

A



CONVERSATION

About Legal Ethics and Social Media

**With Steven Bennett,
Marion Fish,
Bruce Green,
John McCarron,
Patricia Salkin,
and John Szekeres**

Edited by Gary Munneke



GARY MUNNEKE (gmunneke@law.pace.edu) is a Professor of Law at Pace Law School in White Plains, New York, Co-Chair of the NYSBA Law Practice Management Committee and a member of the Task Force on the Future of the Legal Profession. He is guest editor of this issue of the *Journal*.

Editor's Note: This issue of the Journal also contains articles on the challenges facing lawyers in transition ("Reflections on Transitions: Things I Have Learned," by Jessica Thaler), the demise of Dewey LeBoeuf ("When Brahmins Bumble: Dewey Really Care?" by Gary Munneke), and the problem of managing the actual cost of delivering legal services ("The Costs of (Inefficient) Legal Services Delivery," by Anastasia Boyko). These thoughtful pieces are intended to give readers some novel and interesting perspectives on contemporary practice management issues that impact all lawyers.

Panelists

Steven Bennett is a partner in the New York office of Jones Day, and is a frequent contributor to the New York State Bar Association *Journal*.

Marion Fish is a partner in the Syracuse, New York, firm of Hancock Estabrook, and Chair of the NYSBA Attorney Professionalism Committee.

Bruce Green is Louis Stein Professor of Law at Fordham University School of Law, in New York City, and Director of the Stein Center on Legal Ethics.

John McCarron is a partner in the Westchester firm of Montes & McCarron.

Patricia Salkin is Dean of the Touro Law Center, in Central Islip, New York, and an expert on government ethics.

John Szekeres is the Past Chair of the Electronic Communications Committee and a member of the NYSBA Task Force on the Future of the Legal Profession.

 Below is the first of two conversations on the inter-relationship among legal technology, ethics and practice management with leading thinkers in the field. In an area that is still evolving, many principles remain unsettled. For the past two years, the American Bar Association Ethics 20/20 Commission has struggled to define the parameters of ethical and professional behavior in law practice in situations involving computer and related technology. Although there are often no clear answers to the questions being raised, the pervasive existence of technology reminds us that all lawyers need to think about how they will use technology in practice and the pitfalls they might encounter.

This article is a condensed transcript of a program presented at the 2012 New York State Bar Association Annual Meeting titled "Technology in Your Practice: Trends, Tools and Ethics Rules," sponsored by the Committee on Law Practice Management, and co-sponsored by the Committees on Attorney Professionalism, Electronic Communications and Lawyer Assistance. It is a timely discussion of one of the most prominent areas of practice development today: the use of social media by lawyers. Although much of the attention in the legal press has focused on social media in the context of marketing legal services, this discussion makes it clear that other issues are equally important, and that social media can impact client-lawyer communications in a variety of ways.

Ethics and Social Media

John Szekeres: Social media has given us the potential to greatly expand how we interact with our community,

which is not necessarily local anymore. For a lawyer, this represents significant opportunities for networking and knowledge exchange and has created new areas for client representation. But, to take advantage of these opportunities, we must understand how these tools are used and potentially abused. Most importantly, as lawyers, we must be aware of the implications when these tools are used improperly.

Attorneys are governed by complex ethical rules and guidelines that regulate our professional conduct and speech. Internet-based technologies and communication tools have added a whole new dimension of complexity to how we advise our clients, represent them, and conduct ourselves. The issues raised by the use of social networking applications impact advertising, unauthorized practice, conflicts of interest, breaches of confidentiality – inadvertent or otherwise – privileged communications, attorney-client relations, and client expectations. For example, a person who was going through a divorce had an appointment to discuss certain issues with her lawyer, but she was pressed for time, so she requested that she meet with her lawyer via Skype to save her time traveling to her lawyer's office. The lawyer insisted on an in-person meeting with the client, and the client was very annoyed. How is this related to social networking? It's the need to adjust our behavior to the way society is evolving, how it communicates and how networks evolve.

Less obvious and more difficult to assess is the impact on your practice of not having a website or using LinkedIn, writing a blog, or participating in an online chat room or tweeting. Are you missing opportunities to gain new clients? Are you failing to meet client or potential client expectations? While you still have clients coming in the door in sufficient numbers, you may feel that you have not missed any opportunities, but by not using these tools are you failing to gain an understanding of how the tools are used or abused so that when necessary you can effectively represent your clients? How do your existing clients perceive you and your practice?

In the early days of the telephone, it was seen as unprofessional to have a telephone in your office. Having a telephone, it was thought, would take away time from the lawyer's ability to stay intellectually focused on the law. In fact, that observation was probably true, but today you could not function in your practice without a phone. The same scenario played out with computers in law offices in the '90s. Computers were a tool for the secretary. No lawyer would type their own brief. Today, most lawyers have computers on their desks, and they

send and receive dozens if not hundreds of emails a day. Typing your own documents certainly has taken time away from focusing on the higher level work, but it has brought efficiencies as well.

Question 1 – Government Use of Social Media

Szekeres: My first question involves government practice. If a governmental entity allows comments on its website, or a Facebook or LinkedIn page, can the governmental entity put in place a moderator to edit screen comments when a person starts making inappropriate comments?

Patricia Salkin: If you represent a municipality, and they want to set up social media sites, the first thing that you have to be concerned about is setting up a policy before they start the site, because people have First Amendment rights, particularly when it pertains to speaking to their government and about their government. So you have to ask whether you want to allow comments to be posted on your site. But once you allow comments can somebody say, “The Mayor is a jerk”? Can somebody use foul language? What kinds of comments might be appropriate or inappropriate? If you don’t have a policy, somebody is exercising discretion if they pull down those comments, and then you might be cutting off somebody’s free speech. Municipalities often ask their municipal attorneys to be their site moderator. Say no. You don’t want to be the person doing that for the municipality. And before somebody can get onto your organization’s Facebook page, require people to register. Do you want the members of the public to provide their names, their address, or any other information? Sometimes, depending upon what the conversation is about, if you’re using it to engage public participation, you might, because that might demonstrate

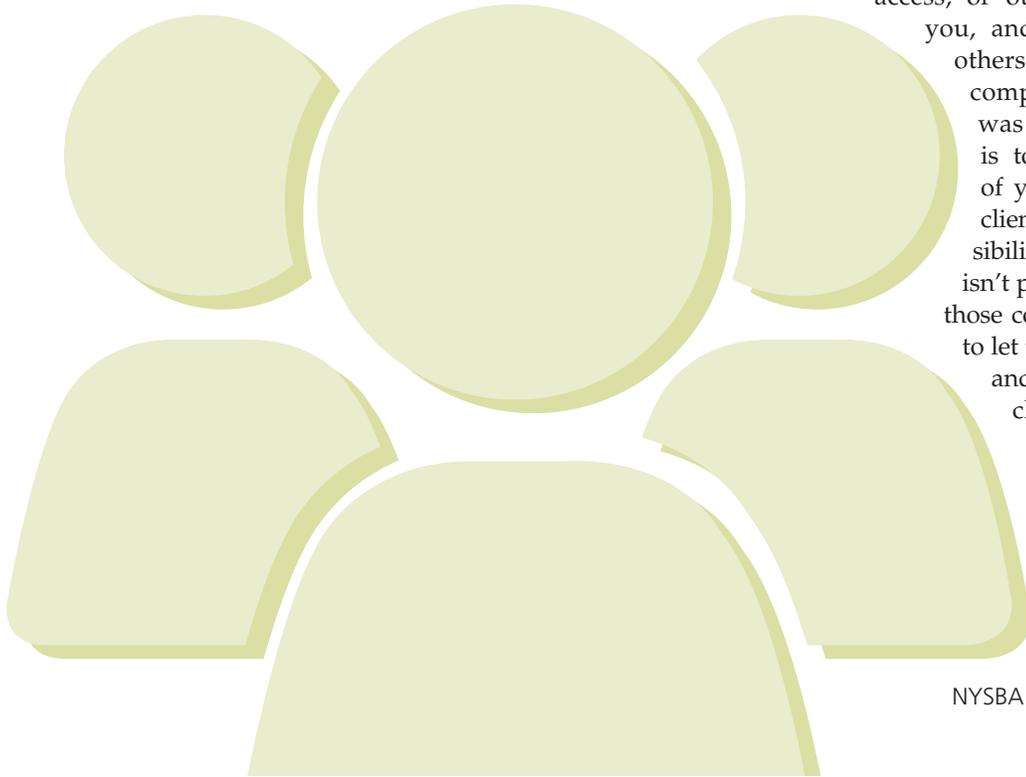
that members of the public did participate. But the question is what public? The public impacted by the project? Or anybody out there in cyberspace who wants to come on board and make a comment about a proposed development project, or some other public hearing that the municipality is trying to collect information on? However, if you collect that information, does it become a record? And what are your obligations? So any time your client is a governmental entity using the social media sites, there are lots of questions.

Question 2 – Expectations of Confidentiality

Szekeres: Can one have a reasonable expectation that when using any of the social media tools or email that attorney-client communications will remain confidential, and if divulged, whether the confidentiality of the communication is going to be preserved? What about emails – for example, clients using their employer’s computer system to communicate with their lawyer? What are the client’s expectations? And what about using email outside of the place of business? Do Internet connections receive the same level of regulated protections that telephone and fax communications receive?

Bruce Green: Lawyers have an obligation to preserve the confidentiality of their communications with clients. That’s why you don’t chat with your clients in the elevator when there are other people there, or at the table in the restaurant when there are other people listening. An ABA ethics opinion in the last year reminded lawyers that although you may have measures to make sure that emails in your office are secure, encrypted or otherwise protected, the same may not be true of the client. The client may be using a workplace computer or smartphone owned by the employer to send emails, or using a computer in a divorce matter to which the spouse has

access, or otherwise corresponding with you, and it’s not protected because others might have access to those computers. What the ABA said was that part of your obligation is to preserve the confidentiality of your communications with the client if there’s a reasonable possibility or likelihood that the client isn’t protecting the confidentiality of those communications. You also have to let the client know about the risks and not communicate with the client if those risks are present. For example, an employer may seize the employee’s computer at the workplace or access a personal email account through the employer’s server, including those that might’ve



been used in communications with the lawyer, and seek to use them in litigation. Cases around the country have varied about whether that is a waiver of attorney-client privilege, but opinions in New York have found that where the employee had been put on notice of the

In the early days of the telephone, it was seen as unprofessional to have a telephone in your office.

employer's policy the employee could not claim the attorney-client privilege. So the lesson from those cases is that lawyers have to be cognizant of the risks when they're communicating with clients and take some measures to prevent them.

Steven Bennett: The basic obligation of competence requires lawyers to know the capabilities of these systems in order to provide guidance to clients. The client ultimately owns the privilege and can decide whether he or she wants to yell across the room to you, fully understanding there probably isn't much privilege associated with that kind of communication. But what if a client doesn't understand the employer's policy, for example, the Beth Israel case (*Scott v. Beth Israel Medical Center*, 17 Misc. 3d 934, 847 N.Y.S.2d 436 (Sup. Ct., N.Y. Co. 2007)) in New York, where a doctor sent messages from a work computer to a lawyer about workplace conditions in an action against the employer. The court ultimately says that the employer owns the computer and the employer has told the employee that he has no expectation of privacy in the computer system; therefore when you talk to your lawyer via that system, you do not maintain the privilege. If the lawyer understands the situation and doesn't remind the client about it, shame on us.

John Szekeres started by asking whether a lawyer can Skype with a client. Can you send them a tweet? The answer is: Not if you want to assure privacy under those circumstances – or at least tell the client that there could be a problem. Opinions about email go back a while, and they basically say that for email there is a reasonable expectation of privacy. Even though it is very easy to deconstruct email, because it's going over the Internet, the fact it's unlawful to do so without consent gives rise to a reasonable expectation of privacy. But perhaps this is not so in the case of tweeting or going to a Starbucks WiFi hotspot where everybody can access it. It is awareness more than anything else.

Marion Fish: Is there something different about Skype as far as confidentiality compared to other media?

John McCarron: Telecommunications regulations are much stricter than those for phone lines. Although antiquated, it is the same reason why there are a lot of taxes on your phones and not on your Internet service. Skype just has a different level of regulation . . .

Szekeres: But the question is what kind of peril do you put yourself in using Internet communications as opposed to using the telephone?

Bennett: Right. The Electronic Communications Privacy Act was written over 15 years ago, well before any of these technologies existed. So if you're making predictions about whether ECPA will be applied in the case of Skype, that is just a guess.

McCarron: As a practical and technical matter, when it comes to BlackBerrys, iPhones, and devices like that, whether they give you the phone or you bring it yourself, the server doesn't care. For example, BlackBerry offers a corporate environment called the BlackBerry Enterprise Server, which pretty much takes over control of your phone. It runs all the security on your phone, can do lots of nifty things on your phone, limit what you can do on the phone, set your home page, move your icons around. The BES can back up your data and has access to pretty much everything on the phone. So it becomes a big security issue, which is why some people still walk around with two BlackBerrys.

Bennett: If the employer claims that it owns the computers and communication systems, and asserts the right to review communications at any time, giving employees no reasonable expectation of privacy, then, to a degree, the employer owns that information – on both the plus side and the negative side. If somebody is using the system to harass somebody else, or to perpetrate a crime, the company may be responsible, because it owns the information; and in the event of a discovery request for all the data in such and such a category, the question then becomes, Does that include all these g-mail accounts and all the rest of that material? So it's a tough question for an employer to decide what to do.

Question 3 – Breaches of Confidentiality

Szekeres: Let's talk about inadvertent breaches of confidentiality. You accidentally send out an email with some client confidential information to the wrong email address, or you post client intake forms or other confidential material on your firm's website. So what about that? Courts are generally unwilling to recognize a reasonable expectation of privacy. Is that right? When people willingly post?

Green: I guess it depends on what the facts are. Are you talking about inadvertent emails? How many people here have never inadvertently sent an email to somebody? I do it all the time. Or do you mean actually posting something on the Internet or a blog or website?

Szekeres: I think they're two different issues. I am referring to posting something inadvertently. You think you're putting up one thing, and it's actually something else.

Green: You are asking about whether the information is privileged or not. It is one thing to inadvertently mail or fax something to one person or a small group. It's another thing to disseminate it to the entire world. I don't know how you put the cat back in the bag. Maybe a court is going to say, we will not let someone make evidentiary use out of it. But even if they say that, it's still out there. And so you've hurt your client, and the whole point is to not do that. In the more conventional case of an inadvertent email, what do you do as the recipient? Rule 4.4(b) of

the ABA Model Rules of Professional Conduct says that if you receive something you know was sent inadvertently, or reasonably believe or have reason to believe, you have to give notice to the person who sent it so they could then take whatever measures they need to take. Some court decisions say that is not enough.

Bennett: From a supervisory perspective, you may be totally aware about this stuff, but your juniors, paralegals and secretaries might not quite get as much of this as you think, and it can be a problem for the folks who are running the firms. For example, where employees didn't manage to perform the redaction properly, so when you pasted the redacted document into another form, you included information that should not go out. And the folks responsible for electronic filing are often very, very junior, or in some docket department. And they're not really inculcated with these ethics values.

When you tell them this thing has to be filed by 5:00, they make it happen, and only later do some of these security issues come up. Concerns about data security apply to businesses in general, but they also apply to lawyers, and so learning this technology and thinking about best practices is just essential in the modern technological era.

Salkin: Some of the responses here are blurring the line between what you're using for business, and the question of whether or not lawyers and people that work with us and for us can have a private life. So, how do you use your firm Facebook and LinkedIn pages versus how you use a personal account? I have seen people comment on their personal Facebook page observations about what they see in the law office, including comments about clients, or witnesses, and fellow employees. They may not attach the person's name but if you knew what was going on, you could figure it out. They might think they can say whatever they want in their private life. I'm not so sure that you can. And I don't think that the younger generations appreciate the difference.

Green: The important point is that you can violate client confidentiality not only by including names and other information, but also by just talking about something in a way



that someone can connect it to a client, and you have to remind these young lawyers about it.

Fish: I also wanted to bring up the point that these are recording devices and video devices, and how that might affect your personal practice. When I meet with a client or I have a private conversation with somebody, I ask them to turn off their phones. And some people are more aggressive when I ask them to leave the phones outside the room, but I know that these recordings have been allowed as discovery, and you don't even know you're being recorded. So as lawyers we also need to think not only about what we're doing on our keyboards and the screen, but also that we're carrying around videos, cameras and voice recordings.

McCarron: Some law firms have a "check your device at the door" policy. They do not want you blogging or Facebooking – especially about work – between the hours of nine to five.

Bennett: It is a Brave New World.

Szekeres: Courthouses routinely require you to leave your electronic devices outside, because even though people are not supposed use recording devices in court, it is possible to record the whole proceeding on a BlackBerry.

Question 4 – Metadata

Szekeres: One of the biggest security dangers today is the metadata imbedded in Word documents. It does not take a great deal of knowledge to go in and ferret out. The safest way to deal with this problem if you do not know how to go in and turn the settings on in Word, is to just print the document, scan it into an image in, and then email the image to the recipient. It makes it difficult if you're trying to search, because the data in the file is no longer searchable. You can also convert your Word documents into text-searchable .pdfs, but creating a pure image protects you.

Green: So if you have an unsophisticated opposing counsel, is it okay to search the metadata in the drafts they send you?

Bennett: There are ethics opinions on that subject – some to the effect that it is devious to do so without indicating to the other side that you've found something. This is in line with the basic ABA rule on inadvertent production of information, to the effect that you should notify the other side. So it would be inappropriate if you found something in the metadata and failed to tell the other side – that would be inappropriate.

Szekeres: And yet there have been some pretty significant situations where the metadata buried in the Word document would become sort of the focal point . . .

Bennett: Oh, there's no question with metadata, you have much more powerful information than you would ever get out of the paper. You know, for example, when things were created, when they were modified, who made comments, exactly what those comments were.

When the government uses Facebook or LinkedIn, are they considered records for purposes of Freedom of Information requests?

Green: But, I mean, in litigation you want to get things in their electronic form. You want . . .

Bennett: You want it searchable.

Green: That's different from when you're corresponding in a transaction or litigation or whatever with counsel. You are not supposed to make evidentiary use of their letters to you. The New York State Bar Association has said it is uncivil, unprofessional, to review metadata. Other bar associations have said it's the problem of the sender.

Szekeres: I have heard recently that certain firms have turned over discovery material with no metadata, and the judge has turned around and said, you can't do that.

Bennett: One of the classic cases on this subject involved somebody taking tens of thousands of sheets of paper, throwing them up in the air, reshuffling them and handing them to the other side as document production. You're not supposed to do that. The rules are pretty clear – you're supposed to keep them as they were originally kept, or organize them according to categories. If you give me a database in paper form, it's utterly useless. Reams and reams of lines that I can read, but I can't analyze. Judge Waxse, in the District of Kansas, said that analyzing this information is key to the case. You have to make it available to the other side in that same analyzable form. Metadata allows that analysis, but a lot of other metadata is just garbage – the font, the margins. Who cares? So it becomes a question of whether you can make some showing that the particular metadata that you're talking about is likely to be useful.

Question 5 – Facebook and FOIL

Szekeres: When the government uses Facebook or LinkedIn, are they considered records for purposes of Freedom of Information requests? How should the government prepare to comply with FOIL requests when they don't host these sites?

Salkin: We don't have an opinion in New York on that, but the Florida Attorney General, responding to a question about Facebook pages, said that they are records. Facebook is not hosted by the municipality or governmental entity. To be on the safe side, many municipal attorneys now advise their clients to regularly make copies and retain copies, because we are not exactly sure

When does posting something on a blog or participating in a chat room or Skyping cross over from advertising into solicitation?

whether or not it is the municipality's responsibility to provide these pages.

McCarron: Interestingly, services have popped up which allow for the archiving of social media pages. Information will be archived on a daily or weekly basis, by taking a snapshot of everything in your Facebook, Twitter, or other social media – whatever the municipality or the company is using – in order to preserve it for e-discovery later on.

Question 6 – Blogging

Salkin: I was hoping that we might be able to talk about lawyers and academics – like myself – who set up blogs to distribute information, and people contact you with questions. We need to be sure not to create the appearance or the belief on the part of the questioner that there is an attorney-client relationship. I find this problematic on my blog, because I allow comments in the hope that people will share information about cases in other states, but I often get legal questions as well. I've tried to be polite and respond, but my pat response now is: Thank you for looking at the blog. Thank you for your question. I'm not engaged in the private practice of law. I can't answer your question. I'm not licensed in Pennsylvania or Kentucky or California. You really need to consult an attorney in that state. When it involves people from New York or New Jersey, where I am licensed, I have to dance around that in another way, but I really avoid answering the questions, even if I think I know the answer, because I don't want the appearance that I'm giving legal advice. I think it's more problematic for law firms that have blogs, because the firms promote themselves through their blogs as a way to attract clients.

Szekeres: It is not just the law firm. What if an associate is at home blogging and on their profile they show where they work? If the associate answers questions or comments on legal matters, do they represent the firm when they speak? And do informal online communications give rise to conflicts of interest that affect the whole firm?

Green: And how does a prospective client become an actual client? Model Rule 1.18 defines prospective attorney-client relationships and establishes a duty of confi-

dentiality to prospective clients. A prospective client is someone who seeks legal assistance. Generally, when someone gives you unsolicited information, it doesn't create an attorney-client relationship, but a lawyer who invites emails or questions on her blog basically invites the creation of a lawyer-client relationship, and the emails create a duty of confidentiality.

Salkin: Some people want to post their comments on the blog, and I moderate my blog. I do not allow every comment to be posted. I'm not a governmental entity, so I don't have to do that, but I have emailed people off-line to the effect that I'm not posting your comment because you've provided personally identifying information about people and situations. I'm not sure that you really intended to post something that everybody could read. I'm not sure if you were trying to message me personally, or if you wanted this posted.

Bennett: Even if you're not practicing law, you may be subject to disciplinary restrictions in another jurisdiction by virtue of these sorts of communications. I think it starts by being as clear as possible as to where you are licensed. I'm only licensed to practice in New York, so you can assume that I have no intention of practicing outside New York without authority. I also think that there's some value in being clear that whatever you put up on a blog is for informational purposes only. It's not a solicitation of an attorney-client relationship.

Green: One of the questions is whether you plan to pick up clients in other jurisdictions. If you're a New York lawyer, but someone in Virginia who reads your blog or website is willing to hire you, and you're willing to do work for them, then Virginia is going to say that you're subject to Virginia advertising rules and unauthorized practice of law, because you're practicing law in Virginia, even though you are physically in New York. Conversely, if you're blasting this stuff to the world from New York, but you're only representing New York clients, I don't think Virginia is going to care too much.

Szekeres: The great thing about blogging, wikis, Facebook, and websites is that suddenly you're projecting yourself far beyond your locality.

Bennett: Not to mention the fact that there are circumstances where you know the access point is someplace else. A client walks into the firm's office in Beijing and says there's a problem in New York. Can you help? The Chinese lawyer on site is the first point of access, but the matter really is a New York matter, and it's perfectly appropriate to forward the problem to the New York office. In fact, that's what large law firms were built to do – to refer internally to get the proper service.

Question 7 – Advertising or Solicitation?

Szekeres: When does posting something on a blog or participating in a chat room or Skyping cross over from advertising (which is allowed) into solicitation (which is prohibited)?

Bennett: The key differentiator according to the Model Rules of Professional Conduct is that real time in interactive communication is treated as solicitation, but sequential communication is treated as advertising. If it is in real time, it's the moral equivalent of calling somebody up on the phone and saying, "Please hire me." It's interactive. You're asking the person to respond. And so that analogy can be applied to things like Facebook, in which somebody interjects themselves into a situation and asks for a response in real time.

Green: New York has a kind of odd definition of solicitation. The standard notion is that advertising involves billboards, ads, television, and other media, and solicitation is reaching out to some individual by telephone or in person. New York defines a lot of what we usually think of as advertising as solicitation if it involves targeting particular individuals. That doesn't mean it's impermissible. It just means it's defined differently, and subject to a stricter set of rules.

Question 8 – Friending

Szekeres: When is it permissible to "friend" somebody during the course of a litigation or any sort of matter where what you're trying to do is friend an adverse witness for purposes of learning information that could be used to impeach that witness?

Salkin: You can't do it. But can you friend a judge? It's another variation on the appearance of campaign contri-

butions. Now it's even more in your face when people can see that the lawyer appearing before the judge is friends with the judge on Facebook. What about people appearing before quasi-judicial bodies like zoning boards of appeals being Facebook "friends" with board members, or connecting with them on LinkedIn? It's a lot different, because there are relationships in the community with lots of different people, but when a relationship is memorialized on the Internet for people to see, it somehow rises to a different kind of appearance.

Green: There are a lot of judicial opinions in the federal district court in New York that allow some use of deceit in evidence gathering, and I'm not sure why those opinions wouldn't apply to the social networking context. I'm not advocating that people should engage in "deceptive friending" – pretending to be someone who you're not – but if you're honest about who you are, then none of the opinions forbid it.

Bennett: City Bar Opinion 2010-2 says it is permissible to use your real name and profile for friending requests. State Bar Opinion 8-43 says you can look at social media information freely even if you're not a friend, and you do not have to friend anybody in order to get it. You can go onto an adversary's website, right, and make copies of information on the site. You can go on a website and buy something in your own name. It may be different, however, to pretend to be somebody you are not. ■

Like what you're reading? To regularly receive issues of the *NYSBA Journal*, join the New York State Bar Association (attorneys only).