Before You Use Social Media, Do You Know the Ethics Rules Involved?

By Natalie Sulimani, Esq.

Social media is a cost effective way to promote your firm, and it helps you connect with potential clients. Before you embark on a social media campaign, let's explore the ethical considerations.

In the case where an attorney or law firm uses social networking as a way to market the practice, the traditional attorney advertising rules still apply. If anyone has ever attended my CLEs regarding social media and ethics, I have started the class by repeating the same line: Technology changes but the ethics rules do not change as quickly, and the rules are applied the same online and offline.

First, make sure you reacquaint yourself with Rule 7 of the Rules of the Professional Conduct. Given the fast pace of the Internet, it may seem burdensome or difficult to abide by these guidelines. My suggestion is to use your firm's website, which is probably already compliant, as the underlying platform for any advertising you may do online.

When setting up your social media for online advertising, first you must decide on your "handle" (in the case of Twitter) or username. It is not advisable to use a name that may be misleading or promise a particular outcome. So, when choosing your handle or username, while your firm name or personal name may be appropriate, be careful if you choose to use a name like "facebook.com/alwaysgofree" as this might create an expectation in a potential client.

Once you have chosen your name and signed up for the account, your next step is usually a description of who you are, what your firm does, etc. You want your message to be unified and cohesive. To comply with the Rules, it should neither contain statements that are deceptive or false nor should it reference yourself as an "expert" unless you do, in fact, fall into that narrow category, e.g., passed the patent bar. On that note, a potential pitfall in LinkedIn is filling out the Specialties section of your profile. According to the Rules, you cannot call yourself an expert unless you have specific credentials, e.g., passed the Patent Bar. So, I would suggest skipping this section altogether and instead fill out the "Skills and Expertise" section.

When utilizing peer or client recommendations post a disclaimer such as *Prior Results Do Not Guarantee Outcome* in a prominent position. Also, get your client's consent in writing that they should never mention an ongoing matter. Lastly, review all recommendations and make sure they accurately portray what you did for the testimonial parties.

Now you are ready to begin the task of marketing yourself through social media or to a lesser extent just interacting with the social stratosphere at large. However, it is vital that you keep in mind and guard against not making representations that will cause unrealistic expectations or provide a false impression. Usually, this takes the form of excited utterances after a great win. Or, perhaps more you had a bad day at court and feel the need to tweet to the world what a <&*%*^*$> the judge was. DANGER! Attorneys cannot speak ill of a judge in public. Cooler heads should always prevail, especially in social networking.

Given the brevity of tweets and the lack of real estate on social media sites, it is difficult to include the necessary disclaimers. To avoid problems is to route your tweets, status updates, etc. to your site where you have enough real estate to disclose what you need to disclose such as:

- Attorney advertising which is prominently displayed on your website; and
- *Prior Results Do Not Guarantee Outcome* especially if you are talking about a recent win.

Finally, let's talk about Groupon. Now I know what you're thinking, but it is probably the same thing attorneys thought when TV advertising began. Indeed, it has worked for a handful of brave attorneys who were willing to try.

In an opinion from December 13, 2011, the New York State Bar Association (NYSBA) weighed in on marketing legal services through a daily deal site. Essentially, an attorney may offer his or her services through such a site provided the advertising is not misleading or deceptive. The attorney also must make clear that there is no relationship formed until the proper checks are performed. If the lawyer is unable to provide services, a full refund must be made. If the client terminates representation, the refund is subject to the *quantum meruit* claim. The opinion goes into greater detail of non-lawyers receiving referral fees. In this case, NYSBA opines that the website is taking a fee for advertising, and the website, therefore, has no individual contact with the client. You must also consider the possibility that your advertising campaign on a daily deal

{ *See* **SOCIAL MEDIA** *on page 6* }

NEW YORK COUNTY LAWYER

Published for
New York County Lawyers' Association
14 Vesey Street
New York, NY 10007
(212) 267-6646
www.nycla.org

Barbara Moses
President

Sophia J Gianacoplos
Executive Director

Toni Valenti
Director of Marketing & Membership Development

Ariella Greenbaum
Editor
Senior Communications & Social Media Manager

Published by
Apogee Publications
6528 Greenleaf Avenue, Ste. 219
Whittier, CA 90601
(562) 698-3424

Publisher
Mel Sturr

Accounts Director
Kathleen Pishotta

Art & Design Adjudicator
Aude Cabaldon

Editor
Nicole Millman-Falk

For advertising information, call (888) 371-4933.

Subscription • *New York County Lawyer* is published monthly (except January and August) for $10 per year by New York County Lawyers' Association, 14 Vesey Street, New York, NY 10007.

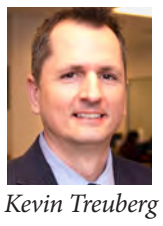
Custodial Self-Collection During Discovery—Defensible Process or Spoliation Guaranteed?

An interview with Mark Sidoti, Esq., and Kevin Treuberg, Esq., moderated by Matthew F. Knouff, Esq. CIPP/US, CEDS

It is without debate that electronic information is the evidentiary currency in which lawyers now trade. E-mail is the predominant form of communication in the business world. Individuals across a broad range of demographics are using social media, webmail accounts, mobile instant messaging, text messaging, and other forms of digital communication with increasing frequency. Sales of mobile devices are skyrocketing, and the use of cloud storage for information continues to proliferate. What does this electronic explosion mean for you as counsel? Well, for one thing, gone are the days of simply telling your client to go through her filing cabinet and pull all the documents related to "Matter X." The digital footprint of even a single custodian could encompass hundreds of thousands of e-mails and other documents spread out across numerous devices, storage media, and online repositories. Unfortunately, with increased data come increased costs. How can you ensure that you find all of the documents you need for your case without bankrupting your client in the process?

Though practically it's not always the case, common sense tells us that those who created and/or maintain documents that may be relevant to a particular case are likely to be in the best position to locate those documents. Absent very unique circumstances, your client is always going to play some role in the collection process during discovery. However, what is the full scope of that role? Having the client assist with the identification and/or harvesting of potentially relevant information is often referred to as self-collection. On its face, the notion that a client would be responsible for rooting out his or her own documents for his or her case brings to mind an impressive array of latent pitfalls. Does self-collection present too much temptation for custodians to delete unfavorable evidence? Even if acting in good faith, doesn't counsel run the risk that custodians may overlook, alter, or delete relevant documents? How can you balance the importance of maintaining the integrity of your discovery efforts against the need for controlling the costs associated with over-collection?


Mark Sidoti


Kevin Treuberg

We will address these questions with the help of two well-known experts: Mark Sidoti, Director of Gibbons P.C.'s Products Liability and Business & Commercial Litigation Departments and Chair of the firm's E-Discovery Task Force, and Kevin Treuberg, former Counterintelligence Special Agent and current Director of Forensic Services at Complete Discovery Source (CDS) with more than 20 years of forensics experience.

KNOUFF: *There have been several opinions in recent years where judges have taken a hardline against custodial self-collection, but yet we're talking about the notion that self-collection can be performed in a defensible manner. Is there some type of common behavior that you see across these cases that highlights self-collections being conducted improperly?*

SIDOTI: The primary concern of the courts appears to be lack of attorney oversight of the process. This goes for both in-house and outside counsel. Mistakes will always be made, particularly where custodians are asked to independently undertake a process with which they are not familiar, involving legal issues the significance of which they do not understand (or that may not be important to them), and in some cases, they may have a personal interest or stake in the outcome of the case. However, the courts are particularly intolerant of such mistakes when custodians are "left to their own devices," and the facts support a conclusion that counsel—who should understand these issues and risks—failed to monitor and assist in the process closely enough.

KNOUFF: *The term "self-collection" gets thrown around a lot and has many meanings. What does self-collection mean to you?*

SIDOTI: The meaning of self-collection varies with the circumstances and the clients from whom we work. From a corporate client standpoint, self-collection most often refers to the company's undertaking to locate and collect its electronically stored information without any (or any significant) assistance from counsel or a third-party service provider. On an individual level, self-collection connotes an individual custodian's undertaking to locate and collect ESI from sources within that custodian's control, again absent significant assistance from third parties, including others at the company for which they work. Under either of these primary definitions, the term self-collection connotes a process

{ *See E-***DISCOVERY** *on page 7* }

E-DISCOVERY

Continued from page 2

that is generally autonomous, unsupervised, and unregulated. This connotation may be altered by a demonstration of appropriate safeguards (such as auditing procedures carried out by counsel) and collection methods (such as reliable and forensically-sound, remote collection tools).

TREUBERG: To me as a forensics practitioner, self-collection means using the proper tools and techniques to collect relevant data in a manner that changes the least amount of metadata (if any). As the sophistication of clients and case teams becomes more prominent, it becomes easier to advise and coach self-collection methods.

KNOUFF: *So each of you believe that self-collection, if performed with the proper safeguards and techniques, can be an appropriate means of collecting electronic evidence. If this is the case, why is self-collection such a controversial topic?*

SIDOTI: I think because it highlights one of the key conflicts in the e-discovery landscape—the tension between cost savings (even if only perceived) and conducting e-discovery activities in the most thorough and appropriate manner. Many companies believe that costs can be minimized when they undertake collections on their own, without the assistance of outside service providers. While this may be true in the short term, when mistakes occur, the cost tables may be turned. This is why regulated and careful self-collection is essential.

TREUBERG: I agree with Mark. It's a controversial topic because there will always be the argument of cost versus risk. For example, a client may decide not to engage in self-collection when the matter is a high-stakes government investigation, whereas self-collection may be used when that same client is conducting an internal investigation. However, in both examples, it is certainly recommended that advice is sought prior to collection.

KNOUFF: *Sedona Conference Principle 6 states: "Responding parties are best situated to evaluate the procedures, methodologies, and technologies appropriate for preserving and producing their own electronically stored information." By corollary, would it be fair to say that individual data custodians are in the best position to know where their documents reside. Does this notion favor self-collection?*

TREUBERG: I agree with the notion that individual custodians are in the best position to assist in identifying where relevant data may reside. However, the actual act of collecting identified data still needs to be done in a manner that ensures the preservation of relevant metadata and gives counsel the ability to indicate the original source location of the data.

SIDOTI: It can be argued that to some extent this principle applies to custodian-level collection activities, although I believe the principle was directed at litigants generally ("parties") and was meant to be construed as applying to the collective efforts of a party in making preservation, collection and production decisions. In fact, the Comment to this principle specifically references the "typical" production process and notes that, typically, "lawyers supervise the collection of relevant information from custodians and other sources." Comments 6.e and 6.f also provide a detailed discussion of the need to carefully select, manage and document the collection process, and the obligation of counsel to supervise the collection process. So again, while custodian self-collection may be permissible under Principle 6, it must be conducted in a defensible manner and generally under counsel supervision and guidance.

KNOUFF: *In* In re Hawaiian Airlines, Inc. v. Mesa Air Group, Inc., *Mesa's executive vice president and CFO was found to have intentionally deleted various documents that were relevant to the proceeding. This behavior was attributed to Mesa and an adverse inference sanction was issued. As a practical matter, is it really possible for counsel to prevent individual bad actors when a collection is underway?*

SIDOTI: It may not be possible to avert all instances of bad conduct when custodians play a role in the collection process, but I do not think the case law requires perfection (here, or anywhere else in the world of e-discovery). Litigants find themselves in a sanctionable situations when they fail to take fundamental steps which could have prevented the data loss, such as interviewing custodians (particularly those assisting with or engaging in self-collection) regarding their personal preservation and deletion practices, and recent deletion activity and the like, or in failing to pursue the existence of documents which should, under company or individual protocols, exist within the custodians' document repositories. Too often, an individual's problematic practices, or even overt bad acts, are not discovered or probed by counsel until a witness is under oath describing activity that cannot then be undone. This situation needs to be avoided at all costs, and sometimes it is as simple as asking your collecting witnesses some simple questions about their data management practices.

TREUBERG: Bad actors are, unfortunately, a fact of life. Short of seizing and imaging all of the computers and servers, a certain level of trust is necessary between the case teams and clients.

KNOUFF: *When a legal hold notice is sent out, counsel relies on individual custodians to properly preserve documents. This is a common and relatively uncontroversial practice. Isn't empowering an individual to comply with a legal hold equivalent to expecting them to adequately self-collect?*

SIDOTI: No. Legal hold notices generate less controversy because fundamentally, they are simply advising a custodian to not allow the deletion or alteration of usually a wide range of targeted documents. On a custodian level at least, this is not a particularly difficult or confusing directive: "Just don't discard anything." Collection, on the other hand, involves far more judgment and discernment regarding the types of documents to be collected and how to go about that process. Thus, it entails expectations that exceed those embodied in the legal hold process and should not be equated with it.

KNOUFF: *The importance of cooperation cannot be overstated, but should a party disclose to opposing counsel that it intends to use self-collection techniques?*

SIDOTI: While this is a controversial issue, unless there is a specific cost or other concern, especially if the concern is mutual, that should be discussed with opposing counsel, I do not believe there is an obligation to disclose to an adversary that self-collection has been or will be undertaken. This is consistent with Principle 6 of the Sedona Guidelines and supporting case law. Of course, when there is a good faith reason to believe that evidence has been (or will be) spoliated, it may be necessary to disclose the specifics of the intended or undertaken collection process to one's adversary.

KNOUFF: *Is it important to make a distinction between a custodian self-identifying potentially relevant documents and a custodian performing the actual physical collection of documents herself?*

SIDOTI: Yes. Self-identification is quite common and can be very helpful, particular in today's world where custodians often possess multiple sources of data. Knowing whether relevant information is stored on a single hard drive, as opposed to several other sources such as an iPhone, iPad, thumb drive, or cloud-based repository, obviously guides the collection process. However, as most IT professionals know, the simple process of accessing ESI on a hard drive alters the document metadata, which can lead to issues in some cases. Moreover, improper collection techniques can result in the failure to retrieve relevant ESI.

KNOUFF: *I am a custodian and my lawyer has asked me to identify some documents and e-mail them to her as attachments. What real damage can I possibly do to my documents in this case?*

TREUBERG: When this occurs, the metadata of the files can be altered (e.g., author field, date created, date accessed, etc.). In addition, if it isn't documented, information indicating the original source location of the data may be lost. Original source location can be extremely relevant and assists in the verification of data integrity which supports admissibility.

KNOUFF: *Facebook has a feature where a user can "Download a copy of your Facebook data." Can this feature work as a self-collection tool?*

TREUBERG: As of this discussion, this specific feature on Facebook has many limitations. Such limitations include the inability to capture video data and a user's posts on other user accounts "walls," or "'timelines."

KNOUFF: *How does self-collection apply to mobile devices and webmail? Is there any type of data source that should never be included in a self-collection protocol, or is everything fair game?*

TREUBERG: Each data point that is to be considered for self-collection should be evaluated individually and the following questions should be asked: Is this data point relevant to the ongoing matter? Is the data I am looking to collect replicated to another system (e.g., a corporate e-mail account that is present on a smartphone and replicated to the corporate mail server.)? Do I have the proper tools and "know-how" to collect this type of data (e.g., the collection of data from mobile devices)? Will my efforts cause the alteration of the data, thereby opening the door to accusations of spoliation?

KNOUFF: *Everyone seems to be buzzing about DropBox, SkyDrive, GoogleDrive, and other document sharing applications in the cloud. Some are even promoted as viable tools for practice management. However, are these viable tools for self-collection?*

TREUBERG: It is always best to collect the data from its original location. Most of the cloud solutions replicate from a certain location on a Mac or PC, but some are the actual "source" of the data. I see using cloud based solutions as more of a way to deliver data than a tool to support self-collection.

Knouff will continue this conversation via a webinar with Mark Sidoti and Kevin Treuberg on Tuesday, April 8th at 11 am EST. Discussion will include actual tactics and strategies for self-collection, sanctions cases such as *Green v. Blitz U.S.A.,* and how to avoid specific mistakes, the proper documentation to create and maintain during a self-collection process, how to verify that tasks were properly completed, degrees of culpability, future developments, and more. E-mail webinar@cdslegal.com to receive credentials for the teleconference.

Matthew F. Knouff, Esq., is General Counsel and E-Discovery Counsel with CDS, an award-winning, global provider of defensible e-discovery services and technologies headquartered in New York City. CDS is a benefit partner of NYCLA and provides a vast array of forensics, e-discovery and other legal technology benefits to NYCLA members.