuracy

Some social networking websites permit a member or other person, including clients and former clients, to recommend or endorse a fellow member's skills or accomplishments. For example, LinkedIn allows a user to "endorse" the skills another user has listed (or for skills created by the user). A user may also request that others endorse him or her for specified skills. LinkedIn also allows a user to remove or limit endorsements. Other sites allow clients to submit reviews of an attorney's performance during representation. Some legal-specific social networking sites focus exclusively on endorsements or recommendations, while other sites with broader purposes can incorporate recommendations and endorsements into their more relaxed format. Thus, the range of sites and the manner in which information is posted varies greatly.

Although an attorney is not responsible for the content that other persons, who are not agents of the attorney, post on the attorney's social networking websites, an attorney (1) should monitor his or her social networking websites, (2) has a duty to verify the accuracy of any information posted, and (3) has a duty to remove or correct any inaccurate endorsements. For example, if a lawyer limits his or her practice to criminal law, and is "endorsed" for his or her expertise on appellate litigation on the attorney's LinkedIn page, the attorney has a duty to remove or correct the inaccurate endorsement on the LinkedIn page. This obligation exists regardless of whether the information was posted by the attorney, by a client, or by a third party. In addition, an attorney may be obligated to remove endorsements or other postings posted on sites that the attorney controls that refer to skills or expertise that the attorney does not possess.

Similarly, the Rules do not prohibit an attorney from soliciting reviews from clients about the attorney's services on an attorney's social networking site, nor do they prohibit an attorney from posting comments by others.[24] Although requests such as these are permissible, the attorney should monitor the information so as to verify its accuracy.

Rule 7.2 states, in relevant part:

> (d) No advertisement or public communication shall contain an endorsement by a celebrity or public figure.
> (e) An advertisement or public communication that contains a paid endorsement shall disclose that the endorser is being paid or otherwise compensated for his or her appearance or endorsement.

Rule 7.2(d) prohibits any endorsement by a celebrity or public figure. A lawyer may not solicit an endorsement nor accept an unsolicited endorsement from a celebrity or public figure on social

[24] In *Dwyer v. Cappell*, 2014 U.S. App. LEXIS 15361 (3d Cir. N.J. Aug. 11, 2014), the Third Circuit ruled that an attorney may include accurate quotes from judicial opinions on his website, and was not required to reprint the opinion in full.

media. Additionally, Rule 7.2(e) mandates disclosure if an endorsement is made by a paid endorser. Therefore, if a lawyer provides any type of compensation for an endorsement made on social media, the endorsement must contain a disclosure of that compensation.

Even if the endorsement is not made by a celebrity or a paid endorser, the post must still be accurate. Rule 8.4(c) is again relevant in this context. This Rule prohibits lawyers from dishonest conduct and making misrepresentations. If a client or former client writes a review of a lawyer that the lawyer knows is false or misleading, then the lawyer has an obligation to correct or remove the dishonest information within a reasonable amount of time. If the lawyer is unable to correct or remove the listing, he or she should contact the person posting the information and request that the person remove or correct the item.

The North Carolina State Bar Ethics Committee issued Formal Ethics Opinion 8,[25] concluding that a lawyer may accept recommendations from current or former clients if the lawyer monitors the recommendations to ensure that there are no ethical rule violations. The Committee discussed recommendations in the context of LinkedIn where an attorney must accept the recommendation before it is posted.[26] Because the lawyer must review the recommendation before it can be posted, there is a smaller risk of false or misleading communication about the lawyer's services. The Committee also concluded that a lawyer may request a recommendation from a current or former client but limited that recommendation to the client's level of satisfaction with the lawyer-client relationship.

This Committee agrees with the North Carolina Committee's findings. Attorneys may request or permit clients to post positive reviews, subject to the limitations of Rule 7.2, but must monitor those reviews to ensure they are truthful and accurate.

7. Attorneys May Comment or Respond to Online Reviews or Endorsements But May Not Reveal Confidential Client Information

Attorneys may not disclose confidential client information without the client's consent. This obligation of confidentiality applies regardless of the context. While the issue of disclosure of confidential client information extends beyond this Opinion, the Committee emphasizes that attorneys may not reveal such information absent client approval under Rule 1.6. Thus, an attorney may not reveal confidential information while posting celebratory statements about a successful matter, nor may the attorney respond to client or other comments by revealing information subject to the attorney-client privilege. Consequently, a lawyer's comments on social media must maintain attorney/client confidentiality, regardless of the context, absent the client's informed consent.

This Committee has opined, in Formal Opinion 2014-200,[27] that lawyers may not reveal client confidential information in response to a negative online review. Confidential client information is defined as "information relating to representation," which is generally very broad. While there are

[25] North Carolina State Bar Ethics Comm., Formal Op. 8 (2012).

[26] Persons with profiles on LinkedIn no longer are required to approve recommendations, but are generally notified of them by the site. This change in procedure highlights the fact that sites and their policies and procedures change rapidly, and that attorneys must be aware of their listings on such sites.

[27] Pennsylvania Bar Assn, Ethics Comm., Formal Op. 2014-200 (2014).

certain circumstances that would allow a lawyer to reveal confidential client information, a negative online client review is not a circumstance that invokes the self-defense exception.

As Rule 1.6 states:

> (a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).
> (b) A lawyer shall reveal such information if necessary to comply with the duties stated in Rule 3.3.
> (c) A lawyer may reveal such information to the extent that the lawyer reasonably believes necessary:
> (4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim or disciplinary proceeding against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client
> (d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.
> (e) The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.

Thus, any information that an attorney posts on social media may not violate attorney/client confidentiality.

An attorney's communications to a client are also confidential. In *Gillard v. AIG Insurance Company,*[28] the Pennsylvania Supreme Court ruled that the attorney-client privilege extends to communications from attorney to client. The Court held that "the attorney-client privilege operates in a two-way fashion to protect confidential client-to-attorney or attorney-to-client communications made for the purpose of obtaining or providing professional legal advice."[29] The court noted that communications from attorney to client come with a certain expectation of privacy. These communications only originate because of a confidential communication from the client. Therefore, even revealing information that the attorney has said to a client may be considered a confidential communication, and may not be revealed on social media or elsewhere.

Responding to a negative review can be tempting but lawyers must be careful about what they write. The Hearing Board of the Illinois Attorney Registration and Disciplinary Commission reprimanded an attorney for responding to a negative client review on the lawyer referral website AVVO[30]. In her response, the attorney mentioned confidential client information, revealing that the client had been in a physical altercation with a co-worker. While the Commission did not prohibit an attorney from

[28] *Gillard v. AIG Insurance Co.*, 15 A.3d 44 (Pa. 2011).
[29] *Id.* at 59.
[30] *In Re Tsamis*, Comm. File No. 2013PR00095 (Ill. 2013).

responding, in general, to a negative review on a site such as AVVO, it did prohibit revealing confidential client information in that type of reply.

The Illinois disciplinary action is consistent with this Committee's recent Opinion and with the Pennsylvania Rules. A lawyer is not permitted to reveal confidential information about a client even if the client posts a negative review about the lawyer. Rule 1.6(d) instructs a lawyer to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of . . . information relating to the representation of a client." This means that a lawyer must be mindful of any information that the lawyer posts pertaining to a client. While a response may not contain confidential client information, an attorney is permitted to respond to reviews or endorsements on social media. These responses must be accurate and truthful representations of the lawyer's services.

Also relevant is Rule 3.6, which states:

> (a) A lawyer who is participating or has participated in the investigation or litigation of a matter shall not make an extrajudicial statement that the lawyer knows or reasonably should know will be disseminated by means of public communication and will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter.

This Rule prohibits lawyers from making extrajudicial statements through public communication during an ongoing adjudication. This encompasses a lawyer updating a social media page with information relevant to the proceeding. If a lawyer's social media account is generally accessible publicly then any posts about an ongoing proceeding would be a public communication. Therefore, lawyers should not be posting about ongoing matters on social media when such matters would reveal confidential client information.

For example, the Supreme Court of Illinois suspended an attorney for 60 days[31] for writing about confidential client information and client proceedings on her personal blog. The attorney revealed information that made her clients easily identifiable, sometimes even using their names. The Illinois Attorney Registration and Disciplinary Commission had argued in the matter that the attorney knew or should have known that her blog was accessible to others using the internet and that she had not made any attempts to make her blog private.

Social media creates a wider platform of communication but that wider platform does not make it appropriate for an attorney to reveal confidential client information or to make otherwise prohibited extrajudicial statements on social media.

8. Attorneys May Generally Endorse Other Attorneys on Social Networking Websites

Some social networking sites allow members to endorse other members' skills. An attorney may endorse another attorney on a social networking website provided the endorsement is accurate and not misleading. However, celebrity endorsements are not permitted nor are endorsements by judges. As previously noted, Rule 8.4(c) prohibits an attorney from being dishonest or making

[31] *In Re Peshek*, No. M.R. 23794 (Il. 2010); Compl.., *In Re Peshek*, Comm. No. 09 CH 89 (Il. 2009).

misrepresentations. Therefore, when a lawyer endorses another lawyer on social media, the endorsing lawyer must only make endorsements about skills that he knows to be true.

9. Attorneys May Review a Juror's Internet Presence

The use of social networking websites can also come into play when dealing with judges and juries. A lawyer may review a juror's social media presence but may not attempt to access the private portions of a juror's page.

Rule 3.5 states:

> A lawyer shall not:
> (a) seek to influence a judge, juror, prospective juror or other official by means prohibited by law;
> (b) communicate ex parte with such a person during the proceeding unless authorized to do so by law or court order;
> (c) communicate with a juror or prospective juror after discharge of the jury if:
> (1) the communication is prohibited by law or court order;
> (2) the juror has made known to the lawyer a desire not to communicate; or
> (3) the communication involves misrepresentation, coercion, duress of harassment; or
> (d) engage in conduct intended to disrupt a tribunal.

During jury selection and trial, an attorney may access the public portion of a juror's social networking website but may not attempt or request to access the private portions of the website. Requesting access to the private portions of a juror's social networking website would constitute an ex parte communication, which is expressly prohibited by Rule 3.5(b).

Rule 3.5(a) prohibits a lawyer from attempting to influence a juror or potential juror. Additionally, Rule 3.5(b) prohibits *ex parte* communications with those persons. Accessing the public portions of a juror's social media profile is ethical under the Rules as discussed in other portions of this Opinion. However, any attempts to gain additional access to private portions of a juror's social networking site would constitute an ex parte communication. Therefore, a lawyer, or a lawyer's agent, may not request access to the private portions of a juror's social networking site.

American Bar Association Standing Committee on Ethics and Professional Responsibility Formal Opinion 466 concluded that a lawyer may view the public portion of the social networking profile of a juror or potential juror but may not communicate directly with the juror or jury panel member. The Committee determined that a lawyer, or his agent, is not permitted to request access to the private portion of a juror's or potential juror's social networking website because that type of *ex parte* communication would violate Model Rule 3.5(b). There is no *ex parte* communication if the social networking website independently notifies users when the page has been viewed. Additionally, a lawyer may be required to notify the court of any evidence of juror misconduct discovered on a social networking website.

This Committee agrees with the guidance provided in ABA Formal Opinion 466, which is consistent with Rule 3.5's prohibition regarding attempts to influence jurors, and *ex parte* communications with jurors.

10. Attorneys May Ethically Connect with Judges on Social Networking Websites Provided the Purpose is not to Influence the Judge

A lawyer may not ethically connect with a judge on social media if the lawyer intends to influence the judge in the performance of his or her official duties. In addition, although the Rules do not prohibit such conduct, the Committee cautions attorneys that connecting with judges may create an appearance of bias or partiality.[32]

Various Rules address this concern. For example, Rule 8.2 states:

> (a) A lawyer shall not make a statement that the lawyer knows to be false or with reckless disregard as to its truth or falsity concerning the qualifications or integrity of a judge, adjudicatory officer or public legal officer, or of a candidate for election or appointment to judicial or legal office.

In addition, Comment [4] to Canon 2.9 of the Code of Judicial Conduct, effective July 1, 2014, states that "A judge shall avoid comments and interactions that may be interpreted as *ex parte* communications concerning pending matters or matters that may appear before the court, including a judge who participates in electronic social media." Thus, the Supreme Court has implicitly agreed that judges may participate in social media, but must do so with care.

Based upon this statement, this Committee believes that attorneys may connect with judges on social media websites provided the purpose is not to influence the judge, and reasonable efforts are taken to assure that there is no ex parte or other prohibited communication. This conclusion is consistent with Rule 3.5(a), which forbids a lawyer to "seek to influence a judge" in an unlawful way.

IV. Conclusion

Social media is a constantly changing area of technology that lawyers keep abreast of in order to remain competent. As a general rule, any conduct that would not be permissible using other forms of communication would also not be permissible using social media. Any use of a social networking website to further a lawyer's business purpose will be subject to the Rules of Professional Conduct.

Accordingly, this Committee concludes that any information an attorney or law firm places on a social networking website must not reveal confidential client information absent the client's consent. Competent attorneys should also be aware that their clients use social media and that what clients reveal on social media can be used in the course of a dispute. Finally, attorneys are permitted to use social media to research jurors and may connect with judges so long as they do not attempt to

[32] American Bar Association Standing Committee on Ethics and Professional Responsibility Formal Opinion 462 concluded that a judge may participate in electronic social networking, but as with all social relationships and contacts, a judge must comply with the relevant provisions of the Code of Judicial Conduct and avoid any conduct that would undermine the judge's independence, integrity, or impartiality, or create an appearance of impropriety.

influence the outcome of a case or otherwise cause the judge to violate the governing Code of Judicial Conduct.

Social media presents a myriad of ethical issues for attorneys, and attorneys should continually update their knowledge of how social media impacts their practice in order to demonstrate competence and to be able to represent their clients effectively.

ATTACHMENT 5

295 Ga. 217
FINAL COPY

S14Y0661. IN THE MATTER OF MARGRETT A. SKINNER.

PER CURIAM.

The State Bar of Georgia made a formal complaint against respondent Margrett A. Skinner (State Bar No. 650748), alleging violations of Rules 1.3, 1.4, 1.6, and 1.16 of the Georgia Rules of Professional Conduct. Prior to an evidentiary hearing on the formal complaint, Skinner filed a petition for voluntary discipline, admitting that she violated Rule 1.6 by improperly disclosing confidential information about a former client, and in which she agreed to accept a Review Panel reprimand for the violation. The special master and the State Bar recommended that we accept the petition for voluntary discipline. We rejected the petition, however, noting that a Review Panel reprimand is "the mildest form of public discipline authorized . . . for the violation of Rule 1.6," In the Matter of Skinner, 292 Ga. 640, 642 (740 SE2d 171) (2013), and noting as well that the petition and accompanying record did not "reflect the nature of the disclosures (except that they concern [unspecified] personal and confidential information) or the actual or potential harm to the

client as a result of the disclosures." Id. at 642, n. 6. Following our rejection of the petition, the special master conducted an evidentiary hearing, and he made his report and recommendation on December 18, 2013, in which he found that Skinner violated Rules 1.4 and 1.6 but not Rules 1.3 and 1.16.[1] Neither party sought review of the report by the Review Panel, and the matter is again before this Court for decision.

In his report, the special master found that a client retained Skinner in July 2009 to represent her in an uncontested divorce, and she paid Skinner $900, including $150 for the filing fee. For six weeks, the client did not hear anything from Skinner, and after multiple attempts to contact Skinner, the client finally was able to reach Skinner again in October 2009. At that point, Skinner informed the client that Skinner had lost the paperwork that the client had given to Skinner in July. Skinner and the client then met again, and Skinner finally began to draft pleadings for the divorce. The initial drafts of the pleadings had multiple errors, and Skinner and the client exchanged several drafts and communicated by e-mail about the status of the case in October and early

[1] Joseph A. Boone was appointed as special master in this matter.

November 2009. Those communications concluded by mid-November, and Skinner and the client had no more communications until March 18, 2010, when the client reported to Skinner that her husband would not sign the divorce papers without changes. In April 2010, both the client and her husband signed the papers.

A disagreement developed about the fees and expenses of the divorce. Skinner asked the client for an additional $185 for certain travel expenses and the filing fee. In April and early May 2010, Skinner and the client exchanged several e-mails about the request for additional money. Then, on May 18, the client informed Skinner that she had hired another lawyer to complete her divorce, and she asked Skinner to deliver her file to new counsel and to refund $750. Skinner replied that she would not release the file unless she were paid. Although Skinner eventually refunded $650 to the client, Skinner never delivered the file to new counsel, contending that it only contained her "work product." New counsel completed the divorce within three months of her engagement.

Around this time, the client posted negative reviews of Skinner on three consumer Internet pages. When Skinner learned of the negative reviews, she

posted a response on the Internet, a response that contained personal and confidential information about her former client that Skinner had obtained in the course of her representation of the client. In particular, Skinner identified the client by name, identified the employer of the client, stated how much the client had paid Skinner, identified the county in which the divorce had been filed, and stated that the client had a boyfriend. The client filed a grievance against Skinner, and in response to the grievance, Skinner said in August 2011 that she would remove her posting from the Internet. It was not removed, however, until February 2012.

The special master found that Skinner violated Rule 1.4 when she failed between July and October 2010 to keep her client reasonably informed of the status of the divorce, and the special master found that Skinner violated Rule 1.6 when she disclosed confidential information about her client on the Internet. The special master found no violation of Rules 1.3 and 1.16.[2] Turning to the

[2] About Rule 1.16, the special master reported his belief that Skinner technically violated the rule by failing to deliver the file of her client to successor counsel based on a mistaken belief that signed pleadings in the file belonged to her as "work product." See Formal Advisory Opinion 87-5; Swift, Currie, McGhee & Hiers v. Henry, 276 Ga. 571 (581 SE2d 37) (2003). But the special master did not actually find a violation nor recommend any discipline under Rule 1.16. The special master reported that he made no such finding or recommendation because there was no clear and convincing evidence of prejudice, insofar

appropriate discipline for these violations, the special master noted that Skinner had substantial experience as a practicing lawyer — she was admitted to the Bar in 1987 — which is an aggravating circumstance. The special master also found, however, a number of mitigating circumstances, including that Skinner had no prior discipline, the absence of a dishonest or selfish motive for her improper conduct, that she refunded a substantial portion of her fee to the client even after doing work for the client, that she accepted responsibility for her misconduct by filing a petition for voluntary discipline, that she otherwise was cooperative in the disciplinary proceedings, and that she had expressed remorse for her misconduct. In addition, the special master found as mitigation that Skinner experienced a number of personal problems during her representation of the client and the subsequent time that she posted the confidential information about her client on the Internet, including colon surgery in April 2010, the diagnosis of both her mother and father with cancer (she was their primary caregiver), and the death of her father. For both violations, the special master recommended a public reprimand, with the additional condition that Skinner "be instructed to

---

as the client already had the documents contained in the file. As to the retention of unearned fees, the special master found the issue moot in light of the refund of $650 to the client.

take advantage of the State Bar's Law Practice Management services and recommendations with respect to internal office procedures, client files, and case tracking procedures."

We have reviewed carefully the record and the very detailed report of the special master, and we agree with his recommendation of a public reprimand, as well as the additional condition that Skinner be instructed to take advantage of the State Bar's Law Practice Management services and recommendations with respect to internal office procedures, client files and case tracking procedures. See In the Matter of Adams, 291 Ga. 173 (729 SE2d 313) (2012). Although other jurisdictions occasionally have disciplined lawyers more severely for improper disclosures of client confidences, we note that those cases involved numerous clients and violations of other rules, see Office of Lawyer Regulation v. Peshek, 334 Wis.2d 373 (798 NW2d 879 (2011) (60-day suspension), or the disclosure of especially sensitive information that posed serious harm or potential harm to the client, see In re Quillinan, 20 DB Rptr. 288 (Ore. Disp. Bd. 2006) (90-day suspension), available at www.osbar.org/_docs/dbreport/dbr20.pdf. In this case, the improper disclosure of confidential information was isolated and limited to a single client, it does not

appear that the information worked or threatened substantial harm to the interests of the client, and there are significant mitigating circumstances. Accordingly, we hereby order that Skinner receive a public reprimand in accordance with Bar Rules 4-102 (b) (3) and 4-220 (c), and we order that she consult with the Law Practice Management Program of the State Bar as set forth above and implement its suggestions in her law practice.

Public reprimand. All the Justices concur.

Decided May 19, 2014.

Public reprimand.

Paula J. Frederick, General Counsel State Bar, Jenny K. Mittelman, Assistant General Counsel State Bar, for State Bar of Georgia.

William H. Noland, for Skinner.

ATTACHMENT 6

ABA Annotations Concerning Lawyer Responsive Disclosures Under Model Rule 1.6

"A lawyer accused of wrongful conduct in connection with the representation of a client, or with complicity in a client's wrongful conduct, need not wait until formal charges are filed. "The lawyer's right to respond arises when an assertion of such complicity has been made. . . . [T]he defense may be established by responding directly to a third party who has made such an assertion." Model Rule 1.6, cmt. [10]; see, e.g., In re Bryan, 61 P.3d 641 (Kan. 2003) (formal proceedings not required before disclosure in self-defense could be made under Rule 1.6(b)); Pa. Ethics Op. 96-48 (1996) (lawyer whose former clients defended against SEC fraud complaint by alleging lawyer's lack of due diligence may discuss matter with SEC even though lawyer not named in complaint); S.C. Ethics Op. 94-23 (1994) (lawyer under investigation by Social Security Administration regarding handling of client's disability claim may disclose client information to defend himself even though no formal grievance proceeding pending). **Mere criticism of the lawyer, however, may be insufficient to warrant disclosures in self defense, even when the criticisms appear in the press.** See, e.g., Louima v. City of N.Y., No. 98 CV 5083(SJ), 2004 WL 2359943 (E.D.N.Y. Oct. 5, 2004) ("mere press reports" about lawyer's conduct do not justify disclosure of client information even if report is false and accusations unfounded); N.Y. County Ethics Op. 711 (1997) (client's criticism of lawyer to neighbor was mere gossip and did not trigger exception to confidentiality rule); Utah Ethics Op. 05-01 (2005) (criminal defense lawyer may not voluntarily disclose client confidences to prosecutor or to court in response to claim that lawyer's prior advice was confusing; no "controversy" between lawyer and client). But see Ariz. Ethics Op. 93-02 (1993) (interpreting "controversy" to include disagreement in public media)."

ABA Annotated Model Rules at pp. 109-110 (2011).

The New York State Bar Association has now joined those prohibiting rejoinder, though its rule has some different language than Georgia's. NYSBA Ethics Opinion 1032 (October 30, 2014).

ATTACHMENT 7

SECOND DIVISION
BARNES, P. J.,
MILLER, and RAY, JJ.

March 12, 2014

In the Court of Appeals of Georgia

A13A2432. PAMPATTIWAR v. HINSON et al.

BARNES, Presiding Judge.

Vivek A. Pampattiwar hired Jan V. Hinson, Esq., and her law firm, Jan V. Hinson, P.C. (collectively, "Hinson") to file a divorce action on his behalf. Hinson ultimately terminated the representation and brought this action against Pampattiwar, alleging, among other things, that Pampattiwar had committed fraud by intentionally misleading Hinson during his initial consultation with her, and had published statements about her and her firm on the Internet that were libelous and placed her in a false light. Pampattiwar filed a motion to dismiss for failure to state a claim for fraud, which the trial court denied. The case proceeded to trial, and the jury returned a verdict in favor of Hinson on her claims for fraud, libel per se, and false light invasion of privacy. Pampattiwar filed motions for judgment notwithstanding the verdict and for new trial, which the trial court denied. Pampattiwar now appeals,

challenging the trial court's denial of his motions. For the reasons discussed below, we affirm.

"When we review the denial of a motion for new trial or judgment notwithstanding the verdict, we must affirm the denial if there is any evidence to support the verdict." *Wellons, Inc. v. Langboard, Inc.*, 315 Ga. App. 183, 187 (2) (726 SE2d 673) (2012). In making this determination, we construe the evidence and every inference arising therefrom in the light most favorable to the prevailing party. *Fletcher v. C.W. Matthews Contracting Co.*, 322 Ga. App. 751 (746 SE2d 230) (2013). "The determinative question is not whether the verdict and the judgment of the trial were merely authorized, but . . . whether a contrary judgment was demanded." (Citation and punctuation omitted.) *Wright v. Apartment Inv. & Mgmt. Co.*, 315 Ga. App. 587, 588 (726 SE2d 779) (2012).

Viewed in this manner, the evidence adduced at trial showed that on July 2, 2010, Pampattiwar met for an initial consultation with Hinson about filing for a divorce. Pampattiwar told Hinson that he was currently represented by other counsel and that he had filed a separate maintenance action against his wife in Fulton County

because both of them had lived there at the time the action was filed.[1] Although the separate maintenance action remained pending, Pampattiwar told Hinson that he now desired a divorce and that both he and his wife currently resided in Gwinnett County. Pampattiwar wanted Hinson to take over the representation of his case and file a petition for divorce on his behalf. He did not inform Hinson that she would be the sixth attorney to represent him in the litigation with his wife.

During the initial consultation, Hinson repeatedly asked Pampattiwar if his wife had filed a counterclaim for divorce in the separate maintenance action. Pampattiwar insisted that a divorce counterclaim had not been filed and invited Hinson to check the online Fulton County docket. Hinson then checked the docket while Pampattiwar watched, and the docket reflected that no divorce counterclaim had been filed. Pampattiwar had documents with him relating to the Fulton County case, but Hinson did not review them as part of the initial consultation.

---

[1] "Although an action for separate maintenance and an action for divorce both grow out of the marriage relationship and relate to the same subject matter, they have different purposes and raise different questions." *Southworth v. Southworth*, 265 Ga. 671, 673 (3) (461 SE2d 215) (1995). An action for separate maintenance is authorized "[w]hen spouses are living separately or in a bona fide state of separation and there is no action for divorce pending." OCGA § 19-6-10.

Hinson advised Pampattiwar that venue for the divorce would be in Gwinnett County given that both parties now lived there and that the filing of a divorce petition would abate the separate maintenance action. Hinson told Pampattiwar that she was willing to represent him in the divorce in Gwinnett County, but not in the separate maintenance action pending in Fulton County in which he already had retained counsel. Pampattiwar agreed to this arrangement, and Hinson subsequently filed a petition for divorce on his behalf in Gwinnett County.

Almost immediately after filing the divorce petition in Gwinnett County, Hinson received what she characterized as a "scathing" response from opposing counsel informing her that Pampattiwar's wife had in fact filed a counterclaim for divorce in the separate maintenance action almost a year earlier. Hinson confronted Pampattiwar, who assured her that he had not known about the divorce counterclaim or the error on the Fulton County docket. Pampattiwar also told Hinson that the attorney who had been representing him in the Fulton County case had now withdrawn and he was currently unrepresented. Believing that Pampattiwar had simply been confused about the filing of the counterclaim, Hinson agreed to represent him in the divorce proceedings in Fulton County.

After entering an appearance in the Fulton County action, Hinson obtained a copy of Pampattiwar's deposition that had been taken earlier in that case. It was clear from the deposition transcript that Pampattiwar knew that his wife had counterclaimed for divorce. Hinson confronted Pampattiwar with the deposition transcript and accused him of knowing about the counterclaim in their initial consultation. She accused him of "playing fast and loose with [her] bar license" and of "making a fool out of [her] in the courts in which [she] practice[d]" by having her file a divorce petition in Gwinnett County when one was already pending in Fulton County. Pampattiwar responded, "You can't get out now. We're on a trial calendar."

In light of the divorce counterclaim pending in Fulton County, Hinson advised Pampattiwar that the divorce petition filed in Gwinnett County was improper and would need to be voluntarily dismissed. Pampattiwar responded that he did not want to dismiss the Gwinnett County action and instead wanted to "take [his] chances" in Gwinnett and was "willing to pay extra for that." However, Hinson insisted that Pampattiwar agree to the dismissal or she would seek to withdraw from representing him. Pampattiwar then signed a dismissal drafted by Hinson, but he returned to her office after she left for lunch and took the document with him so that she could not file it. After another confrontation, Pampattiwar signed a new dismissal drafted by

Hinson, which she was able to file successfully. The divorce petition filed in Gwinnett County ultimately was dismissed while the divorce case proceeded in Fulton County.

Over the ensuing months, Hinson and Pampattiwar had multiple heated confrontations over billing issues and other matters relating to the Fulton County divorce case. Hinson moved to withdraw from representing Pampattiwar, but the trial court denied her motion. Hinson later filed a motion for reconsideration, which the trial court granted on the eve of arbitration that had been scheduled between Pampattiwar and his wife. However, Pampattiwar pleaded with Hinson to represent him in the arbitration that was set to commence in three days, and she acquiesced to his request.

Hinson ended her representation of Pampattiwar on September 15, 2010 after the arbitration. In October 2010, Pampattiwar contacted Hinson's law firm because he was upset over his legal bills. Pampattiwar spoke with a paralegal at the firm and accused Hinson and her staff of being "crooks" and claimed that they had "duped" him.

In November 2010, Hinson became concerned because "the phones just stopped ringing" in her office. One of Hinson's assistants "Googled" Hinson's name

on the Internet and discovered a review of her law firm that had recently been posted on the website Kudzu.com under the screen name "STAREA." The reviewer described Hinson as "a CROOK Lawyer" and an "Extremely Fraudulent Lady." The reviewer claimed that Hinson "inflates her bills by 10 times" and had "duped 12 people i[n] the last couple of years." Further investigation revealed that the Internet protocol ("IP") address used for the STAREA review matched the IP address used by Pampattiwar in several emails that he had sent to Hinson.

Hinson subsequently filed the instant action against Pampattiwar, alleging, among other things, that he had published statements about her and her firm on Kudzu.com that constituted libel per se. Hinson also alleged that Pampattiwar had committed fraud during his initial consultation with her by falsely representing that no divorce counterclaim had been filed in the Fulton County case and by encouraging her to confirm this fact on the online docket, even though Pampattiwar knew that his wife had filed a counterclaim and that the docket was inaccurate. Hinson further alleged that she detrimentally relied on Pampattiwar's misrepresentation about the counterclaim by improperly filing a petition for divorce on his behalf in Gwinnett County, leading her to suffer professional embarrassment and humiliation.

After Hinson filed her lawsuit, an additional review was posted on Kudzu.com under the screen name "REALPOLICE." The reviewer warned viewers not to "trust" positive reviews appearing for Hinson on Kudzu.com because she "asks her office staff to post bogus reviews every where on the [I]nternet." Further investigation revealed that the Kudzu.com user accounts for STAREA and REALPOLICE had the same password, "pampa012." As with the STAREA review, the IP address used for the REALPOLICE review matched the IP address used by Pampattiwar in his emails with Hinson. After the posting of the REALPOLICE review, Hinson amended her complaint to include a claim for false light invasion of privacy.

Pampattiwar filed a motion to dismiss Hinson's fraud claim for failure to state a claim upon which relief could be granted, and the trial court denied the motion. The case proceeded to trial, where Hinson testified to the events as set out above. Hinson called several additional witnesses, including an information technology ("IT") communications expert who traced the source of the two Kudzu.com reviews to the IP address associated with Pampattiwar. On her claims for fraud, libel per se, and false light invasion of privacy, Hinson did not assert that she suffered any pecuniary

loss from the misrepresentations and instead sought damages for "wounded feelings" under OCGA § 51-12-6.[2]

Pampattiwar moved for a directed verdict on several of Hinson's claims, which the trial court denied. During the defense's case-in-chief, Pampattiwar testified that he had been aware that his wife had filed a counterclaim for divorce in the separate maintenance action in Fulton County when he met for his initial consultation with Hinson. But Pampattiwar claimed that he told Hinson about the counterclaim and showed her pleadings from the Fulton County case during the initial consultation. Pampattiwar also denied posting the two reviews on Kudzu.com.

After hearing all of the evidence, the jury found in favor of Hinson and, among other things, awarded her damages for fraud, libel per se, and false light invasion of privacy using a special verdict form. Pampattiwar filed motions for judgment notwithstanding the verdict and for new trial, which the trial court denied. This appeal followed.

---

[2] OCGA § 51-12-6, entitled "Damages for injury to peace, happiness, or feelings," provides in relevant part: "In a tort action in which the entire injury is to the peace, happiness, or feelings of the plaintiff, no measure of damages can be prescribed except the enlightened consciences of impartial jurors."

1. Pampattiwar contends that the trial court erred in denying his motion for judgment notwithstanding the verdict on Hinson's claim for fraud predicated on his alleged misrepresentation about the divorce counterclaim because Hinson failed to prove justifiable reliance. Hinson testified that she checked the online docket in the Fulton County action to confirm Pampattiwar's statement that no divorce counterclaim had been filed in that action, but Pampattiwar contends that checking the docket was insufficient due diligence on her part. According to Pampattiwar, Hinson should have investigated further into what claims were being asserted in the Fulton County action before she filed the divorce petition in Gwinnett County, such as by reviewing the documents from the Fulton County action that Pampattiwar brought with him to the initial consultation. We are unpersuaded that the evidence *demanded* a finding in favor of Pampattiwar on the issue of reasonable reliance.

"One of the essential elements of an action for fraud is justifiable reliance by the plaintiff." (Citation and punctuation omitted.) *Bithoney v. Fulton-DeKalb Hosp. Auth.*, 313 Ga. App. 335, 344 (2), n. 23 (721 SE2d 577) (2011). "Blind reliance precludes a fraud claim as a matter of law." *Baxter v. Fairfield Fin. Svcs.*, 307 Ga. App. 286, 294-295 (4) (704 SE2d 423) (2010). But

> [w]hile a party must exercise reasonable diligence to protect himself against the fraud of another, he is not bound to exhaust all means at his command to ascertain the truth before relying upon the representations. Ordinarily the question whether the complaining party could have ascertained the falsity of the representations by proper diligence is for determination by the jury.

Elliott v. Marshall, 179 Ga. 639, 640 (176 SE 70) (1934). See *Morgan v. Morgan*, 193 Ga. App. 302, 304-305 (5) (388 SE2d 2) (1989); *Adkins v. Lee*, 127 Ga. App. 261, 264 (4) (193 SE2d 252) (1972).

In the present case, Hinson testified that she had practiced domestic law for 16 years and had performed civil case searches on the online Fulton County docket for "hundreds" of cases. Hinson testified that based on her experience, the online docket normally would reflect that a divorce counterclaim had been filed in a domestic case in the pleadings index and in the description of the case type. According to Hinson, she relied on the online docket as confirmation of what Pampattiwar had told her about the Fulton County case because the docket "always" listed "answer and counterclaim" in the pleadings index and listed "divorce" as the case type if a divorce counterclaim had been filed, but here the docket listed the responsive pleading simply as "answer" and the case type as "separate maintenance action." Hinson further

testified that she declined to review the documents from the Fulton County case that Pampattiwar brought with him to the initial consultation because Pampattiwar already had counsel representing him in that case and she did not want to become involved in the separate maintenance action, which she had believed would be dismissed upon the filing of the divorce petition in Gwinnett County. Hinson also noted that while clients in domestic cases are stressed and sometimes are forgetful, they do not usually forget that they are "going through a divorce," and she does not "typically assume that a client is lying" to her about such a basic fact.

In light of this testimony, it was for the jury to determine whether Hinson exercised sufficient due diligence by checking the online docket to confirm Pampattiwar's statement that his wife had not filed a counterclaim for divorce in the Fulton County case. "Justifiable reliance generally is a question for the jury, and jury resolution [was] necessary here." *Catrett v. Landmark Dodge, Inc.*, 253 Ga. App. 639, 641 (1) (560 SE2d 101) (2002). The trial court therefore did not err in denying Pampattiwar's motion for judgment notwithstanding the verdict on Hinson's fraud claim. See *Johnson v. GAPVT Motors, Inc.*, 292 Ga. App. 79, 83 (1) (663 SE2d 779) (2008) (although the evidence would have "*authorized*" the jury to find that plaintiff should have discovered the alleged misrepresentation, "this conclusion was not

demanded by the evidence") (emphasis in original). See also *Catrett*, 253 Ga. App. at 641 (1) (whether plaintiff reasonably relied upon defendant's misrepresentation that the car was "new" should be submitted to the jury, where plaintiff relied upon documents reflecting that the car was "new," but there were other documents available that referred to the car as "used"); *Parks v. Howard*, 197 Ga. App. 405, 407-408 (4) (398 SE2d 308) (1990) (whether plaintiff exercised due diligence by relying upon the inspection report presented by defendant, or whether plaintiff should have obtained an independent inspection report, was for the jury to resolve).

Pampattiwar's reliance upon *Isbell v. Credit Nation Lending Svc., LLC*, 319 Ga. App. 19, 25-26 (2) (b) (735 SE2d 46) (2012), is unpersuasive. In *Isbell*, the buyers of a used truck asserted fraud claims against the seller and the seller's financier, contending that the condition of the truck had been misrepresented to them. Id. at 19-21. The uncontroverted evidence showed that the buyers failed to obtain a vehicle history report or have their own mechanic inspect the truck even though they "were specifically warned that the vehicle may have a bent frame" and were offered an opportunity to have the truck inspected. Id. at 26 (2) (b). Consequently, we concluded that, as a matter of law, the buyers had failed to exercise due diligence to discover that the used truck had suffered frame damage in a prior automobile

accident. Id. We reasoned that the buyers' "blind reliance on the salesman's representations when the means of knowledge were at hand show[ed] an unjustified lack of due diligence." (Citation and punctuation omitted.) Id.

Relying on *Isbell*, Pampattiwar argues that Hinson ignored the documents from the Fulton County case that he brought with him to the initial consultation and thus blindly relied on his representation that there was no divorce counterclaim "when the means of knowledge were at hand." Notably, however, the plaintiff buyers in *Isbell* were put on notice that there might be a defect in the used truck that they were purchasing, but nevertheless failed to take additional steps to determine if a defect existed that were readily available to them. See *Isbell*, 319 Ga. App. at 26 (2) (b). But Hinson was never put on notice that a divorce counterclaim might have been filed in the Fulton Case; to the contrary, the online docket reviewed by Hinson reflected that no such counterclaim had been filed and thus appeared to confirm Pampattiwar's representation to her. Hence, unlike in *Isbell*, this is not a case of "blind reliance." Under these circumstances, it was for the jury to resolve whether Hinson should have

reviewed the documents that Pampattiwar brought to the initial consultation before filing the divorce petition in Gwinnett County.[3]

2. Pampattiwar also contends that the trial court erred in denying his motion for new trial on Hinson's fraud claim because she failed to show "actual damages" resulting from the alleged misrepresentation about the divorce counterclaim. Hinson did not allege that she suffered any pecuniary losses from improperly filing the divorce petition in Gwinnett County in reliance on Pampattiwar's misrepresentation about the counterclaim. Rather, Hinson alleged that the entire injury she suffered from the misfiling of the divorce petition was to her peace, happiness, and feelings and sought damages pursuant to OCGA § 51-12-6. According to Pampattiwar, damages for "wounded feelings" under OCGA § 51-12-6 are not "actual damages" and thus could not be recovered by Hinson for her fraud claim. We disagree.

---

[3] Pampattiwar separately contends that the trial court erred in denying his motion to dismiss Hinson's fraud claim for failure to state a claim upon which relief could be granted. In moving to dismiss the fraud claim, Pampattiwar argued that the element of reasonable reliance had not been pled with sufficient particularity in Hinson's complaint. See OCGA § 9-11-9 (b). "However, the proper remedy for seeking more particularity is by motion for a more definite statement at the pleading stage or by the rules of discovery thereafter." (Citation and punctuation omitted.) *Odom v. Hughes*, 293 Ga. 447, 455 (3), n. 6 (748 SE2d 839) (2013). Accordingly, the trial court committed no error in denying Pampattiwar's motion to dismiss. See id.; *Miller v. Lomax*, 266 Ga. App. 93, 98 (2) (b) (596 SE2d 232) (2004).

As we have recently reiterated,

> In order to recover for fraud, a plaintiff must prove that actual damages, not simply nominal damages, flowed from the fraud alleged. The expression "actual damages" is not necessarily limited to pecuniary loss, or loss of ability to earn money. General damages are those which the law presumes to flow from any tortious act, and they may be awarded on a fraud claim. Wounding a man's feelings is as much *actual damage* as breaking his limbs. Injury to reputation is a personal injury, and personal injury damages can be recovered in a fraud action.

(Emphasis in original.) *Kelley v. Cooper*, __ Ga. App. __ (4) (c) (Case No. A13A0982, decided Nov. 22, 2013), quoting *Zieve v. Hairston*, 266 Ga. App. 753, 759 (2) (c) (598 SE2d 25) (2004). See also *Johnson*, 292 Ga. App. at 83 (1). Thus, we have held that recovery for "wounded feelings" under OCGA § 51-12-6 is permitted for fraudulent misrepresentation where, as here, the plaintiff claims that the entire injury she suffered from the misrepresentation was to her peace, happiness, or feelings. See *Mallard v. Jenkins*, 186 Ga. App. 167, 168 (1) (366 SE2d 775) (1988). Compare *Kent v. White*, 238 Ga. App. 792, 794 (1) (c) (520 SE2d 481) (1999) (plaintiff could not recover damages under OCGA § 51-12-6 for fraud because "at no point did [the plaintiff] claim that the entire injury to him was to his peace, happiness, or feelings"). It follows that the trial court did not err in determining that Hinson

could recover damages under OCGA § 51-12-6 on her fraud claim and in denying Pampattiwar's motion for new trial.

3. As with Hinson's fraud claim, Pampattiwar contends that the trial court erred in denying his motion for new trial on Hinson's claim for libel per se because Hinson could not recover "wounded feelings" damages under OCGA § 51-12-6 for the alleged defamatory statements. In this regard, Pampattiwar notes that the trial court ruled before trial that Hinson could not recover punitive damages on her libel claim because she never made a written request for correction or retraction of the defamatory statements before filing her complaint. See OCGA § 51-5-11; *Mathis v. Cannon*, 276 Ga. 16, 28 (4) (573 SE2d 376) (2002). In light of the failure to request retraction, Pampattiwar argues that OCGA § 51-12-6 damages could not be recovered on Hinson's libel claim because the damages awarded under that statute are in part punitive. We again disagree.

It is true that before the passage of the Tort Reform Act of 1987 (the "Act"), Ga. L. 1987, p. 915, § 6, "wounded feelings" damages awarded under OCGA § 51-12-6 were in part punitive because the statute authorized the jury to consider "circumstances relevant to deterrence of the wrongdoer." *Westview Cemetary v.*

Blanchard, 234 Ga. 540, 546 (2) (B) (216 SE2d 776) (1975). Specifically, the pre-1987 version of OCGA § 51-12-6 stated:

> In a tort action in which the entire injury is to the peace, happiness, or feelings of the plaintiff, no measure of damages can be prescribed except the enlightened consciences of impartial jurors. In such a case, the *worldly circumstances of the parties, the amount of bad faith in the transaction*, and all the attendant facts should be weighed; and the verdict of the jury should not be disturbed unless the court suspects bias or prejudice from its excess or its inadequacy.

(Emphasis supplied.) Because the statute allowed for consideration of all the attendant circumstances, including the "worldly circumstances of the parties" and any "bad faith in the transaction," "the jury [was] not restricted to consideration of circumstances relevant to compensation (i.e., the extent of the injury) but [was] entitled to consider as well circumstances relevant to deterrence (i.e., any aggravated aspects of the defendant's misconduct plus the defendant's 'worldly circumstances')." *Westview Cemetary*, 234 Ga. at 545 (2) (B). As such, damages under the pre-1987 version of OCGA § 51-12-6 were, "at least in part, punitive damages." Id.

However, the 1987 Act significantly revised OCGA § 51-12-6, as our Supreme Court recently explained:

> In the Act, the General Assembly . . . enacted the current version of OCGA § 51-12-6, and deleted from the pre-1987 statute the language: "the worldly circumstances of the parties, the amount of bad faith in the transaction, and all the attendant facts should be weighed." In its place, the legislature inserted the text: "In such an action, punitive damages under Code Section 51-12-5 or Code Section 51-12-5.1 shall not be awarded." And, the General Assembly specifically encompassed within the term "punitive damages" those damages that might be "awarded . . . in order to . . . deter a defendant." OCGA § 51-12-5.1 (a). Thus, the General Assembly eliminated from OCGA § 51-12-6 the language that was intended to deter misconduct . . . .

Holland v. Caviness, 292 Ga. 332, 334-335 (737 SE2d 669) (2013). Given the elimination of the statutory language aimed at deterrence, the current version of OCGA § 51-12-6, applicable in the present case, does not contain "a punitive award provision." Id. at 335, n.8. Consequently, Pampattiwar's argument that OCGA § 51-12-6 damages could not be recovered for Hinson's libel claim because of the failure to request retraction is misplaced because it is predicated on an obsolete version of the statute.

We are cognizant that the trial court charged the jury on OCGA § 51-12-6 damages using language from the Georgia pattern jury instructions, which still includes reference to the "worldly circumstances of the parties" and "the amount of

bad faith in the transaction" even though that language was deleted from the statute in 1987. See Suggested Pattern Jury Instructions, Vol. I: Civil Cases, § 66.600. Our Supreme Court has noted that "the jury should no longer be instructed using that language." See *Holland*, 292 Ga. at 333, n. 3. Notably, however, in his reply brief, Pampattiwar concedes that he did not properly object to the charge at trial and expressly states that he is not claiming that the giving of the charge constituted "a substantial error . . . which was harmful as a matter of law" even absent objection. OCGA § 5-5-24 (c). Pampattiwar emphasizes that "he does not challenge any charge" on appeal and instead argues more broadly that "section 51-12-6 damages inherently incorporate punitive damages" and thus could not be awarded in this case as a matter of law in light of Hinson's failure to seek retraction. Under these circumstances, Pampattiwar has abandoned any possible challenge to the jury charge on OCGA § 51-12-6 damages, and his broader argument regarding OCGA § 51-12-6 and retraction fails for the reasons previously discussed. The trial court therefore committed no error in denying Pampattiwar's motion for new trial on the libel claim.

4. Lastly, Pampattiwar contends that the trial court erred in denying his motion for new trial on Hinson's claim for "false light" invasion of privacy. Pampattiwar argues that Hinson's false light claim was predicated on the second review on

Kudzu.com submitted under the screen name "REALPOLICE," and he contends that it was undisputed by the parties at trial that the review was flagged and rejected by Kudzu.com for violating its internal policy guidelines before the review was ever posted for the general public to see on the Internet. Given that the second review allegedly was never posted on the Internet, Pampattiwar asserts that Hinson failed to prove that the review was distributed to the public at large and thus could not establish the essential element of publicity as a matter of law. See *Williams v. Cobb County Farm Bureau*, 312 Ga. App. 350, 354 (2) (b) (718 SE2d 540) (2011); *Assn. Svcs., Inc. v. Smith*, 249 Ga. App. 629, 633-634 (4) (549 SE2d 454) (2001). We disagree.

Although Pampattiwar asserts that it was undisputed at trial that the second Kudzu.com review was never posted on the Internet, he cites to nothing in the record to support his assertion. And the record reflects that during closing argument, counsel for Hinson in fact argued that Pampattiwar twice posted reviews to the Internet:

> And this claim [of] putting this on the Internet not once, understand, not once but twice. Once wasn't good enough. He had to do it again. Each time she saw this, each time she was subjected to seeing this on Kudzu and then having to go to Kudzu and have them take it down . . . and then to see it pop back up again, you know, that caused injury to her peace, happiness, and feelings.

Thus, from the jury's perspective, the issue of whether the second Kudzu.com review was posted on the Internet was in dispute.

Furthermore, there was at least some evidence from which the jury could find that the second review was posted on the Internet. Business records from Kudzu.com were admitted at trial that included a screen shot of the second review and a notation that the review was "Posted: 4/19/2011." When asked what the date beside the word "Posted" field signified on these business records, the employee who handled site operations for Kudzu.com testified that it reflects "[t]he date the review was posted. Posted meaning you can view it on Kudzu.com" When all inferences are interpreted in the light most favorable to the verdict, the jury could have inferred from the Kudzu.com business records and the employee's testimony that the second review submitted under the user name "REALPOLICE" was posted to the Internet for the general public to see. Because there was evidence from which the jury could find that the element of publicity had been met, the trial court committed no error in denying Pampattiwar's motion for new trial on Hinson's claim for false light invasion of privacy.

Judgment affirmed. Miller, J. concurs. Ray, J., concurs in Divisions 1, 2, and 4, and concurs in the judgment only as to Division 3.

ATTACHMENT 8

PENNSYLVANIA BAR ASSOCIATION COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY

ETHICAL OBLIGATIONS FOR ATTORNEYS USING CLOUD COMPUTING/ SOFTWARE AS A SERVICE WHILE FULFILLING THE DUTIES OF CONFIDENTIALITY AND PRESERVATION OF CLIENT PROPERTY

FORMAL OPINION 2011-200

I. Introduction and Summary

If an attorney uses a Smartphone or an iPhone, or uses web-based electronic mail (e-mail) such as Gmail, Yahoo!, Hotmail or AOL Mail, or uses products such as Google Docs, Microsoft Office 365 or Dropbox, the attorney is using "cloud computing." While there are many technical ways to describe cloud computing, perhaps the best description is that cloud computing is merely "a fancy way of saying stuff's not on your computer."[1]

From a more technical perspective, "cloud computing" encompasses several similar types of services under different names and brands, including: web-based e-mail, online data storage, software-as-a-service ("SaaS"), platform-as-a-service ("PaaS"), infrastructure-as-a-service ("IaaS"), Amazon Elastic Cloud Compute ("Amazon EC2"), and Google Docs.

This opinion places all such software and services under the "cloud computing" label, as each raises essentially the same ethical issues. In particular, the central question posed by "cloud computing" may be summarized as follows:

> May an attorney ethically store confidential client material in "the cloud"?

In response to this question, this Committee concludes:

> Yes. An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all such materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.

****

In recent years, technological advances have occurred that have dramatically changed the way attorneys and law firms store, retrieve and access client information. Many law firms view these

[1] Quinn Norton, "Byte Rights," *Maximum PC*, September 2010, at 12.

technological advances as an opportunity to reduce costs, improve efficiency and provide better client service. Perhaps no area has seen greater changes than "cloud computing," which refers to software and related services that store information on a remote computer, *i.e.,* a computer or server that is not located at the law office's physical location. Rather, the information is stored on another company's server, or many servers, possibly all over the world, and the user's computer becomes just a way of accessing the information.[2]

The advent of "cloud computing," as well as the use of electronic devices such as cell phones that take advantage of cloud services, has raised serious questions concerning the manner in which lawyers and law firms handle client information, and has been the subject of numerous ethical inquiries in Pennsylvania and throughout the country. The American Bar Association Commission on Ethics 20/20 has suggested changes to the Model Rules of Professional Conduct designed to remind lawyers of the need to safeguard client confidentiality when engaging in "cloud computing."

Recent "cloud" data breaches from multiple companies, causing millions of dollars in penalties and consumer redress, have increased concerns about data security for cloud services. The Federal Trade Commission ("FTC") has received complaints that inadequate cloud security is placing consumer data at risk, and it is currently studying the security of "cloud computing" and the efficacy of increased regulation. Moreover, the Federal Bureau of Investigations ("FBI") warned law firms in 2010 that they were being specifically targeted by hackers who have designs on accessing the firms' databases.

This Committee has also considered the client confidentiality implications for electronic document transmission and storage in Formal Opinions 2009-100 ("Metadata") and 2010-200 ("Virtual Law Offices"), and an informal Opinion directly addressing "cloud computing." Because of the importance of "cloud computing" to attorneys – and the potential impact that this technological advance may have on the practice of law – this Committee believes that it is appropriate to issue this Formal Opinion to provide guidance to Pennsylvania attorneys concerning their ethical obligations when utilizing "cloud computing."

This Opinion also includes a section discussing the specific implications of web-based electronic mail (e-mail). With regard to web-based email, *i.e.,* products such as Gmail, AOL Mail, Yahoo! and Hotmail, the Committee concludes that attorneys may use e-mail but that, when circumstances require, attorneys must take additional precautions to assure the confidentiality of client information transmitted electronically.

II. Background

For lawyers, "cloud computing" may be desirable because it can provide costs savings and increased efficiency in handling voluminous data. Better still, cloud service is elastic, and users can have as much or as little of a service as they want at any given time. The service is sold on demand, typically by the minute, hour or other increment. Thus, for example, with "cloud computing," an attorney can simplify document management and control costs.

---

[2] *Id.*

The benefits of using "cloud computing" may include:

- Reduced infrastructure and management;
- Cost identification and effectiveness;
- Improved work production;
- Quick, efficient communication;
- Reduction in routine tasks, enabling staff to elevate work level;
- Constant service;
- Ease of use;
- Mobility;
- Immediate access to updates; and
- Possible enhanced security.

Because "cloud computing" refers to "offsite" storage of client data, much of the control over that data and its security is left with the service provider. Further, data may be stored in other jurisdictions that have different laws and procedures concerning access to or destruction of electronic data. Lawyers using cloud services must therefore be aware of potential risks and take appropriate precautions to prevent compromising client confidentiality, *i.e.*, attorneys must take great care to assure that any data stored offsite remains confidential and not accessible to anyone other than those persons authorized by their firms. They must also assure that the jurisdictions in which the data are physical stored do not have laws or rules that would permit a breach of confidentiality in violation of the Rules of Professional Conduct.

III. Discussion

A. Prior Pennsylvania Opinions

In Formal Opinion 2009-100, this Committee concluded that a transmitting attorney has a duty of reasonable care to remove unwanted metadata from electronic documents before sending them to an adverse or third party. Metadata is hidden information contained in an electronic document that is not ordinarily visible to the reader. The Committee also concluded, *inter alia*, that a receiving lawyer has a duty pursuant to RPC 4.4(b) to notify the transmitting lawyer if an inadvertent metadata disclosure occurs.

Formal Opinion 2010-200 advised that an attorney with a virtual law office "is under the same obligation to maintain client confidentiality as is the attorney in a traditional physical office." Virtual law offices generally are law offices that do not have traditional brick and mortar facilities. Instead, client communications and file access exist entirely online. This Committee also concluded that attorneys practicing in a virtual law office need not take additional precautions beyond those utilized by traditional law offices to ensure confidentiality, because virtual law firms and many brick-and-mortar firms use electronic filing systems and incur the same or similar risks endemic to accessing electronic files remotely.

Informal Opinion 2010-060 on "cloud computing" stated that an attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney makes reasonable efforts to protect confidential electronic communications and information. Reasonable efforts

discussed include regularly backing up data, installing firewalls, and avoiding inadvertent disclosures.

B. Pennsylvania Rules of Professional Conduct

An attorney using "cloud computing" is under the same obligation to maintain client confidentiality as is the attorney who uses offline documents management. While no Pennsylvania Rule of Profession Conduct specifically addresses "cloud computing," the following rules, *inter alia,* are implicated:

Rule 1.0 ("Terminology");
Rule 1.1 ("Competence");
Rule 1.4 ("Communication");
Rule 1.6 ("Confidentiality of Information");
Rule 1.15 ("Safekeeping Property"); and
Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistants").

Rule 1.1 ("Competence") states:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Comment [5] ("Thoroughness and Preparation") of Rule 1.1 provides further guidance about an attorney's obligations to clients that extend beyond legal skills:

> Competent handling of particular matter includes inquiry into and analysis of the factual and legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. ...

Competency is affected by the manner in which an attorney chooses to represent his or her client, or, as Comment [5] to Rule 1.1 succinctly puts it, an attorney's "methods and procedures." Part of a lawyer's responsibility of competency is to take reasonable steps to ensure that client data and information is maintained, organized and kept confidential when required. A lawyer has latitude in choosing how or where to store files and use software that may best accomplish these goals. However, it is important that he or she is aware that some methods, like "cloud computing," require suitable measures to protect confidential electronic communications and information. The risk of security breaches and even the complete loss of data in "cloud computing" is magnified because the security of any stored data is with the service provider. For example, in 2011, the syndicated children's show "Zodiac Island" lost an entire season's worth of episodes when a fired employee for the show's data hosting service accessed the show's content without authorization and wiped it out.[3]

---

[3] Eriq Gardner, "Hacker Erased a Season's Worth of 'Zodiac Island'," *Yahoo! TV* (March 31, 2011), available at http://tv.yahoo.com/news/article/tv-news.en.reuters.com/tv-news.en.reuters.com-20110331-us_zodiac

Rule 1.15 ("Safekeeping Property") requires that client property should be "appropriately safeguarded."[4] Client property generally includes files, information and documents, including those existing electronically. Appropriate safeguards will vary depending on the nature and sensitivity of the property. Rule 1.15 provides in relevant part:

> (b) A lawyer shall hold all Rule 1.15 Funds and property separate from the lawyer's own property. Such property shall be identified and appropriately safeguarded.

Rule 1.6 ("Confidentiality of Information") states in relevant part:

> (a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).
>
> (d) The duty not to reveal information relating to representation of a client continues after the client-lawyer relationship has terminated.

Comment [2] of Rule 1.6 explains the importance and some of the foundation underlying the confidential relationship that lawyers must afford to a client. It is vital for the promotion of trust, justice and social welfare that a client can reasonably believe that his or her personal information or information related to a case is kept private and protected. Comment [2] explains the nature of the confidential attorney-client relationship:

> A fundamental principle in the client-lawyer relationship is that, in the absence of the client's informed consent, the lawyer must not reveal information relating to the representation. See Rule 1.0(e) for the definition of informed consent. This contributes to the trust that is the hallmark of the client-lawyer relationship. The client is thereby encouraged to seek legal assistance and to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. ...

Also relevant is Rule 1.0(e) defining the requisite "Informed Consent":

> "Informed consent" denotes the consent by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.

Rule 1.4 directs a lawyer to promptly inform the client of any decision with respect to which the client's informed consent is required. While it is not necessary to communicate every minute

---

[4] In previous Opinions, this Committee has noted that the intent of Rule 1.15 does not extend to the entirety of client files, information and documents, including those existing electronically. In light of the expansion of technology as a basis for storing client data, it would appear that the strictures of diligence required of counsel under Rule 1.15 are, at a minimum, analogous to the "cloud."

detail of a client's representation, "adequate information" should be provided to the client so that the client understands the nature of the representation and "material risks" inherent in an attorney's methods. So for example, if an attorney intends to use "cloud computing" to manage a client's confidential information or data, it may be necessary, depending on the scope of representation and the sensitivity of the data involved, to inform the client of the nature of the attorney's use of "cloud computing" and the advantages as well as the risks endemic to online storage and transmission.

Absent a client's informed consent, as stated in Rule 1.6(a), confidential client information cannot be disclosed unless either it is "impliedly authorized" for the representation or enumerated among the limited exceptions in Rule 1.6(b) or Rule 1.6(c).[5] This may mean that a third party vendor, as with "cloud computing," could be "impliedly authorized" to handle client data provided that the information remains confidential, is kept secure, and any disclosure is confined only to necessary personnel. It also means that various safeguards should be in place so that an attorney can be reasonably certain to protect any information that is transmitted, stored, accessed, or otherwise processed through cloud services. Comment [24] to Rule 1.6(a) further clarifies an attorney's duties and obligations:

> When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy. Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this Rule.

An attorney utilizing "cloud computing" will likely encounter circumstances that require unique considerations to secure client confidentiality. For example, because a server used by a "cloud computing" provider may physically be kept in another country, an attorney must ensure that the data in the server is protected by privacy laws that reasonably mirror those of the United States. Also, there may be situations in which the provider's ability to protect the information is compromised, whether through hacking, internal impropriety, technical failures, bankruptcy, or other circumstances. While some of these situations may also affect attorneys who use offline

[5] The exceptions covered in Rule 1.6(b) and (c) are not implicated in "cloud computing." Generally, they cover compliance with Rule 3.3 ("Candor Toward the Tribunal"), the prevention of serious bodily harm, criminal and fraudulent acts, proceedings concerning the lawyer's representation of the client, legal advice sought for Rule compliance, and the sale of a law practice.

storage, an attorney using "cloud computing" services may need to take special steps to satisfy his or her obligation under Rules 1.0, 1.6 and 1.15.[6]

Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistants") states:

> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> (a) A partner and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer.
>
> (b) A lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and
>
> (c) A lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:
>
> (1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
>
> (2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and in either case knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

At its essence, "cloud computing" can be seen as an online form of outsourcing subject to Rule 5.1 and Rule 5.3 governing the supervision of those who are associated with an attorney. Therefore, a lawyer must ensure that tasks are delegated to competent people and organizations. This means that any service provider who handles client information needs to be able to limit authorized access to the data to only necessary personnel, ensure that the information is backed up, reasonably available to the attorney, and reasonably safe from unauthorized intrusion.

It is also important that the vendor understands, embraces, and is obligated to conform to the professional responsibilities required of lawyers, including a specific agreement to comply with all ethical guidelines, as outlined below. Attorneys may also need a written service agreement that can be enforced on the provider to protect the client's interests. In some circumstances, a client may need to be advised of the outsourcing or use of a service provider and the identification of the provider. A lawyer may also need an agreement or written disclosure with the client to outline the nature of the cloud services used, and its impact upon the client's matter.

C. Obligations of Reasonable Care for Pennsylvania/Factors to Consider

[6] Advisable steps for an attorney to take reasonable care to meet his or her obligations for Professional Conduct are outlined below.

In the context of "cloud computing," an attorney must take reasonable care to make sure that the conduct of the cloud computing service provider conforms to the rules to which the attorney himself is subject. Because the operation is outside of an attorney's direct control, some of the steps taken to ensure reasonable care are different from those applicable to traditional information storage.

While the measures necessary to protect confidential information will vary based upon the technology and infrastructure of each office – and this Committee acknowledges that the advances in technology make it difficult, if not impossible to provide specific standards that will apply to every attorney – there are common procedures and safeguards that attorneys should employ.

These various safeguards also apply to traditional law offices. Competency extends beyond protecting client information and confidentiality; it also includes a lawyer's ability to reliably access and provide information relevant to a client's case when needed. This is essential for attorneys regardless of whether data is stored onsite or offsite with a cloud service provider. However, since cloud services are under the provider's control, using "the cloud" to store data electronically could have unwanted consequences, such as interruptions in service or data loss. There are numerous examples of these types of events. Amazon EC2 has experienced outages in the past few years, leaving a portion of users without service for hours at a time. Google has also had multiple service outages, as have other providers. Digital Railroad, a photo archiving service, collapsed financially and simply shut down. These types of risks should alert anyone contemplating using cloud services to select a suitable provider, take reasonable precautions to back up data and ensure its accessibility when the user needs it.

Thus, the standard of reasonable care for "cloud computing" may include:

- Backing up data to allow the firm to restore data that has been lost, corrupted, or accidentally deleted;
- Installing a firewall to limit access to the firm's network;
- Limiting information that is provided to others to what is required, needed, or requested;
- Avoiding inadvertent disclosure of information;
- Verifying the identity of individuals to whom the attorney provides confidential information;
- Refusing to disclose confidential information to unauthorized individuals (including family members and friends) without client permission;
- Protecting electronic records containing confidential data, including backups, by encrypting the confidential data;
- Implementing electronic audit trail procedures to monitor who is accessing the data;

- Creating plans to address security breaches, including the identification of persons to be notified about any known or suspected security breach involving confidential data;

- Ensuring the provider:
    - explicitly agrees that it has no ownership or security interest in the data;
    - has an enforceable obligation to preserve security;
    - will notify the lawyer if requested to produce data to a third party, and provide the lawyer with the ability to respond to the request before the provider produces the requested information;
    - has technology built to withstand a reasonably foreseeable attempt to infiltrate data, including penetration testing;
    - includes in its "Terms of Service" or "Service Level Agreement" an agreement about how confidential client information will be handled;
    - provides the firm with right to audit the provider's security procedures and to obtain copies of any security audits performed;
    - will host the firm's data only within a specified geographic area. If by agreement, the data are hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and Pennsylvania;
    - provides a method of retrieving data if the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity; and,
    - provides the ability for the law firm to get data "off" of the vendor's or third party data hosting company's servers for the firm's own use or in-house backup offline.

- Investigating the provider's:
    - security measures, policies and recovery methods;
    - system for backing up data;
    - security of data centers and whether the storage is in multiple centers;
    - safeguards against disasters, including different server locations;
    - history, including how long the provider has been in business;
    - funding and stability;
    - policies for data retrieval upon termination of the relationship and any related charges; and,
    - process to comply with data that is subject to a litigation hold.

- Determining whether:
    - data is in non-proprietary format;
    - the Service Level Agreement clearly states that the attorney owns the data;
    - there is a 3rd party audit of security; and,
    - there is an uptime guarantee and whether failure results in service credits.

- Employees of the firm who use the SaaS must receive training on and are required to abide by all end-user security measures, including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

- Protecting the ability to represent the client reliably by ensuring that a copy of digital data is stored onsite.[7]

- Having an alternate way to connect to the internet, since cloud service is accessed through the internet.

The terms and conditions under which the "cloud computing" services are offered, *i.e.,* Service Level Agreements ("SLAs"), may also present obstacles to reasonable care efforts. Most SLAs are essentially "take it or leave it,"[8] and often users, including lawyers, do not read the terms closely or at all. As a result, compliance with ethical mandates can be difficult. However, new competition in the "cloud computing" field is now causing vendors to consider altering terms. This can help attorneys meet their ethical obligations by facilitating an agreement with a vendor that adequately safeguards security and reliability.[9]

Additional responsibilities flow from actual breaches of data. At least forty-five states, including Pennsylvania, currently have data breach notification laws and a federal law is expected. Pennsylvania's notification law, 73 P.S. § 2303 (2011) ("Notification of Breach"), states:

> (a) GENERAL RULE. -- An entity that maintains, stores or manages computerized data that includes personal information shall provide notice of any breach of the security of the system following discovery of the breach of the security of the system to any resident of this Commonwealth whose unencrypted and unredacted personal information was or is reasonably believed to have been accessed and acquired by an unauthorized person. Except as provided in section 4 or in order to take any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the data system, the notice shall be made without unreasonable delay. For the purpose of this section, a resident of this Commonwealth may be determined to be an individual whose principal mailing address, as reflected in the computerized data which is maintained, stored or managed by the entity, is in this Commonwealth.
>
> (b) ENCRYPTED INFORMATION. -- An entity must provide notice of the breach if encrypted information is accessed and acquired in an unencrypted form, if the security breach is linked to a breach of the security of the encryption or if the security breach involves a person with access to the encryption key.

---

[7] This is recommended even though many vendors will claim that it is not necessary.

[8] Larger providers can be especially rigid with SLAs, since standardized agreements help providers to reduce costs.

[9] One caveat in an increasing field of vendors is that some upstart providers may not have staying power. Attorneys are well advised to consider the stability of any company that may handle sensitive information and the ramifications for the data in the event of bankruptcy, disruption in service or potential data breaches.

> (c) VENDOR NOTIFICATION. -- A vendor that maintains, stores or manages computerized data on behalf of another entity shall provide notice of any breach of the security system following discovery by the vendor to the entity on whose behalf the vendor maintains, stores or manages the data. The entity shall be responsible for making the determinations and discharging any remaining duties under this act.

A June, 2010, Pew survey highlighted concerns about security for "cloud computing." In the survey, a number of the nearly 900 internet experts surveyed agreed that it "presents security problems and further exposes private information," and some experts even predicted that "the cloud" will eventually have a massive breach from cyber-attacks.[10] Incident response plans should be in place before attorneys move to "the cloud", and the plans need to be reviewed annually. Lawyers may need to consider that at least some data may be too important to risk inclusion in cloud services.

One alternative to increase security measures against data breaches could be "private clouds." Private clouds are not hosted on the Internet, and give users completely internal security and control. Therefore, outsourcing rules do not apply to private clouds. Reasonable care standards still apply, however, as private clouds do not have impenetrable security. Another consideration might be hybrid clouds, which combine standard and private cloud functions.

D. Web-based E-mail

Web-based email ("webmail") is a common way to communicate for individuals and businesses alike. Examples of webmail include AOL Mail, Hotmail, Gmail, and Yahoo! Mail. These services transmit and store e-mails and other files entirely online and, like other forms of "cloud computing," are accessed through an internet browser. While pervasive, webmail carries with it risks that attorneys should be aware of and mitigate in order to stay in compliance with their ethical obligations. As with all other cloud services, reasonable care in transmitting and storing client information through webmail is appropriate.

In 1999, The ABA Standing Commission on Ethics and Professional Responsibility issued Formal Opinion No. 99-413, discussed in further detail above, and concluded that using unencrypted email is permissible. Generally, concerns about e-mail security are increasing, particularly unencrypted e-mail. Whether an attorney's obligations should include the safeguard of encrypting emails is a matter of debate. An article entitled, "Legal Ethics in the Cloud: Avoiding the Storms," explains:

> Respected security professionals for years have compared e-mail to postcards or postcards written in pencil. Encryption is being increasingly required in areas like banking and health care. New laws in Nevada and Massachusetts (which apply to attorneys as well as others) require defined personal information to be encrypted when it is electronically transmitted. As the use of encryption grows in areas like

[10] Janna Quitney Anderson & Lee Rainie, The Future of Cloud Computing. Pew Internet & American Life Project, June 11, 2010, http://www.pewinternet.org/Reports/2010/The-future-of-cloud-computing/Main-Findings.aspx?view=all

> these, it will become difficult for attorneys to demonstrate that confidential client data needs lesser protection.[11]

The article also provides a list of nine potential e-mail risk areas, including: confidentiality, authenticity, integrity, misdirection or forwarding, permanence (wanted e-mail may become lost and unwanted e-mail may remain accessible even if deleted), and malware. The article further provides guidance for protecting e-mail by stating:

> In addition to complying with any legal requirements that apply, the most prudent approach to the ethical duty of protecting confidentiality is to have an express understanding with clients about the nature of communications that will be (and will not be) sent by e-mail and whether or not encryption and other security measures will be utilized.
>
> It has now reached the point (or at least is reaching it) where most attorneys should have encryption available for use in appropriate circumstances.[12]

Compounding the general security concerns for e-mail is that users increasingly access webmail using unsecure or vulnerable methods such as cell phones or laptops with public wireless internet connections. Reasonable precautions are necessary to minimize the risk of unauthorized access to sensitive client information when using these devices and services, possibly including precautions such as encryption and strong password protection in the event of lost or stolen devices, or hacking.

The Committee further notes that this issue was addressed by the District of Columbia Bar in Opinion 281 (Feb. 18, 1998) ("Transmission of Confidential Information by Electronic Mail"), which concluded that, "In most circumstances, transmission of confidential information by unencrypted electronic mail does not per se violate the confidentiality rules of the legal profession. However, individual circumstances may require greater means of security."

The Committee concluded, and this Committee agrees, that the use of unencrypted electronic mail is not, by itself, a violation of the Rules of Professional Conduct, in particular Rule 1.6 ("Confidentiality of Information").

> Thus, we hold that the mere use of electronic communication is not a violation of Rule 1.6 absent special factors. We recognize that as to any confidential communication, the sensitivity of the contents of the communication and/or the circumstances of the transmission may, in specific instances, dictate higher levels of security. Thus, it may be necessary in certain circumstances to use extraordinary means to protect client confidences. To give an obvious example, a lawyer representing an associate in a dispute with the associate's law firm could very easily violate Rule 1.6 by sending a fax concerning the dispute to the law firm's mail room if that message contained client confidential

---

[11] David G. Ries, Esquire, "Legal Ethics in the Cloud: Avoiding the Storms," course handbook, *Cloud Computing 2011: Cut Through the Fluff & Tackle the Critical Stuff* (June 2011) (internal citations omitted).

[12] *Id.*

information. It is reasonable to suppose that employees of the firm, other lawyer employed at the firm, indeed firm management, could very well inadvertently see such a fax and learn of its contents concerning the associate's dispute with the law firm. Thus, what may ordinarily be permissible—the transmission of confidential information by facsimile—may not be permissible in a particularly factual context.

By the same analysis, what may ordinarily be permissible – the use of unencrypted electronic transmission – may not be acceptable in the context of a particularly heightened degree of concern or in a particular set of facts. But with that exception, we find that a lawyer takes reasonable steps to protect his client's confidence when he uses unencrypted electronically transmitted messages.

E. Opinions From Other Ethics Committees

Other Ethics Committees have reached conclusions similar in substance to those in this Opinion. Generally, the consensus is that, while "cloud computing" is permissible, lawyers should proceed with caution because they have an ethical duty to protect sensitive client data. In service to that essential duty, and in order to meet the standard of reasonable care, other Committees have determined that attorneys must (1) include terms in any agreement with the provider that require the provider to preserve the confidentiality and security of the data, and (2) be knowledgeable about how providers will handle the data entrusted to them. Some Committees have also raised ethical concerns regarding confidentiality issues with third-party access or general electronic transmission (*e.g.*, web-based email) and these conclusions are consistent with opinions about emergent emergent "cloud computing" technologies.

The American Bar Association Standing Committee on Ethics and Professional Responsibility has not yet issued a formal opinion on "cloud computing." However, the ABA Commission on Ethics 20/20 Working Group on the Implications of New Technologies, published an "Issues Paper Concerning Client Confidentiality and Lawyers' Use of Technology" (Sept. 20, 2010) and considered some of the concerns and ethical implications of using "the cloud." The Working Group found that potential confidentiality problems involved with "cloud computing" include:

- Storage in countries with less legal protection for data;
- Unclear policies regarding data ownership;
- Failure to adequately back up data;
- Unclear policies for data breach notice;
- Insufficient encryption;
- Unclear data destruction policies;
- Bankruptcy;
- Protocol for a change of cloud providers;
- Disgruntled/dishonest insiders;
- Hackers;
- Technical failures;
- Server crashes;
- Viruses;

- Data corruption;
- Data destruction;
- Business interruption (*e.g.*, weather, accident, terrorism); and,
- Absolute loss (*i.e.*, natural or man-made disasters that destroy everything).

Id. The Working Group also stated, "[f]orms of technology other than 'cloud computing' can produce just as many confidentiality-related concerns, such as when laptops, flash drives, and smart phones are lost or stolen." *Id.* Among the precautions the Commission is considering recommending are:

- Physical protection for devices (*e.g.*, laptops) or methods for remotely deleting data from lost or stolen devices;
- Strong passwords;
- Purging data from replaced devices (*e.g.*, computers, smart phones, and copiers with scanners);
- Safeguards against malware (*e.g.*, virus and spyware protection);
- Firewalls to prevent unauthorized access;
- Frequent backups of data;
- Updating to operating systems with the latest security protections;
- Configuring software and network settings to minimize security risks;
- Encrypting sensitive information;
- Identifying or eliminating metadata from electronic documents; and
- Avoiding public Wi-Fi when transmitting confidential information (*e.g.*, sending an email to a client).

Id. Additionally, the ABA Commission on Ethics 20/20 has drafted a proposal to amend, *inter alia*, Model Rule 1.0 ("Terminology"), Model Rule 1.1 ("Competence"), and Model Rule 1.6 ("Duty of Confidentiality") to account for confidentiality concerns with the use of technology, in particular confidential information stored in an electronic format. Among the proposed amendments (insertions underlined, deletions ~~struck through~~):

> Rule 1.1 ("Competence") Comment [6] ("Maintaining Competence"): "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."
>
> Rule 1.6(c) ("Duty of Confidentiality"): "A lawyer shall make reasonable efforts to prevent the inadvertent disclosure of, or unauthorized access to, information relating to the representation of a client."
>
> Rule 1.6 ("Duty of Confidentiality") Comment [16] ("Acting Competently to Preserve Confidentiality"): "Paragraph (c) requires a ~~A~~ lawyer ~~must~~ to act competently to safeguard information relating to the representation of a client against inadvertent or unauthorized disclosure by the lawyer or other persons or entities who are participating in the representation of the client or who are subject to the lawyer's supervision or monitoring. See Rules 1.1, 5.1, and 5.3. Factors to

> be considered in determining the reasonableness of the lawyer's efforts include the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, and the cost of employing additional safeguards. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules.

In Formal Opinion No. 99-413 (March 10, 1999), the ABA Standing Committee on Ethics and Professional Responsibility determined that using e-mail for professional correspondence is acceptable. Ultimately, it concluded that unencrypted e-mail poses no greater risks than other communication modes commonly relied upon. As the Committee reasoned, "The risk of unauthorized interception and disclosure exists in every medium of communication, including e-mail. It is not, however, reasonable to require that a mode of communicating information must be avoided simply because interception is technologically possible, especially when unauthorized interception or dissemination of the information is a violation of the law." *Id.*

Also relevant is ABA Formal Opinion 08-451 (August 5, 2008), which concluded that the ABA Model Rules generally allow for outsourcing of legal and non-legal support services if the outsourcing attorney ensures compliance with competency, confidentiality, and supervision. The Committee stated that an attorney has a supervisory obligation to ensure compliance with professional ethics even if the attorney's affiliation with the other lawyer or nonlawyer is indirect. An attorney is therefore obligated to ensure that any service provider complies with confidentiality standards. The Committee advised attorneys to utilize written confidentiality agreements and to verify that the provider does not also work for an adversary.

The Alabama State Bar Office of General Council Disciplinary Commission issued Ethics Opinion 2010-02, concluding that an attorney must exercise reasonable care in storing client files, which includes becoming knowledgeable about a provider's storage and security and ensuring that the provider will abide by a confidentiality agreement. Lawyers should stay on top of emerging technology to ensure security is safeguarded. Attorneys may also need to back up electronic data to protect against technical or physical impairment, and install firewalls and intrusion detection software.

State Bar of Arizona Ethics Opinion 09-04 (Dec. 2009) stated that an attorney should take reasonable precautions to protect the security and confidentiality of data, precautions which are satisfied when data is accessible exclusively through a Secure Sockets Layer ("SSL") encrypted connection and at least one other password was used to protect each document on the system. The Opinion further stated, "It is important that lawyers recognize their own competence limitations regarding computer security measures and take the necessary time and energy to become competent or alternatively consult experts in the field." *Id.* Also, lawyers should ensure reasonable protection through a periodic review of security as new technologies emerge.

The California State Bar Standing Committee on Professional Responsibility and Conduct concluded in its Formal Opinion 2010-179 that an attorney using public wireless connections to conduct research and send e-mails should use precautions, such as personal firewalls and encrypting files and transmissions, or else risk violating his or her confidentiality and competence obligations. Some highly sensitive matters may necessitate discussing the use of

public wireless connections with the client or in the alternative avoiding their use altogether. Appropriately secure personal connections meet a lawyer's professional obligations. Ultimately, the Committee found that attorneys should (1) use technology in conjunction with appropriate measures to protect client confidentiality, (2) tailor such measures to each unique type of technology, and (3) stay abreast of technological advances to ensure those measures remain sufficient.

The Florida Bar Standing Committee on Professional Ethics, in Opinion 06-1 (April 10, 2006), concluded that lawyers may utilize electronic filing provided that attorneys "take reasonable precautions to ensure confidentiality of client information, particularly if the lawyer relies on third parties to convert and store paper documents to electronic records." *Id.*

Illinois State Bar Association Ethics Opinion 10-01 (July 2009) stated that "[a] law firm's use of an off-site network administrator to assist in the operation of its law practice will not violate the Illinois Rules of Professional Conduct regarding the confidentiality of client information if the law firm makes reasonable efforts to ensure the protection of confidential client information."[13]

The Maine Board of Overseers of the Bar Professional Ethics Commission adopted Opinion 194 (June 30, 2008) in which it stated that attorneys may use third-party electronic back-up and transcription services so long as appropriate safeguards are taken, including "reasonable efforts to prevent the disclosure of confidential information," and at minimum an agreement with the vendor that contains "a legally enforceable obligation to maintain the confidentiality of the client data involved." *Id.*

Of note, and the Maine Ethics Commission, in a footnote, suggests in Opinion 194 that the federal Health Insurance Portability and Accountability Act ("HIPAA") Privacy and Security Rule 45 C.F.R. Subpart 164.314(a)(2) provides a good medical field example of contract requirements between medical professionals and third party service providers ("business associates") that handle confidential patient information. SLAs that reflect these or similar requirements may be advisable for lawyers who use cloud services.

45 C.F.R. Subpart 164.314(a)(2)(i) states:

> The contract between a covered entity and a business associate must provide that the business associate will:
>
> (A) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the covered entity as required by this subpart;

---

[13] Mark Mathewson, *New ISBA Ethics Opinion Re: Confidentiality and Third-Party Tech Vendors*, Illinois Lawyer Now, July 24, 2009, available at http://www.illinoislawyernow.com/2009/07/24/new-isba-ethics-opinion-re-confidentiality-and-third-party-tech-vendors/

(B) Ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it;

(C) Report to the covered entity any security incident of which it becomes aware;

(D) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract.

Massachusetts Bar Association Ethics Opinion 05-04 (March 3, 2005) addressed ethical concerns surrounding a computer support vendor's access to a firm's computers containing confidential client information. The committee concluded that a lawyer may provide a third-party vendor with access to confidential client information to support and maintain a firm's software. Clients have "impliedly authorized" lawyers to make confidential information accessible to vendors "pursuant to Rule 1.6(a) in order to permit the firm to provide representation to its clients." *Id.* Lawyers must "make reasonable efforts to ensure" a vendor's conduct comports with professional obligations. *Id.*

The State Bar of Nevada Standing Committee on Ethics and Professional Responsibility issued Formal Opinion No. 33 (Feb. 9, 2006) in which it stated, "an attorney may use an outside agency to store confidential information in electronic form, and on hardware located outside an attorney's direct supervision and control, so long as the attorney observed the usual obligations applicable to such arrangements for third party storage services." *Id.* Providers should, as part of the service agreement, safeguard confidentiality and prevent unauthorized access to data. The Committee determined that an attorney does not violate ethical standards by using third-party storage, even if a breach occurs, so long as he or she acts competently and reasonably in protecting information.

The New Jersey State Bar Association Advisory Committee on Professional Ethics issued Opinion 701 (April 2006) in which it concluded that, when using electronic filing systems, attorneys must safeguard client confidentiality by exercising "sound professional judgment" and reasonable care against unauthorized access, employing reasonably available technology. *Id.* Attorneys should obligate outside vendors, through "contract, professional standards, or otherwise," to safeguard confidential information. *Id.* The Committee recognized that Internet service providers often have better security than a firm would, so information is not necessarily safer when it is stored on a firm's local server. The Committee also noted that a strict guarantee of invulnerability is impossible in any method of file maintenance, even in paper document filing, since a burglar could conceivably break into a file room or a thief could steal mail.

The New York State Bar Association Committee on Professional Ethics concluded in Opinion 842 (Sept. 10, 2010) that the reasonable care standard for confidentiality should be maintained for online data storage and a lawyer is required to stay abreast of technology advances to ensure protection. Reasonable care may include: (1) obligating the provider to preserve confidentiality and security and to notify the attorney if served with process to produce client information, (2) making sure the provider has adequate security measures, policies, and recoverability methods,

and (3) guarding against "reasonably foreseeable" data infiltration by using available technology. *Id.*

The North Carolina State Bar Ethics Committee has addressed the issue of "cloud computing" directly, and this Opinion adopts in large part the recommendations of this Committee. Proposed Formal Opinion 6 (April 21, 2011) concluded that "a law firm may use SaaS[14] if reasonable care is taken effectively to minimize the risks to the disclosure of confidential information and to the security of client information and client files." *Id.* The Committee reasoned that North Carolina Rules of Professional Conduct do not require a specific mode of protection for client information or prohibit using vendors who may handle confidential information, but they do require reasonable care in determining the best method of representation while preserving client data integrity. Further, the Committee determined that lawyers "must protect against security weaknesses unique to the Internet, particularly 'end-user' vulnerabilities found in the lawyer's own law office." *Id.*

The Committee's minimum requirements for reasonable care in Proposed Formal Opinion 6 included:[15]

- An agreement on how confidential client information will be handled in keeping with the lawyer's professional responsibilities must be included in the SaaS vendor's Terms of Service or Service Level Agreement, or in a separate agreement that states that the employees at the vendor's data center are agents of the law firm and have a fiduciary responsibility to protect confidential client information and client property;

- The agreement with the vendor must specify that firm's data will be hosted only within a specified geographic area. If by agreement the data is hosted outside of the United States, the law firm must determine that the hosting jurisdiction has privacy laws, data security laws, and protections against unlawful search and seizure that are as rigorous as those of the United States and the state of North Carolina;

- If the lawyer terminates use of the SaaS product, the SaaS vendor goes out of business, or the service otherwise has a break in continuity, the law firm must have a method for retrieving the data, the data must be available in a non-proprietary format that is compatible with other firm software or the firm must have access to the vendor's software or source code, and data hosted by the vendor or third party data hosting company must be destroyed or returned promptly;

---

[14] SaaS, as stated above, stands for Software-as-a-Service and is a type of "cloud computing."

[15] The Committee emphasized that these are minimum requirements, and, because risks constantly evolve, "due diligence and perpetual education as to the security risks of SaaS are required." Consequently, lawyers may need security consultants to assess whether additional measures are necessary.

- The law firm must be able get data "off" the vendor's or third party data hosting company's servers for lawyers' own use or in-house backup offline; and,

- Employees of the firm who use SaaS should receive training on and be required to abide by end-user security measures including, but not limited to, the creation of strong passwords and the regular replacement of passwords.

In Opinion 99-03 (June 21, 1999), the **State Bar Association of North Dakota** Ethics Committee determined that attorneys are permitted to use online data backup services protected by confidential passwords. Two separate confidentiality issues that the Committee identified are, (1) transmission of data over the internet, and (2) the storage of electronic data. The Committee concluded that the transmission of data and the use of online data backup services are permissible provided that lawyers ensure adequate security, including limiting access only to authorized personnel and requiring passwords.

Vermont Bar Association Advisory Ethics Opinion 2003-03 concluded that lawyers can use third-party vendors as consultants for confidential client data-base recovery if the vendor fully understands and embraces the clearly communicated confidentiality rules. Lawyers should determine whether contractors have sufficient safety measures to protect information. A significant breach obligates a lawyer to disclose the breach to the client.

Virginia State Bar Ethics Counsel Legal Ethics Opinion 1818 (Sept. 30, 2005) stated that lawyers using third party technical assistance and support for electronic storage should adhere to Virginia Rule of Professional Conduct 1.6(b)(6)[16], requiring "due care" in selecting the service provider and keeping the information confidential. *Id.*

These opinions have offered compelling rationales for concluding that using vendors for software, service, and information transmission and storage is permissible so long as attorneys meet the existing reasonable care standard under the applicable Rules of Professional Conduct, and are flexible in contemplating the steps that are required for reasonable care as technology changes.

IV. Conclusion

The use of "cloud computing," and electronic devices such as cell phones that take advantage of cloud services, is a growing trend in many industries, including law. Firms may be eager to capitalize on cloud services in an effort to promote mobility, flexibility, organization and efficiency, reduce costs, and enable lawyers to focus more on legal, rather than technical and

[16] Virginia Rule of Professional Conduct 1.6(b) states in relevant part:

> To the extent a lawyer reasonably believes necessary, the lawyer may reveal:
>
> (6) information to an outside agency necessary for statistical, bookkeeping, accounting, data processing, printing, or other similar office management purposes, provided the lawyer exercises due care in the selection of the agency, advises the agency that the information must be kept confidential and reasonably believes that the information will be kept confidential.

administrative, issues. However, lawyers must be conscientious about maintaining traditional confidentiality, competence, and supervisory standards.

This Committee concludes that the Pennsylvania Rules of Professional Conduct require attorneys to make reasonable efforts to meet their obligations to ensure client confidentiality, and confirm that any third-party service provider is likewise obligated.

Accordingly, as outlined above, this Committee concludes that, under the Pennsylvania Rules of Professional Conduct an attorney may store confidential material in "the cloud." Because the need to maintain confidentiality is crucial to the attorney-client relationship, attorneys using "cloud" software or services must take appropriate measures to protect confidential electronic communications and information. In addition, attorneys may use email but must, under appropriate circumstances, take additional precautions to assure client confidentiality.

ATTACHMENT 9

Rule 1.0(h)

"Informed consent" denotes the agreement by a person to a proposed course of conduct after the lawyer has communicated adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct.

ATTACHMENT 10

RULE 1.1 COMPETENCE

A lawyer shall provide competent representation to a client. Competent representation as used in this Rule means that a lawyer shall not handle a matter which the lawyer knows or should know to be beyond the lawyer's level of competence without associating another lawyer who the original lawyer reasonably believes to be competent to handle the matter in question. Competence requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

The maximum penalty for a violation of this Rule is disbarment.

Comment

Legal Knowledge and Skill

[1A] The purpose of these rules is not to give rise to a cause of action nor to create a presumption that a legal duty has been breached. These Rules are designed to provide guidance to lawyers and to provide a structure for regulating conduct through disciplinary agencies. They are not designed to be a basis for civil liability.

[1B] In determining whether a lawyer employs the requisite knowledge and skill in a particular matter, relevant factors include the relative complexity and specialized nature of the matter, the lawyer's general experience, the lawyer's training and experience in the field in question, the preparation and study the lawyer is able to give the matter and whether it is feasible to refer the matter to, or associate or consult with, a lawyer of established competence in the field in question. In many instances, the required proficiency is that of a general practitioner. Expertise in a particular field of law may be required in some circumstances.

[2] A lawyer need not necessarily have special training or prior experience to handle legal problems of a type with which the lawyer is unfamiliar. A newly admitted lawyer can be as competent as a practitioner with long experience. Some important legal skills, such as the analysis of precedent, the evaluation of evidence and legal drafting, are required in all legal problems. Perhaps the most fundamental legal skill consists of determining what kind of legal problems a situation may involve, a skill that necessarily transcends any particular specialized knowledge. A lawyer can provide adequate representation in a wholly novel field through necessary study. Competent representation can also be provided through the association of a lawyer of established competence in the field in question.

[3] In an emergency a lawyer may give advice or assistance in a matter in which the lawyer does not have the skill ordinarily required where referral to or consultation or association with another lawyer would be impractical. Even in an emergency, however, assistance should be limited to that reasonably necessary in the circumstances, for ill-considered action under emergency conditions can jeopardize the client's interest.

[4] A lawyer may accept representation where the requisite level of competence can be achieved by reasonable preparation. This applies as well to a lawyer who is appointed as counsel for an unrepresented person subject to Rule 6.2: Accepting Appointments.

Thoroughness and Preparation

[5] Competent handling of a particular matter includes inquiry into and analysis of the factual and

legal elements of the problem, and use of methods and procedures meeting the standards of competent practitioners. It also includes adequate preparation. The required attention and preparation are determined in part by what is at stake; major litigation and complex transactions ordinarily require more elaborate treatment than matters of lesser consequence.

Maintaining Competence

[6] To maintain the requisite knowledge and skill, a lawyer should engage in continuing study and education.

ATTACHMENT 11

RULE 1.2 SCOPE OF REPRESENTATION AND ALLOCATION OF AUTHORITY BETWEEN CLIENT AND LAWYER

a. Subject to paragraphs (c) and (d), a lawyer shall abide by a client's decisions concerning the scope and objectives of representation and, as required by Rule 1.4, shall consult with the client as to the means by which they are to be pursued. A lawyer may take such action on behalf of the client as is impliedly authorized to carry out the representation. A lawyer shall abide by a client's decision whether to settle a matter. In a criminal case, the lawyer shall abide by the client's decision, after consultation with the lawyer, as to a plea to be entered, whether to waive jury trial and whether the client will testify.
b. A lawyer's representation of a client, including representation by appointment, does not constitute an endorsement of the client's political, economic, social or moral views or activities.
c. A lawyer may limit the scope and objectives of the representation if the limitation is reasonable under the circumstances and the client gives informed consent.
d. A lawyer shall not counsel a client to engage in conduct that the lawyer knows is criminal or fraudulent, nor knowingly assist a client in such conduct, but a lawyer may discuss the legal consequences of any proposed course of conduct with a client and may counsel or assist a client to make a good faith effort to determine the validity, scope, meaning or application of the law.

The maximum penalty for a violation of this Rule is disbarment.

Comment

Allocation of Authority between Client and Lawyer

[1] Paragraph (a) confers upon the client the ultimate authority to determine the purposes to be served by legal representation, within the limits imposed by law and the lawyer's professional obligations. The decisions specified in paragraph (a), such as whether to settle a civil matter, must also be made by the client. See Rule 1.4(a)(1) for the lawyer's duty to communicate with the client about such decisions. With respect to the means by which the client's objectives are to be pursued, the lawyer shall consult with the client as required by Rule 1.4(a)(2) and may take such action as is impliedly authorized to carry out the representation.

[2] On occasion, however, a lawyer and a client may disagree about the means to be used to accomplish the client's objectives. Clients normally defer to the special knowledge and skill of their lawyer with respect to the means to be used to accomplish their objectives, particularly with respect to technical, legal and tactical matters. Conversely, lawyers usually defer to the client regarding such questions as the expense to be incurred and concern for third persons who might be adversely affected. Because of the varied nature of the matters about which a lawyer and client might disagree and because the actions in question may implicate the interests of a tribunal or other persons, this Rule does not prescribe how such disagreements are to be resolved. Other law, however, may be applicable and should be consulted by the lawyer. The lawyer should also consult with the client and seek a mutually acceptable resolution of the disagreement. If such efforts are unavailing and the lawyer has a fundamental disagreement with the client, the lawyer may withdraw from the representation. See Rule 1.16(b)(4). Conversely, the client may resolve the disagreement by

discharging the lawyer. See Rule 1.16(a)(3).

[3] At the outset of a representation, the client may authorize the lawyer to take specific action on the client's behalf without further consultation. Absent a material change in circumstances and subject to Rule 1.4, a lawyer may rely on such an advance authorization. The client may, however, revoke such authority at any time.

[4] In a case in which the client appears to be suffering from diminished capacity, the lawyer's duty to abide by the client's decisions is to be guided by reference to Rule 1.14.

Independence from Client's Views or Activities

[5] Legal representation should not be denied to people who are unable to afford legal services, or whose cause is controversial or the subject of popular disapproval. By the same token, representing a client does not constitute approval of the client's views or activities.

Agreements Limiting Scope of Representation

[6] The scope of services to be provided by a lawyer may be limited by agreement with the client or by the terms under which the lawyer's services are made available to the client. When a lawyer has been retained by an insurer to represent an insured, for example, the representation may be limited to matters related to the insurance coverage. A limited representation may be appropriate because the client has limited objectives for the representation. In addition, the terms upon which representation is undertaken may exclude specific means that might otherwise be used to accomplish the client's objectives. Such limitations may exclude actions that the client thinks are too costly or that the lawyer regards as repugnant or imprudent.

[7] Although this Rule affords the lawyer and the client substantial latitude to limit the representation, the limitation must be reasonable under the circumstances. If, for example, a client's objective is limited to securing general information about the law the client needs in order to handle a common and typically uncomplicated legal problem, the lawyer and client may agree that the lawyer's services will be limited to a brief telephone consultation. Such a limitation, however, would not be reasonable if the time allotted was not sufficient to yield advice upon which the client could rely. Although an agreement for a limited representation does not exempt a lawyer from the duty to provide competent representation, the limitation is a factor to be considered when determining the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation. See Rule 1.1.

[8] All agreements concerning a lawyer's representation of a client must accord with the Rules of Professional Conduct and other law. See, e.g., Rules 1.1, 1.8 and 5.6.

Criminal, Fraudulent and Prohibited Transactions

[9] Paragraph (d) prohibits a lawyer from knowingly counseling or assisting a client to commit a crime or fraud. This prohibition, however, does not preclude the lawyer from giving an honest opinion about the actual consequences that appear likely to result from a client's conduct. Nor does the fact that a client uses advice in a course of action that is criminal or fraudulent of itself make a lawyer a party to the course of action. There is a critical distinction between presenting an analysis of legal aspects of questionable conduct and recommending the means by which a crime or fraud might be committed with impunity.

[10] When the client's course of action has already begun and is continuing, the lawyer's responsibility is especially delicate. The lawyer is required to avoid assisting the client, for example, by drafting or delivering documents that the lawyer knows are fraudulent or by suggesting how the wrongdoing might be concealed. A lawyer may not continue assisting a client in conduct that the lawyer originally supposed was legally proper but then discovers is criminal or fraudulent. The lawyer must, therefore, withdraw from the representation of the client in the matter. See Rule 1.16(a). In some cases, withdrawal alone might be insufficient. It may be necessary for the lawyer to give notice of the fact of withdrawal and to disaffirm any opinion, document, affirmation or the like. See Rule 4.1.

[11] Where the client is a fiduciary, the lawyer may be charged with special obligations in dealings with a beneficiary.

[12] Paragraph (d) applies whether or not the defrauded party is a party to the transaction. Hence, a lawyer must not participate in a transaction to effectuate criminal or fraudulent voidance of tax liability. Paragraph (d) does not preclude undertaking a criminal defense incident to a general retainer for legal services to a lawful enterprise. The last clause of paragraph (d) recognizes that determining the validity or interpretation of a statute or regulation may require a course of action involving disobedience of the statute or regulation or of the interpretation placed upon it by governmental authorities.

[13] If a lawyer comes to know or reasonably should know that a client expects assistance not permitted by the Rules of Professional Conduct or other law or if the lawyer intends to act contrary to the client's instructions, the lawyer must consult with the client regarding the limitations on the lawyer's conduct. See Rule 1.4(a)(5).

ATTACHMENT 12

RULE 1.4 COMMUNICATION

a. A lawyer shall:
   1. promptly inform the client of any decision or circumstance with respect to which the client's informed consent, as defined in Rule 1.0(h), is required by these Rules;
   2. reasonably consult with the client about the means by which the client's objectives are to be accomplished;
   3. keep the client reasonably informed about the status of the matter;
   4. promptly comply with reasonable requests for information; and
   5. consult with the client about any relevant limitation on the lawyer's conduct when the lawyer knows that the client expects assistance not permitted by the Rules of Professional Conduct or other law.

b. A lawyer shall explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

The maximum penalty for a violation of this Rule is a public reprimand.

Comment

[1] Reasonable communication between the lawyer and the client is necessary for the client effectively to participate in the representation.

Communicating with Client

[2] If these Rules require that a particular decision about the representation be made by the client, paragraph (a)(1) requires that the lawyer promptly consult with and secure the client's informed consent prior to taking action unless prior discussions with the client have resolved what action the client wants the lawyer to take. For example, a lawyer who receives from opposing counsel an offer of settlement in a civil controversy or a proffered plea bargain in a criminal case must promptly inform the client of its substance unless the client has previously indicated that the proposal will be acceptable or unacceptable or has authorized the lawyer to accept or to reject the offer. See Rule 1.2(a).

[3] Paragraph (a)(2) requires the lawyer to reasonably consult with the client about the means to be used to accomplish the client's objectives. In some situations - depending on both the importance of the action under consideration and the feasibility of consulting with the client - this duty will require consultation prior to taking action. In other circumstances, such as during a trial when an immediate decision must be made, the exigency of the situation may require the lawyer to act without prior consultation. In such cases the lawyer must nonetheless act reasonably to inform the client of actions the lawyer has taken on the client's behalf. Additionally, paragraph (a)(3) requires that the lawyer keep the client reasonably informed about the status of the matter, such as significant developments affecting the timing or the substance of the representation.

[4] A lawyer's regular communication with clients will minimize the occasions on which a client will need to request information concerning the representation. When a client makes a reasonable request for information, however, paragraph (a)(4) requires prompt compliance with the request, or if a prompt response is not feasible, that the lawyer, or a member of the lawyer's staff, acknowledge receipt of the request and advise the client when a response may be expected. Client telephone calls should be promptly returned or acknowledged. The timeliness of a lawyer's communication must be judged by all the controlling factors. "Prompt" communication with the client does not equate to

"instant" communication with the client and is sufficient if reasonable under the relevant circumstances.

Explaining Matters

[5] The client should have sufficient information to participate intelligently in decisions concerning the objectives of the representation and the means by which they are to be pursued, to the extent the client is willing and able to do so. Adequacy of communication depends in part on the kind of advice or assistance that is involved. For example, where there is time to explain a proposal made in a negotiation, the lawyer should review all important provisions with the client before proceeding to an agreement. In litigation a lawyer should explain the general strategy and prospects of success and ordinarily should consult the client on tactics that are likely to result in significant expense or to injure or coerce others. On the other hand, a lawyer ordinarily will not be expected to describe trial or negotiation strategy in detail. The guiding principle is that the lawyer should fulfill reasonable client expectations for information consistent with the duty to act in the client's best interests, and the client's overall requirements as to the character of representation. In certain circumstances, such as when a lawyer asks a client to consent to a representation affected by a conflict of interest, the client must give informed consent, as defined in Rule 1.0(h).

[6] Ordinarily, the information to be provided is that appropriate for a client who is a comprehending and responsible adult. However, fully informing the client according to this standard may be impracticable, for example, where the client is a child or suffers from diminished capacity. See Rule 1.14. When the client is an organization or group, it is often impossible or inappropriate to inform every one of its members about its legal affairs; ordinarily, the lawyer should address communications to the appropriate officials of the organization. See Rule 1.13. Where many routine matters are involved, a system of limited or occasional reporting may be arranged with the client.

Withholding Information

[7] In some circumstances, a lawyer may be justified in delaying transmission of information when the client would be likely to react imprudently to an immediate communication. Thus, a lawyer might withhold a psychiatric diagnosis of a client when the examining psychiatrist indicates that disclosure would harm the client. A lawyer may not withhold information to serve the lawyer's own interest or convenience or the interests or convenience of another person. Rules or court orders governing litigation may provide that information supplied to a lawyer may not be disclosed to the client.

ATTACHMENT 13

RULE 1.6 CONFIDENTIALITY OF INFORMATION

a. A lawyer shall maintain in confidence all information gained in the professional relationship with a client, including information which the client has requested to be held inviolate or the disclosure of which would be embarrassing or would likely be detrimental to the client, unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, or are required by these Rules or other law, or by order of the Court.

b. 1. A lawyer may reveal information covered by paragraph (a) which the lawyer reasonably believes necessary:
   i. to avoid or prevent harm or substantial financial loss to another as a result of client criminal conduct or third party criminal conduct clearly in violation of the law;
   ii. to prevent serious injury or death not otherwise covered by subparagraph (i) above;
   iii. to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;
   iv. to secure legal advice about the lawyer's compliance with these Rules.

2. In a situation described in paragraph (b)(1), if the client has acted at the time the lawyer learns of the threat of harm or loss to a victim, use or disclosure is permissible only if the harm or loss has not yet occurred.

3. Before using or disclosing information pursuant to paragraph (b)(1), if feasible, the lawyer must make a good faith effort to persuade the client either not to act or, if the client has already acted, to warn the victim.

c. The lawyer may, where the law does not otherwise require, reveal information to which the duty of confidentiality does not apply under paragraph (b) without being subjected to disciplinary proceedings.

d. The lawyer shall reveal information under paragraph (b) as the applicable law requires.

e. The duty of confidentiality shall continue after the client-lawyer relationship has terminated.

The maximum penalty for a violation of this Rule is disbarment.

Comment

[1] The lawyer is part of a judicial system charged with upholding the law. One of the lawyer's functions is to advise clients so that they avoid any violation of the law in the proper exercise of their rights.

[2] The observance of the ethical obligation of a lawyer to hold inviolate confidential information of the client not only facilitates the full development of facts essential to proper representation of the client but also encourages people to seek early legal assistance.

[3] Almost without exception, clients come to lawyers in order to determine what their rights are and what is, in the maze of laws and regulations, deemed to be legal and correct. The common law recognizes that the client's confidences must be protected from disclosure. Based upon experience, lawyers know that almost all clients follow the advice given, and the law is upheld.

[4] A fundamental principle in the client-lawyer relationship is that the lawyer maintain confidentiality of information relating to the representation. The client is thereby encouraged to

communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter.

[4A] Information gained in the professional relationship includes information gained from a person (prospective client) who discusses the possibility of forming a client-lawyer relationship with respect to a matter. Even when no client-lawyer relationship ensues, the restrictions and exceptions of these Rules as to use or revelation of the information apply, e.g. Rules 1.9 and 1.10.

[5] The principle of confidentiality is given effect in two related bodies of law, the attorney-client privilege (which includes the work product doctrine) in the law of evidence and the rule of confidentiality established in professional ethics. The attorney-client privilege applies in judicial and other proceedings in which a lawyer may be called as a witness or otherwise required to produce evidence concerning a client. The rule of client-lawyer confidentiality applies in situations other than those where evidence is sought from the lawyer through compulsion of law. Rule 1.6 applies not merely to matters communicated in confidence by the client but also to all information gained in the professional relationship, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law. See also Scope. The requirement of maintaining confidentiality of information gained in the professional relationship applies to government lawyers who may disagree with the client's policy goals.

Authorized Disclosure

[6] A lawyer is impliedly authorized to make disclosures about a client when appropriate in carrying out the representation, except to the extent that the client's instructions or special circumstances limit that authority. In litigation, for example, a lawyer may disclose information by admitting a fact that cannot properly be disputed, or in negotiation by making a disclosure that facilitates a satisfactory conclusion.

[7] Lawyers in a firm may, in the course of the firm's practice, disclose to each other information relating to a client of the firm, unless the client has instructed that particular information be confined to specified lawyers.

[7A] A lawyer's confidentiality obligations do not preclude a lawyer from securing confidential legal advice about the lawyer's personal responsibility to comply with these Rules. In most situations, disclosing information to secure such advice will be impliedly authorized for the lawyer to carry out the representation. Even when the disclosure is not impliedly authorized paragraph (b)(1)(iv) permits such disclosure because of the importance of a lawyer's compliance with the Rules of Professional Conduct.

Disclosure Adverse to Client

[8] The confidentiality rule is subject to limited exceptions. In becoming privy to information about a client, a lawyer may foresee that the client intends serious harm to another person. The public is better protected if full and open communication by the client is encouraged than if it is inhibited.

[9] Several situations must be distinguished. First, the lawyer may not knowingly assist a client in conduct that is criminal or fraudulent. See Rule 1.2(d). Similarly, a lawyer has a duty under Rule 3.3(a)(4) not to use false evidence.

[10] Second, the lawyer may have been innocently involved in past conduct by the client that was criminal or fraudulent. In such a situation the lawyer has not violated Rule 1.2(d), because to

"knowingly assist" criminal or fraudulent conduct requires knowing that the conduct is of that character.

[11] Third, the lawyer may learn that a client intends prospective conduct that is criminal and likely to result in death or substantial bodily harm. As stated in paragraph (b)(1), the lawyer has professional discretion to reveal information in order to prevent such consequences. The lawyer may make a disclosure in order to prevent death or serious bodily injury which the lawyer reasonably believes will occur. It is very difficult for a lawyer to "know" when such a heinous purpose will actually be carried out, for the client may have a change of mind.

[12] The lawyer's exercise of discretion requires consideration of such factors as the nature of the lawyer's relationship with the client and with those who might be injured by the client, the lawyer's own involvement in the transaction and factors that may extenuate the conduct in question. Where practical, the lawyer should seek to persuade the client to take suitable action. In any case, a disclosure adverse to the client's interest should be no greater than the lawyer reasonably believes necessary to the purpose. A lawyer's decision not to take preventive action permitted by paragraph (b)(1) does not violate this Rule.

Withdrawal

[13] If the lawyer's services will be used by the client in materially furthering a course of criminal or fraudulent conduct, the lawyer must withdraw, as stated in Rule 1.16(a)(1).

[14] After withdrawal the lawyer is required to refrain from making disclosure of the client's confidences, except as otherwise provided in Rule 1.6. Neither this rule nor Rule 1.8(b) nor Rule 1.16(d) prevents the lawyer from giving notice of the fact of withdrawal, and the lawyer may also withdraw or disaffirm any opinion, document, affirmation, or the like.

[15] Where the client is an organization, the lawyer may be in doubt whether contemplated conduct will actually be carried out by the organization. Where necessary to guide conduct in connection with this Rule, the lawyer may make inquiry within the organization as indicated in Rule 1.13(b).

Dispute Concerning a Lawyer's Conduct

[16] Where a legal claim or disciplinary charge alleges complicity of the lawyer in a client's conduct or other misconduct of the lawyer involving representation of the client, the lawyer may respond to the extent the lawyer reasonably believes necessary to establish a defense. The same is true with respect to a claim involving the conduct or representation of a former client. The lawyer's right to respond arises when an assertion of such complicity has been made. Paragraph (b)(1)(iii) does not require the lawyer to await the commencement of an action or proceeding that charges such complicity, so that the defense may be established by responding directly to a third party who has made such an assertion. The right to defend, of course, applies where a proceeding has been commenced. Where practicable and not prejudicial to the lawyer's ability to establish the defense, the lawyer should advise the client of the third party's assertion and request that the client respond appropriately. In any event, disclosure should be no greater than the lawyer reasonably believes is necessary to vindicate innocence, the disclosure should be made in a manner which limits access to the information to the tribunal or other persons having a need to know it, and appropriate protective orders or other arrangements should be sought by the lawyer to the fullest extent practicable.

[17] If the lawyer is charged with wrongdoing in which the client's conduct is implicated, the rule of confidentiality should not prevent the lawyer from defending against the charge. Such a charge can

arise in a civil, criminal or professional disciplinary proceeding, and can be based on a wrong allegedly committed by the lawyer against the client, or on a wrong alleged by a third person; for example, a person claiming to have been defrauded by the lawyer and client acting together. A lawyer entitled to a fee is permitted by paragraph (b)(1)(iii) to prove the services rendered in an action to collect it. This aspect of the rule expresses the principle that the beneficiary of a fiduciary relationship may not exploit it to the detriment of the fiduciary. As stated above, the lawyer must make every effort practicable to avoid unnecessary disclosure of information relating to a representation, to limit disclosure to those having the need to know it, and to obtain protective orders or make other arrangements minimizing the risk of disclosure.

Disclosures Otherwise Required or Authorized

[18] The attorney-client privilege is differently defined in various jurisdictions. If a lawyer is called as a witness to give testimony concerning a client, absent waiver by the client, paragraph (a) requires the lawyer to invoke the privilege when it is applicable. The lawyer must comply with the final orders of a court or other tribunal of competent jurisdiction requiring the lawyer to give information about the client.

[19] The Rules of Professional Conduct in various circumstances permit or require a lawyer to disclose information relating to the representation. See Rules 2.2, 2.3, 3.3 and 4.1. In addition to these provisions, a lawyer may be obligated or permitted by other provisions of law to give information about a client. Whether another provision of law supersedes Rule 1.6 is a matter of interpretation beyond the scope of these Rules, but a presumption should exist against such a supersession.

ATTACHMENT 14

RULE 3.6 TRIAL PUBLICITY

a. A lawyer who is participating or has participated in the investigation or litigation of a matter shall not make an extrajudicial statement that a person would reasonably believe to be disseminated by means of public communication if the lawyer knows or reasonably should know that it will have a substantial likelihood of materially prejudicing an adjudicative proceeding in the matter.
b. Reserved.
c. Notwithstanding paragraph (a), a lawyer may make a statement that a reasonable lawyer would believe is required to protect a client from the substantial undue prejudicial effect of recent publicity not initiated by the lawyer or the lawyer's client. A statement made pursuant to this paragraph shall be limited to such information as is necessary to mitigate the recent adverse publicity.
d. No lawyer associated in a firm or government entity with a lawyer subject to paragraph (a) shall make a statement prohibited by paragraph (a).

The maximum penalty for a violation of this Rule is a public reprimand.

Comment

[1] It is difficult to strike a balance between protecting the right to a fair trial and safeguarding the right of free expression. Preserving the right to a fair trial necessarily entails some curtailment of the information that may be disseminated about a party prior to trial, particularly where trial by jury is involved. If there were no such limits, the result would be the practical nullification of the protective effect of the rules of forensic decorum and the exclusionary rules of evidence. On the other hand, there are vital social interests served by the free dissemination of information about events having legal consequences and about legal proceedings themselves. The public has a right to know about threats to its safety and measures aimed at assuring its security. It also has a legitimate interest in the conduct of judicial proceedings, particularly in matters of general public concern. Furthermore, the subject matter of legal proceedings is often of direct significance in debate and deliberation over questions of public policy.

[2] Special rules of confidentiality may validly govern proceedings in juvenile, domestic relations and mental disability proceedings, and perhaps other types of litigation.

[3] The Rule sets forth a basic general prohibition against a lawyer's making statements that the lawyer knows or should know will have a substantial likelihood of materially prejudicing an adjudicative proceeding. Recognizing that the public value of informed commentary is great and the likelihood of prejudice to a proceeding by the commentary of a lawyer who is not involved in the proceeding is small, the rule applies only to lawyers who are, or who have been involved in the investigation or litigation of a case, and their associates.

[4] Reserved.

[5A] There are, on the other hand, certain subjects which are more likely than not to have a material prejudicial effect on a proceeding, particularly when they refer to a civil matter triable to a jury, a criminal matter, or any other proceeding that could result in incarceration. These subjects relate to:

a. the character, credibility, reputation or criminal record of a party, suspect in a criminal investigation or witness, or the identity of a witness, or the expected testimony of a party or witness;

b. in a criminal case or proceeding that could result in incarceration, the possibility of a plea of guilty to the offense or the existence or contents of any confession, admission, or statement given by a defendant or suspect or that person's refusal or failure to make a statement;
c. the performance or results of any examination or test or the refusal or failure of a person to submit to an examination or test, or the identity or nature of physical evidence expected to be presented;
d. any opinion as to the guilt or innocence of a defendant or suspect in a criminal case or proceeding that could result in incarceration;
e. information that the lawyer knows or reasonably should know is likely to be inadmissible as evidence in a trial and that would, if disclosed, create a substantial risk of prejudicing an impartial trial; or
f. the fact that a defendant has been charged with a crime, unless there is included therein a statement explaining that the charge is merely an accusation and that the defendant is presumed innocent until and unless proven guilty.

[5B] In addition, there are certain subjects which are more likely than not to have no material prejudicial effect on a proceeding. Thus, a lawyer may usually state:

a. the claim, offense or defense involved and, except when prohibited by law, the identity of the persons involved;
b. information contained in a public record;
c. that an investigation of a matter is in progress;
d. the scheduling or result of any step in litigation;
e. a request for assistance in obtaining evidence and information necessary thereto;
f. a warning of danger concerning the behavior of a person involved, when there is reason to believe that there exists the likelihood of substantial harm to an individual or to the public interest; and
g. in a criminal case, in addition to subparagraphs (1) through (6):
    i. the identity, residence, occupation and family status of the accused;
    ii. if the accused has not been apprehended, information necessary to aid in apprehension of that person;
    iii. the fact, time and place of arrest; and
    iv. the identity of investigating and arresting officers or agencies and the length of the investigation.

[6] Another relevant factor in determining prejudice is the nature of the proceeding involved. Criminal jury trials will be most sensitive to extrajudicial speech. Civil trials may be less sensitive. Non-jury hearings and arbitration proceedings may be even less affected. The Rule will still place limitations on prejudicial comments in these cases, but the likelihood of prejudice may be different depending on the type of proceeding.

[7] Finally, extrajudicial statements that might otherwise raise a question under this Rule may be permissible when they are made in response to statements made publicly by another party, another party's lawyer, or third persons, where a reasonable lawyer would believe a public response is required in order to avoid prejudice to the lawyer's client. When prejudicial statements have been publicly made by others, responsive statements may have the salutary effect of lessening any resulting adverse impact on the adjudicative proceeding. Such responsive statements should be limited to contain only such information as is necessary to mitigate undue prejudice created by the statements made by others.

ATTACHMENT 15

RULE 5.1 RESPONSIBILITIES OF PARTNERS, MANAGERS AND SUPERVISORY LAWYERS

a. A law firm partner as defined in Rule 1.0 (l), and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Georgia Rules of Professional Conduct.
b. A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Georgia Rules of Professional Conduct.
c. A lawyer shall be responsible for another lawyer's violation of the Georgia Rules of Professional Conduct if:
    1. the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or
    2. the lawyer is a partner or has comparable maganerial authority in the law firm in which the other lawyer practices or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

The maximum penalty for a violation of this Rule is disbarment.

Comment

[1] Paragraph (a) applies to lawyers who have managerial authority over the professional work of a firm. *See Rule 1.0(e)*. This includes members of a partnership, the shareholders in a law firm organized as a professional corporation, and members of other associations authorized to practice law; lawyers having comparable managerial authority in a legal services organization or a law department of an enterprise or government agency; and lawyers who have intermediate managerial responsibilities in a firm. Paragraph (b) applies to lawyers who have supervisory authority over the work of other lawyers in a firm.

[2] Paragraph (a) requires lawyers with managerial authority within a firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that all lawyers in the firm will conform to the Georgia Rules of Professional Conduct. Such policies and procedures include those designed to detect and resolve conflicts of interest, identify dates by which actions must be taken in pending matters, account for client funds and property and ensure that inexperienced lawyers are properly supervised.

[3] Other measures that may be required to fulfill the responsibility prescribed in paragraph (a) can depend on the firm's structure and the nature of its practice. In a small firm of experienced lawyers, informal supervision and periodic review of compliance with the required systems ordinarily will suffice. In a large firm, or in practice situations in which difficult ethical problems frequently arise, more elaborate measures may be necessary. Some firms, for example, have a procedure whereby junior lawyers can make confidential referral of ethical problems directly to a designated senior partner or special committee. *See Rule 5.2.* Firms, whether large or small, may also rely on continuing legal education in professional ethics. In any event, the ethical atmosphere of a firm can influence the conduct of all its members, and the partners may not assume that all lawyers associated with the firm will inevitably conform to the Rules.

[4] Paragraph (c) expresses a general principle of personal responsibility for acts of another. *See also Rule 8.4(a)*.

[5] Paragraph (c)(2) defines the duty of a partner or other lawyer having comparable managerial authority in a law firm, as well as a lawyer who has direct supervisory authority over performance of specific legal work by another lawyer. Whether a lawyer has supervisory authority in particular circumstances is a question of fact. Partners and lawyers with comparable authority have at least indirect responsibility for all work being done by the firm, while a partner or manager in charge of a particular matter ordinarily also has supervisory responsibility for the work of other firm lawyers engaged in the matter. Appropriate remedial action by a partner or managing lawyer would depend on the immediacy of that lawyer's involvement and the seriousness of the misconduct. A supervisor is required to intervene to prevent avoidable consequences of misconduct if the supervisor knows that the misconduct occurred. Thus, if a supervising lawyer knows that a subordinate misrepresented a matter to an opposing party in negotiation, the supervisor as well as the subordinate has a duty to correct the resulting misapprehension.

[6] Professional misconduct by a lawyer under supervision could reveal a violation of paragraph (b) on the part of the supervisory lawyer even though it does not entail a violation of paragraph (c) because there was no direction, ratification or knowledge of the violation.

[7] Apart from this Rule and Rule 8.4(a), a lawyer does not have disciplinary liability for the conduct of a partner, associate or subordinate. Whether a lawyer may be liable civilly or criminally for another lawyer's conduct is a question of law beyond the scope of these Rules.

[8] The duties imposed by this Rule on managing and supervising lawyers do not alter the personal duty of each lawyer in a firm to abide by the Georgia Rules of Professional Conduct. *See Rule 5.2(a)*.

ATTACHMENT 16

RULE 5.3 RESPONSIBILITIES REGARDING NONLAWYER ASSISTANTS

With respect to a nonlawyer employed or retained by or associated with a lawyer:

a. a partner, and a lawyer who indiviually or together with other lawyers possesses managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the professional obligations of the lawyer;
b. a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer;
c. a lawyer shall be responsible for conduct of such a person that would be a violation of the Georgia Rules of Professional Conduct if engaged in by a lawyer if:
    1. the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or
    2. the lawyer is a partner in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action; and
d. a lawyer shall not allow any person who has been suspended or disbarred and who maintains a presence in an office where the practice of law is conducted by the lawyer, to:
    1. represent himself or herself as a lawyer or person with similar status;
    2. have any contact with the clients of the lawyer either in person, by telephone or in writing; or
    3. have any contact with persons who have legal dealings with the office either in person, by telephone or in writing.

The maximum penalty for a violation of this Rule is disbarment.

Comment

[1] Lawyers generally employ assistants in their practice, including secretaries, investigators, law student interns, and paraprofessionals. Such assistants, whether employees or independent contractors, act for the lawyer in rendition of the lawyer's professional services. A lawyer should give such assistants appropriate instruction and supervision concerning the ethical aspects of their employment, particularly regarding the obligation not to disclose information relating to representation of the client, and should be responsible for their work product. The measures employed in supervising nonlawyers should take account of the fact that they do not have legal training and are not subject to professional discipline.

[2] Paragraph (a) requires lawyers with managerial authority within a law firm to make reasonable efforts to establish internal policies and procedures designed to provide reasonable assurance that nonlawyers in the firm will act in a way compatible with the Georgia Rules of Professional Conduct. See Comment [1] to Rule 5.1. Paragraph (b) applies to lawyers who have supervisory authority over the work of a nonlawyer. Paragraph (c) specifies the circumstances in which a lawyer is responsible for conduct of a nonlawyer that would be a violation of the Georgia Rules of Professional Conduct if engaged in by a lawyer.

[3] The prohibitions of paragraph (d) apply to professional conduct and not to social conversation unrelated to the representation of clients or legal dealings of the law office, or the gathering of general information in the course of working in a law office. The thrust of the restriction is to

prevent the unauthorized practice of law in a law office by a person who has been suspended or disbarred.

ATTACHMENT 17

RULE 7.1 COMMUNICATIONS CONCERNING A LAWYER'S SERVICES

a. A lawyer may advertise through all forms of public media and through written communication not involving personal contact so long as the communication is not false, fraudulent, deceptive or misleading. By way of illustration, but not limitation, a communication is false, fraudulent, deceptive or misleading if it:
    1. contains a material misrepresentation of fact or law or omits a fact necessary to make the statement considered as a whole not materially misleading;
    2. is likely to create an unjustified expectation about results the lawyer can achieve, or states or implies that the lawyer can achieve results by means that violate the Georgia Rules of Professional Conduct or other law;
    3. compares the lawyer's services with other lawyers' services unless the comparison can be factually substantiated;
    4. fails to include the name of at least one lawyer responsible for its content; or
    5. contains any information regarding contingent fees, and fails to conspicuously present the following disclaimer:

       "Contingent attorneys' fees refers only to those fees charged by attorneys for their legal services. Such fees are not permitted in all types of cases. Court costs and other additional expenses of legal action usually must be paid by the client."
    6. contains the language 'no fee unless you win or collect' or any similar phrase and fails to conspicuously present the following disclaimer:

       "No fee unless you win or collect" [or insert the similar language used in the communication] refers only to fees charged by the attorney. Court costs and other additional expenses of legal action usually must be paid by the client. Contingent fees are not permitted in all types of cases.
b. A public communication for which a lawyer has given value must be identified as such unless it is apparent from the context that it is such a communication.
c. A lawyer retains ultimate responsibility to insure that all communications concerning the lawyer or the lawyer's services comply with the Georgia Rules of Professional Conduct.

The maximum penalty for a violation of this Rule is disbarment.

Comment

[1] This rule governs the content of all communications about a lawyer's services, including the various types of advertising permitted by Rules 7.3 through 7.5. Whatever means are used to make known a lawyer's services, statements about them should be truthful.

[2] The prohibition in sub-paragraph (a)(2) of this Rule 7.1: Communications Concerning a Lawyer's Services of statements that may create "unjustified expectations" would ordinarily preclude advertisements about results obtained on behalf of a client, such as the amount of a damage award or the lawyer's record in obtaining favorable verdicts, and advertisements containing client endorsements. Such information may create the unjustified expectation that similar results can be obtained for others without reference to the specific factual and legal circumstances.

Affirmative Disclosure

[3] In general, the intrusion on the First Amendment right of commercial speech resulting from rationally-based affirmative disclosure requirements is minimal, and is therefore a preferable form

of regulation to absolute bans or other similar restrictions. For example, there is no significant interest in failing to include the name of at least one accountable attorney in all communications promoting the services of a lawyer or law firm as required by sub-paragraph (a)(5) of Rule 7.1: Communications Concerning a Lawyer's Services. Nor is there any substantial burden imposed as a result of the affirmative disclaimer requirement of sub-paragraph (a)(6) upon a lawyer who wishes to make a claim in the nature of "no fee unless you win." Indeed, the United States Supreme Court has specifically recognized that affirmative disclosure of a client's liability for costs and expenses of litigation may be required to prevent consumer confusion over the technical distinction between the meaning and effect of the use of such terms as "fees" and "costs" in an advertisement.

[4] Certain promotional communications of a lawyer may, as a result of content or circumstance, tend to mislead a consumer to mistakenly believe that the communication is something other than a form of promotional communication for which the lawyer has paid. Examples of such a communication might include advertisements for seminars on legal topics directed to the lay public when such seminars are sponsored by the lawyer, or a newsletter or newspaper column which appears to inform or to educate about the law. Paragraph (b) of this Rule 7.1: Communications Concerning a Lawyer's Services would require affirmative disclosure that a lawyer has given value in order to generate these types of public communications if such is in fact the case.

Accountability

[5] Paragraph (c) makes explicit an advertising attorney's ultimate responsibility for all the lawyer's promotional communications and would suggest that review by the lawyer prior to dissemination is advisable if any doubts exist concerning conformity of the end product with these Rules. Although prior review by disciplinary authorities is not required by these Rules, lawyers are certainly encouraged to contact disciplinary authorities prior to authorizing a promotional communication if there are any doubts concerning either an interpretation of these Rules or their application to the communication.

ATTACHMENT 18

RULE 7.2 ADVERTISING

a. Subject to the requirements of Rules 7.1 and 7.3, a lawyer may advertise services through:
    1. public media, such as a telephone directory, legal directory, newspaper or other periodical;
    2. outdoor advertising;
    3. radio or television;
    4. written, electronic or recorded communication.
b. A copy or recording of an advertisement or communication shall be kept for two years after its last dissemination along with a record of when and where it was used.
c. Prominent disclosures. Any advertisement for legal services directed to potential clients in Georgia, or intended to solicit employment for delivery of any legal services in Georgia, must include prominent disclosures, clearly legible and capable of being read by the average person, if written, and clearly intelligible by an average person, if spoken aloud, of the following:
    1. Disclosure of identity and physical location of attorney. Any advertisement shall include the name, physical location and telephone number of each lawyer or law firm who paid for the advertisement and who takes full personal responsibility for the advertisement. In disclosing the physical location, the responsible lawyer shall state the full address of the location of the principal bona fide office of each lawyer who is prominently identified pursuant to this paragraph. For the purposes of this Rule, a bona fide office is defined as a physical location maintained by the lawyer or law firm from which the lawyer or law firm furnishes legal services on a regular and continuing basis. In the absence of a bona fide physical office, the lawyer shall prominently disclose the full address listed with the State Bar of Georgia or other Bar to which the lawyer is admitted. A lawyer who uses a referral service shall ensure that the service discloses the location of the lawyer's bona fide office, or the registered bar address, when a referral is made.
    2. Disclosure of referral practice. If the lawyer or law firm will refer the majority of callers to other attorneys, that fact must be disclosed and the lawyer or law firm must comply with the provisions of Rule 7.3(c) regarding referral services.
    3. Disclosure of spokespersons and portrayals. Any advertisement that includes a non-attorney spokesperson, portrayal of a lawyer by a non-lawyer, portrayal of a client by a non-client, or any paid testimonial or endorsement, shall include prominent disclosure of the use of a non-attorney spokesperson, portrayal of a lawyer by a non-lawyer, or of a client by a non-client.
    4. Disclosures regarding fees. A lawyer or law firm advertising any fixed fee for specified legal services shall, at the time of fee publication, have available to the public a written statement clearly describing the scope of each advertised service, which statement shall be available to the client at the time of retainer for any such service.
    5. Appearance of legal notices or pleadings. Any advertisement that includes any representation that resembles a legal pleading, notice, contract or other legal document shall include prominent disclosure that the document is an advertisement rather than a legal document.

The maximum penalty for a violation of this Rule is a public reprimand.

Comment

[1] To assist the public in obtaining legal services, lawyers should be allowed to make known

their services not only through reputation but also through organized information campaigns in the form of advertising. Advertising involves an active quest for clients, contrary to the tradition that a lawyer should not seek clientele. However, the public's need to know about legal services can be fulfilled in part through advertising. This need is particularly acute in the case of persons of moderate means who have not made extensive use of legal services. The interest in expanding public information about legal services ought to prevail over considerations of tradition. Nevertheless, advertising by lawyers entails the risk of practices that are misleading or overreaching.

[2] This Rule permits public dissemination of information concerning a lawyer's name or firm name, address and telephone number; the kinds of services the lawyer will undertake; the basis on which the lawyer's fees are determined, including prices for specific services and payment and credit arrangements; a lawyer's foreign language ability; names of references and, with their consent, names of clients regularly represented; and other information that might invite the attention of those seeking legal assistance.

[3] Questions of effectiveness and taste in advertising are matters of speculation and subjective judgment. Some jurisdictions have had extensive prohibitions against television advertising, against advertising going beyond specified facts about a lawyer, or against "undignified" advertising. Television is now one of the most powerful media for getting information to the public, particularly persons of low and moderate income; prohibiting television advertising, therefore, would impede the flow of information about legal services to many sectors of the public. Limiting the information that may be advertised has a similar effect and assumes that the bar can accurately forecast the kind of information that the public would regard as relevant.

[4] Neither this Rule nor Rule 7.3: Direct Contact with Prospective Clients prohibits communications authorized by law, such as notice to members of a class in class action litigation.

Record of Advertising

[5] Paragraph (b) requires that a record of the content and use of advertising be kept in order to facilitate enforcement of this Rule.

ATTACHMENT 19

RULE 7.3 DIRECT CONTACT WITH PROSPECTIVE CLIENTS

a. A lawyer shall not send, or knowingly permit to be sent, on behalf of the lawyer, the lawyer's firm, lawyer's partner, associate, or any other lawyer affiliated with the lawyer or the lawyer's firm, a written communication to a prospective client for the purpose of obtaining professional employment if:
    1. it has been made known to the lawyer that a person does not desire to receive communications from the lawyer;
    2. the communication involves coercion, duress, fraud, overreaching, harassment, intimidation or undue influence;
    3. the written communication concerns an action for personal injury or wrongful death or otherwise relates to an accident or disaster involving the person to whom the communication is addressed or a relative of that person, unless the accident or disaster occurred more than 30 days prior to the mailing of the communication; or
    4. the lawyer knows or reasonably should know that the physical, emotional or mental state of the person is such that the person could not exercise reasonable judgment in employing a lawyer.

b. Written communications to a prospective client, other than a close friend, relative, former client or one whom the lawyer reasonably believes is a former client, for the purpose of obtaining professional employment shall be plainly marked "Advertisement" on the face of the envelope and on the top of each page of the written communication in type size no smaller than the largest type size used in the body of the letter.

c. A lawyer shall not compensate or give anything of value to a person or organization to recommend or secure the lawyer's employment by a client, or as a reward for having made a recommendation resulting in the lawyer's employment by a client; except that the lawyer may pay for public communications permitted by Rule 7.1 and except as follows:
    1. A lawyer may pay the usual and reasonable fees or dues charged by a bona fide lawyer referral service operated by an organization authorized by law and qualified to do business in this state; provided, however, such organization has filed with the State Disciplinary Board, at least annually, a report showing its terms, its subscription charges, agreements with counsel, the number of lawyers participating, and the names and addresses of lawyers participating in the service;
    2. A lawyer may pay the usual and reasonable fees or dues charged by a bar-operated non-profit lawyer referral service, including a fee which is calculated as a percentage of the legal fees earned by the lawyer to whom the service has referred a matter, provided such bar-operated non-profit lawyer referral service meets the following criteria:
        i. the lawyer referral service shall be operated in the public interest for the purpose of referring prospective clients to lawyers, pro bono and public service legal programs, and government, consumer or other agencies who can provide the assistance the clients need. Such organization shall file annually with the State Disciplinary Board a report showing its rules and regulations, its subscription charges, agreements with counsel, the number of lawyers participating and the names and addresses of the lawyers participating in the service;
        ii. the sponsoring bar association for the lawyer referral service must be open to all lawyers licensed and eligible to practice in this state who maintain an office within the geographical area served, and who meet reasonable objectively determinable experience requirements established by the bar association;
        iii. The combined fees charged by a lawyer and the lawyer referral service to a client

referred by such service shall not exceed the total charges which the client would have paid had no service been involved; and,

iv. A lawyer who is a member of the qualified lawyer referral service must maintain in force a policy of errors and omissions insurance in an amount no less than $100,000 per occurrence and $300,000 in the aggregate.

3. A lawyer may pay the usual and reasonable fees to a qualified legal services plan or insurer providing legal services insurance as authorized by law to promote the use of the lawyer's services, the lawyer's partner or associates services so long as the communications of the organization are not false, fraudulent, deceptive or misleading;
4. A lawyer may pay the usual and reasonable fees charged by a lay public relations or marketing organization provided the activities of such organization on behalf of the lawyer are otherwise in accordance with these Rules.
5. A lawyer may pay for a law practice in accordance with Rule 1.17: Sale of Law Practice.

d. A lawyer shall not solicit professional employment as a private practitioner for the lawyer, a partner or associate through direct personal contact or through live telephone contact, with a non-lawyer who has not sought advice regarding employment of a lawyer.
e. A lawyer shall not accept employment when the lawyer knows or it is obvious that the person who seeks to employ the lawyer does so as a result of conduct by any person or organization prohibited under Rules 7.3(c)(1), 7.3(c)(2) or 7.3(d): Direct Contact with Prospective Clients.

The maximum penalty for a violation of this Rule is disbarment.

Comment

Direct Personal Contact

[1] There is a potential for abuse inherent in solicitation through direct personal contact by a lawyer of prospective clients known to need legal services. It subjects the lay person to the private importuning of a trained advocate, in a direct interpersonal encounter. A prospective client often feels overwhelmed by the situation giving rise to the need for legal services, and may have an impaired capacity for reason, judgment and protective self-interest. Furthermore, the lawyer seeking the retainer is faced with a conflict stemming from the lawyer's own interest, which may color the advice and representation offered the vulnerable prospect.

[2] The situation is therefore fraught with the possibility of undue influence, intimidation, and overreaching. The potential for abuse inherent in solicitation of prospective clients through personal contact justifies its prohibition, particularly since the direct written contact permitted under paragraph (b) of this Rule offers an alternative means of communicating necessary information to those who may be in need of legal services. Also included in the prohibited types of personal contact are direct personal contact through an intermediary and live contact by telephone.

Direct Mail Solicitation

[3] Subject to the requirements of Rule 7.1: Communications Concerning a Lawyer's Services and paragraphs (b) and (c) of this Rule 7.3: Direct Contact with Prospective Clients, promotional communication by a lawyer through direct written contact is generally permissible. The public's need to receive information concerning their legal rights and the availability of legal services has been consistently recognized as a basis for permitting direct written communication since this type of communication may often be the best and most effective means of informing. So long as this stream of information flows cleanly, it will be permitted to flow freely.

[4] Certain narrowly-drawn restrictions on this type of communication are justified by a substantial state interest in facilitating the public's intelligent selection of counsel, including the restrictions of sub-paragraph (a)(3) & (4) which proscribe direct mailings to persons such as an injured and

hospitalized accident victim or the bereaved family of a deceased.

[5] In order to make it clear that the communication is commercial in nature, paragraph (b) requires inclusion of an appropriate affirmative "advertisement" disclaimer. Again, the traditional exception for contact with close friends, relatives and former clients is recognized and permits elimination of the disclaimer in direct written contact with these persons.

[6] This Rule does not prohibit communications authorized by law, such as notice to members of a class in class action litigation.

Paying Others to Recommend a Lawyer

[7] A lawyer is allowed to pay for communications permitted by these Rules, but otherwise is not permitted to pay another person for channeling professional work. This restriction does not prevent an organization or person other than the lawyer from advertising or recommending the lawyer's services. Thus, a legal aid agency, a prepaid legal services plan or prepaid legal insurance organization may pay to advertise legal services provided under its auspices. Likewise, a lawyer may participate in lawyer referral programs and pay the usual fees charged by such programs, provided the programs are in compliance with the registration requirements of sub-paragraph (c)(1) or (c)(2)of this Rule 7.3: Direct Contact with Prospective Clients and the communications and practices of the organization are not deceptive or misleading.

[8] A lawyer may not indirectly engage in promotional activities through a lay public relations or marketing firm if such activities would be prohibited by these Rules if engaged in directly by the lawyer.

ATTACHMENT 20

RULE 7.4 COMMUNICATION OF FIELDS OF PRACTICE

A lawyer may communicate the fact that the lawyer does or does not practice in particular fields of law. A lawyer who is a specialist in a particular field of law by experience, specialized training or education, or is certified by a recognized and bona fide professional entity, may communicate such specialty or certification so long as the statement is not false or misleading.

The maximum penalty for a violation of this Rule is a public reprimand.

Comment

[1] This Rule permits a lawyer to indicate areas of practice in communications about the lawyer's services. If a lawyer practices only in certain fields, or will not accept matters except in such fields, the lawyer is permitted to so indicate.

[2] A lawyer may truthfully communicate the fact that the lawyer is a specialist or is certified in a particular field of law by experience or as a result of having been certified as a "specialist" by successfully completing a particular program of legal specialization. An example of a proper use of the term would be "Certified as a Civil Trial Specialist by XYZ Institute" provided such was in fact the case, such statement would not be false or misleading and provided further that the Civil Trial Specialist program of XYZ Institute is a recognized and bona fide professional entity.

ATTACHMENT 21

RULE 7.5 FIRM NAMES AND LETTERHEADS

a. A lawyer shall not use a firm name, letterhead or other professional designation that violates Rule 7.1.
b. A law firm with offices in more than one jurisdiction may use the same name in each jurisdiction, but identification of the lawyers in an office of the firm shall indicate the jurisdictional limitations on those not licensed to practice in the jurisdiction where the office is located.
c. The name of a lawyer holding public office shall not be used in the name of a law firm, or in communications on its behalf, during any substantial period in which the lawyer is not actively and regularly practicing with the firm.
d. Lawyers may state or imply that they practice in a partnership or other organization only when that is the fact.
e. A trade name may be used by a lawyer in private practice if:
    1. the trade name includes the name of at least one of the lawyers practicing under said name. A law firm name consisting solely of the name or names of deceased or retired members of the firm does not have to include the name of an active member of the firm; and
    2. the trade name does not imply a connection with a government entity, with a public or charitable legal services organization or any other organization, association or institution or entity, unless there is, in fact, a connection.

The maximum penalty for a violation of this Rule is a public reprimand.

Comment

[1] Firm names and letterheads are subject to the general requirement of all advertising that the communication must not be false, fraudulent, deceptive or misleading. Therefore, lawyers sharing office facilities, but who are not in fact partners, may not denominate themselves as, for example, "Smith and Jones," for that title suggests partnership in the practice of law.

[2] Trade names may be used so long as the name includes the name of at least one or more of the lawyers actively practicing with the firm. Firm names consisting entirely of the names of deceased or retired partners have traditionally been permitted and have proven a useful means of identification. Sub-paragraph (e)(1) permits their continued use as an exception to the requirement that a firm name include the name of at least one active member.