5-1-2014

Discovery of Social Network Data in Litigation

Jeffrey Brian Richter

Discovery of Social Network Data in Litigation

Jeffrey Richter

I. Introduction

The advent of the digital age and its subsequent proliferation have rapidly reshaped society, forever altering how individuals interact with the world and one another on a daily basis. Social media in particular has significantly transformed societal norms, as people the world over have been forced to adapt to constantly changing technology and the consequences that accompany it. After breaking down the barriers of nearly all facets of everyday life, it is of no surprise that social media has now infiltrated the confines of the courtroom, and in particular civil litigation. While individuals take full advantage of social media sites to voice their opinions and share the minutia of their daily lives, once an opposing party seeks to pry into these accounts, privacy concerns are quickly raised. This new and developing technology is now challenging courts throughout the country to balance these privacy concerns with an established affinity for broad pretrial discovery. The resulting balancing process is creating a legal and ethical minefield for practicing attorneys seeking access to this information.

As the Ninth Circuit aptly stated, "[t]he Internet has opened new channels of communication and self-expression… While such intermediaries enable the user-driven digital age, they also create new legal problems."[1] Given the rise of social media, lawyers practicing in all fields have been forced to acquire a better understanding of the resource or risk substantial

[1] Fair Housing Council of San Fernando Valley v. Roommates.com, LLC, 489 F.3d 921, 924 (9th Cir. 2007).

harm to their clients. Attempts to excavate useful information from the social media landscape have raised new concerns about attorney ethics and the rules of discovery, which were drafted decades ago before technology like this was even conceived let alone commonplace. A relative lack of consistent judicial precedent on the discoverability of such evidence has not hindered the development of the use of social media information in litigation, as evidenced by the 88 published opinions this past September alone in which evidence mined from social media was of critical importance.[2]

While no hard line rules currently exist for evidence taken from social media platforms, a common theme does seem to be shared among the jurisdictions that have dealt with the issue: individuals who willingly choose to share information with others on platforms designed to broadcast these postings into cyberspace cannot rightfully seek shelter behind privacy concerns when those postings later prove damaging. The broad latitude afforded litigants by the current rules of discoverability and the traditional preference for broad pretrial discovery have been used to justify intrusions into both the public and private sectors of individuals' social media profiles. With the constant and rapid transformation of technology and the advent of products such as Google Glass, there may come a time when new discovery rules may have to be drafted, rules that are specifically geared toward social media. Rules that are centrally focused on social media would allow for uniformity, practicality, and comprehensibility, while also bringing an end to the bevy of litigation that is currently plaguing the judicial system. For now, however, courts seem complacent to use the existing rules of discovery and the rules of professional conduct to answer the questions of what content is discoverable and how that content can be discovered legally and ethically.

[2] John Patzakis, Social Media Case Law Update: The Acceleration Continues, Next Generation eDiscovery Law & Tech Blog (Oct. 4, 2013, 8:42 AM), http:// blog.x1discovery.com/2013/10/04/social-media-case-law-update-the-acceleration-continues.

II. What is Social Media?

According to the Merriam-Webster Dictionary, social media refers to "electronic communication through which users create online communities to share information, ideas, personal messages, and other content."[3] The American Bar Association has defined social media more broadly as "any tool or service that uses the internet to facilitate conversations."[4] Regardless of the definition, it is clear that the phrase encompasses social networking sites like Twitter, Facebook and LinkedIn, blogs, forums, photo-sharing sites like Flickr, and video-steaming websites like internet giant YouTube. Social media as a digital platform for social interaction is a relatively young phenomenon but has experienced explosive growth over the last decade. It has never been more popular than it is today. As of March 2013, Facebook, which is not even ten years old yet, had 1.11 billion active users, with 699 million of these users posting on average at least once per day.[5] Moreover, there have been over 170 billion tweets since 2006, and over 6 billion hours of video are watched each month on YouTube with 100 hours of video being uploaded to the site every minute.[6] As the sheer number of social media platforms and their popularity continue to rise, understanding the nature and functions of the tools at the core of the phenomenon has been crucial to a legal community lambasted with legal and ethical issues.

Social media websites exist primarily to foster and enhance open communication. The unrestricted and public nature of services like Instagram, Facebook, and Twitter, allow and encourage users to instantaneously communicate and share information with not only their

[3] *Social Media Definition*, Merriam-Webster Online Dictionary, http://www.merriam-webster.com/dictionary/social%20media (last visited December 3, 2013).
[4] Catherine Sanders Reach, A Guided Tour of Social Media, Am. Bar Ass'n Legal Tech. Res. Ctr., 2 (2010), http://apps.americanbar.org/legalservices/lpl/downloads/a_guided_tour_of_social_ media.pdf.
[5] Kim Garst, *Social Media Grows Up*, HuffingtonPost.com (Sept. 11, 2013, 12:37 PM), http://www.huffingtonpost.com/kim-garst/social-media-grows-up_b_3906360.html (last visited December 3, 2013).
[6] Doug Gross, *Library of Congress Digs into 170 Billion Tweets*, CNN.com (Jan. 7, 2013, 12:18PM), http://www.cnn.com/2013/01/07/tech/social-media/library-congress-twitter (last visited December 3, 2013); *Statistics*, YouTube.com, http://www.youtube.com/yt/press/statistics.html (last visited December 3, 2013).

personal friends but also acquaintances and the general public as well. Today, information that was once considered private is being broadcasted via social media to an entire world of strangers. By promoting the public exposure of thoughts, feelings, and other personal content, the fundamental nature and characteristics of social media make it a ripe treasure trove of information for attorneys in all fields of practice.

Social media not only promotes the sharing of information and open dialogue, but generally, this personal information is recorded and stored, sometimes permanently. Furthermore, each posting is often stamped with a date, time, and location of the individual at the time of posting. These features can give lawyers unfettered access to a bevy of information that is easy to quickly collect, store, and interpret. With this information readily available at the click of a mouse, what once could only be discovered through a lengthy and potentially arduous process, can now be found by combing through a collection of documents that can be downloaded in mere seconds. Even though the source of this information is rapidly advancing and groundbreaking technology, until now courts have chosen to use the existing rules of discovery to determine what evidence can be subjected to discovery in civil litigation.

III. The Existing Rules of Discovery

In response to a wildfire of issues concerning electronically stored information, the Federal Rules of Civil Procedure were amended in 2006 to better handle issues regarding computer-based discovery. Rather than following this path and drafting new rules, lawmakers have instead chosen to allow courts to mold social media issues into the existing discovery rules. These courts have generally refused to look upon this type of evidence any differently than its

predecessors. As one court stated, "[t]he fact that the [d]efendant is seeking social networking information as opposed to traditional discovery materials does not change the Court's analysis."[7]

The current rules of discovery, both in New Jersey and at the federal level, are broad-sweeping rules that favor the admissibility of pretrial evidence. These rules focus on the content of the information sought as opposed to the information's source. Given that the rules were drafted to be purposefully broad, they often offer courts little guidance when determining whether certain evidence is properly discoverable. The gatekeeping function these rules were meant to serve has thus been significantly nullified by broad judicial interpretation that has afforded litigants wide latitude in the pretrial discovery process under the supposition that this better serves equality and the judicial process as a whole.

Under the Federal Rules of Evidence, whether or not evidence is discoverable ultimately breaks down into an issue of relevancy. According to Rule 26(b), "any nonprivileged matter that is relevant to any party's claim or defense is discoverable."[8] Basically, if the information being sought is relevant to the claims or defenses of the parties to the case, then it should be discoverable. At the pretrial stage this creates an incredibly vast scope of information that must be turned over to the opposing party.

Similar to the broad federal rules of discovery, New Jersey's discovery rules are to be construed liberally in favor of broad pretrial discovery.[9] The primary rule of discovery in New Jersey is Rule 4:10-2 which reads:

---

[7] Giacchetto v. Patchogue-Medford Union Free Sch. Dist., No. CV 11-6323 ADS AKT, 2013 WL 2897054 (E.D.N.Y. May 6, 2013) citing EEOC v. Simply Storage Mgmt., LLC, 270 F.R.D. 430, 434 (S.D. Ind. 2010) ("Discovery of [social networking postings] requires the application of basic discovery principles in a novel context.").

[8] FED. R. CIV. P. 26(b).

[9] See Jenkins v. Rainner, 69 N.J. 50 (1976) ("Our court system has long been committed to the view that essential justice is better achieved when there has been full disclosure so that the parties are conversant with all the available facts.").

> Unless otherwise limited by order of the court in accordance with these rules, the scope of discovery is as follows:
> (a) In General. Parties may obtain discovery regarding any matter, not privileged, which is relevant to the subject matter involved in the pending action, whether it relates to the claim or defense of the party seeking discovery or to the claim or defense of any other party, including the existence, description, nature, custody, condition and location of any books, documents, or other tangible things and the identity and location of persons having knowledge of any discoverable matter. It is not ground for objection that the information sought will be inadmissible at the trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence; nor is it ground for objection that the examining party has knowledge of the matters as to which discovery is sought.[10]

Under the rule, courts possess the power to order a party to produce all relevant, unprivileged information which could potentially lead to the discovery of relevant evidence.[11] While this seemingly provides the court with broad-sweeping powers, a significant shortcoming of the rule's language is that it fails to define the term "relevant" which is vital to a proper understanding of the rule's scope. Under N.J.R.E. 401, however, relevant evidence is defined as "evidence having a tendency in reason to prove or disprove any fact of consequence to the determination of the action."[12] Therefore, in order to establish that evidence is discoverable at the state or federal level, a party must simply satisfy the rather low burden of demonstrating that the evidence is somehow relevant to the issues involved in the case.

IV. Relevancy in the Social Media Landscape

Because of the sheer amount of information contained in a litigant's social media accounts, asking a party to turn over the entirety of his or her account will no doubt produce both relevant and irrelevant evidence. Courts cannot rightfully ask a litigant to turn over all of this irrelevant information, and they are therefore struggling with delineating the scope of relevancy as it pertains to social media evidence. Even though it is has been established that there is no Facebook privilege or privacy expectation in social media postings, a party seeking access to an

[10] N.J. CT. R. 4:10-2(a).
[11] See Huie v. Newcomb Hospital, 112 N.J. Super. 429 (App. Div. 1970).
[12] N.J.R.E. 401.

adversary's social media footprint must still establish that the desired information is relevant or will lead to the discovery of relevant evidence. This relevancy standard has created a bevy of litigation with parties ardently disputing whether certain postings or messages fall under the standard's purview.

A. Who Determines Relevancy

Federal Rule 26(b) and the discovery rules of many states, as exemplified by New Jersey's Rule 4:10, hinge the discoverability of evidence on the issue of relevance. While this may be clear from a plain reading of the rules, what often remains unclear is who determines what is relevant to the issues and defenses of the case.

When an opposing party requests access to evidence located in an adversary's social media accounts, it is often done so through the typical document request for the production of materials. According to common practice, this means that the party producing the requested documents reviews them prior to turning them over, making an initial determination of relevancy as the party will only turn over documents he or she feels are relevant to the case, and specifically the document request. Thus, in a typical case relevancy is determined by the producing party, at least initially. Allowing the producing party to initially determine relevance has proven to be a more favorable alternative than forcing that party to needlessly turn over a mass of information for the adversary to rummage through freely. While this may seem sensible, the process can often become problematic because even the most honest party may seek to hide certain postings under the veil of irrelevance.

When the issue of relevancy becomes contentious, however, courts can be forced to supervise the discovery process by determining what is relevant, often through *in camera* reviews of the materials.[13] Although this ensures that the proper evidence is turned over to the

[13] Bianca v. North Fork Bancorp, 2012 WL. 5199007 (N.Y. 2012).

opposing party, judicial supervision of this nature cannot be relied upon as a steadfast measure for determining relevancy. Such a process is too judicially time-consuming and expensive to be used in every case involving social media evidence. The litigation process must instead be able to rely on the honest production of relevant evidence, as determined by the adversaries themselves, with judicial assistance given only on an as-need basis.

B. Relevancy and Social Media Evidence

Even though the parties initially determine relevancy, courts have been inundated with social media discovery disputes concerning the relevancy of account information and the corresponding postings within those accounts. The relevancy standard has proven a rather low hurdle for parties looking to access an adversary's social media postings, but at the same time has also prevented carte blanche invasions of privacy. An adversary does not have the ability to force the production of all social media evidence. It must limit that discovery to content that is relevant to the case. Courts are currently defining the scope of relevance with regards to social media evidence, and, unsurprisingly, many have come to varying conclusions.

An Indiana court recently defined the scope of relevancy for social media discovery as "any profile, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries) and social networking site applications for the claimant… that reveal, refer, or relate to any emotion, feeling, or mental state, as well as communications that reveal, refer, or relate to events that could reasonably be expected to produce a significant emotion, feeling, or mental state."[14] The defendant employer sought access to two employees' Facebook profiles after the E.E.O.C. brought suit for sexual harassment on the

[14] E.E.O.C. v. Simply Storage Mgmt, LLC, 270 F.R.D. 430, 437 (S.D. Ind. 2010).

employees' behalves.[15] In limiting the scope of discoverability, the court recognized that discovery does have limits and "the challenge is to define appropriately broad limits – but limits nevertheless – on the discoverability of social communications in light of a subject as amorphous as emotional and mental health…"[16] The court also stated that a picture posted on a third-party's profile in which a litigant is merely tagged in, is less likely to be relevant to the case at hand, while photographs or videos of third-parties, unrelated to the case at hand, are most likely irrelevant.[17]

Similarly, the Eastern District of New York has recognized that the broad nature of relevancy must be somewhat restrained when confronted with a motion to compel seeking to force the plaintiff to release all records contained in her social networking accounts.[18] The plaintiff attempted to argue that the request violated her privacy rights and was based on nothing more than "pure speculation."[19] The defendants, however, contended that the information sought reflected the plaintiff's "levels of social interaction and daily functioning" as well as her "emotional and psychological state."[20] After a lengthy discussion of how other jurisdictions had managed the issues of social networking discovery and its effect on emotional damages, the court concluded that plaintiff's general postings and "routine updates" were not relevant to her claim of emotional damages.[21] However, the plaintiff was required to produce "any specific references to the emotional distress she claims she suffered or treatment she received in connection with the incidents underlying her Amended Complaint."[22] In response to plaintiff's claim for physical damages the court held that "[p]ostings or photographs on social networking

[15] Id. at 430.
[16] Id. at 433.
[17] Id. at 436.
[18] Giacchetto, 2013 WL 2897054 at *1.
[19] Id.
[20] Id.
[21] Id. at *4.
[22] Id.

websites that reflect physical capabilities inconsistent with a plaintiff's claimed injury are relevant."[23] The court went further to require plaintiff to produce "any social networking postings that refer or relate to any of the events alleged in the Amended Complaint."[24]

Courts have continually used the low-burden relevancy standard found within the current discovery rules to establish that social media evidence should be treated no differently than evidence the court has been confronting for decades. However, the issue of whether pretrial discovery can breach the privacy settings of an individual's account has raised new concerns and somewhat conflicted rulings.

C. Relevancy and Private Postings

While social media users willingly choose to share information online, many do so with the belief that they can use privacy settings to control who sees the posted content. Broad pretrial discovery, however, allows adversarial parties to pierce through these privacy settings to acquire relevant evidence. Even though parties may go through great lengths to protect certain postings, there is no social media privilege. Parties to litigation have always been forced to turn over incredibly personal, and often intrusive, information including medical records and tax returns. If these materials are not protected discovery, then neither are postings published into cyberspace, no matter the privacy settings. Unless the party can raise a successful claim of privilege under Rule 26(c) or parallel state laws, if the information is relevant to the issues at hand then it is discoverable.[25] The general view is that all relevant social media evidence, no matter its classification as private or public, is discoverable, but some courts have improperly established relevancy thresholds for obtaining this private information.

[23] Id.
[24] Id.
[25] Fed. R. Civ. P. 26.

Generally, relevant information, even in the private sections of these accounts is discoverable because it is neither privileged nor protected by a common law right of privacy.[26] "Merely locking a profile from public access does not prevent discovery."[27] According to the New York Supreme Court of Suffolk County, the private information located in the plaintiff's social media accounts is discoverable given the nature of social networking websites.[28] The court recognized that the plaintiff did not have a reasonable expectation of privacy in postings published online and any privacy concerns that could be raised were outweighed by the need for information and went against the values of New York's discovery rules.[29] "Preventing [d]efendant from accessing to [p]laintiff's private postings on Facebook and MySpace would be in direct contravention to the liberal disclosure policy in New York State."[30] The court also acknowledged that the public information on plaintiff's accounts seemingly contained material evidence that contradicted plaintiff's personal injury claims.[31] According to the court, this meant a reasonable likelihood existed that the private information of plaintiff's accounts would contain other relevant information.[32] While the court used this logic to further support its position, other courts have taken the private-public dichotomy further by demanding a party show the producing party's public information was relevant before granting access to any private postings.

These courts create a threshold issue for the discovering party to satisfy: if a party wishes to access the private information of the social media account, that party must first establish the public parts of the profile contain information relevant to the issues. The theory seems to be that

[26] See Glazer v. Fireman's Fund Ins. Co., No. 11 CIV. 4374 PGG FM, 2012 WL 1197167, *3-4 (S.D.N.Y. April 5, 2012); see also Tompkins v. Detroit Metro. Airport, 278 F.R.D. 387 (E.D. Mich. 2012). "The fact that [d]efendant is seeking social networking information as opposed to traditional discovery materials does not change the Court's analysis."
[27] E.E.O.C., 270 F.R.D. at 434.
[28] See Romano v. Steelcase Inc., 907 N.Y.S.2d 650 (Sup. Ct. 2010).
[29] Id. at 656, citing U.S. v. Lifshitz, 369 F.3d 173 (2d Cir. 2004).
[30] Id.
[31] Id. at 654.
[32] Id.

mere suspicion or speculation that the private contents of an individual's social media accounts contain relevant information is not enough to just the production of such information.[33] The logic involved in these holdings places too heavy a burden on the discovering party, given the nature and dichotomy of private and public social media postings. Generally, information that is shared privately is more personal and revealing because the posting party believes he or she is in control of the post's audience. These postings are more likely to contain relevant information with regards to emotional and physical well-being than the generic everyday posts that the user wishes to share with the world. Moreover, some parties may not share any information publicly and complete shroud all postings or messages. Forcing a litigant to meet the threshold showing of relevancy as to the public postings improperly parallels the two portions of the adversary's profiles and can prevent the disclosure of pertinent evidence.

Even though some courts require this threshold showing, judicial precedent has at least established that litigants cannot hide their damaging social media postings simply by making their accounts private. At the very most, this process simply creates another hurdle for the adversary to overcome during discovery. Regardless of the select group who has access to the private postings, the fact remains that information is being shared on a digital platform. Therefore, if the information is relevant, a litigant has a right to access that content. Although the information is generally deemed discoverable, as long as the low hurdle of relevancy is met, the judicial precedent has established that there is a method to properly obtaining this information without clashing with the opposing party or the established values of discovery.

V. How Social Media Evidence Can Be Discovered Properly

Given the amount of information available to opposing parties, it is easy to serve an opposing party with an overdrawn discovery request that seeks the adversary's entire social

[33] See Mackelprang v. Fid. Nat. Title Agency of Nevada, Inc., No. 2:06-CV-00788-JCM, 2007 WL 119149 (D. Nev. Jan. 9, 2007).

media history. Assuredly, if an attorney were to dig through an adversary's digital footprint long enough he or she would find something relevant to the disputed issues. However, requesting the entirety of an individual's social media accounts runs afoul of the established principle that discovery should not be disproportionate to the needs of the case. Although this guideline appears to be well-established, courts have struggled to establish a definitive scope as to what constitutes proper discovery and what crosses that line into the proverbial fishing expedition.

When confronted with issues of discoverability, courts have consistently reiterated that the discovery of social media should be equated with the discovery of other evidence. These courts should therefore hold steadfast to this analogy when determining how that evidence can be discovered. For example, if a party had in its possession handwritten letters that were relevant to the claims of the case, that party must turn over those letters in response to a proper discovery request. However, if that party kept those letters in a large box labeled "correspondence" which contained all letters that the individual had sent and received over the last several years, that individual should not have to turn over the entirety of the box for the opposing party's search for relevant evidence.[34] An individual should not be forced to turn over such personal information just because relevant evidence may exist somewhere in the box. Similarly, although it is likely that a party's social media accounts contain relevant information, that party should not then be forced to turn over the entirety of the social media accounts for the opposing party to rummage through freely.

Although parties are entitled to broad pretrial discovery, they are not entitled to turn the discovery process into an invasive, unfocussed expedition based on nothing more than the mere

[34] Steven S. Gensler, Special Rules for Social Media Discovery?, 65 Ark. L. Rev. 7, 15 (2012).

suspicion or hope that relevant evidence will turn up eventually.[35] Neither party has the "generalized right to rummage at will through information that Plaintiff has limited from public view.[36] Litigants are best served using a narrowly-tailored discovery request that outlines the material being sought and why that material is relevant to the claims of the case. Courts are more apt to respond approvingly of these requests that feature some degree of specificity.

For example, in Ford v. United States, the government sought an order compelling plaintiffs to produce "any documents [,] postings, pictures, messages [,] or entries of any kind on social media within the covered period relating to [c]laims by plaintiffs or their [e]xperts."[37] The information sought covered the time period between the incident at issue in the matter and the date of the discovery request.[38] The plaintiffs objected to the request claiming that it was "invasive, overbroad, and not calculated to lead to the discovery of admissible information."[39] The court recognized that other courts required the production of social media information "in response to more narrowly tailored requests, such as those relating to events alleged in the complaint."[40] Accordingly, the court found that the government's request was not narrowly tailored because it did not "describe the categories of material sought; rather it reli[ed] on [p]laintiffs to determine what might be relevant. Thus it is overbroad and vague."[41]

Similarly, in response to a defendant's discovery request seeking plaintiff's personal emails and messages sent via a private MySpace account, a Nevada court concluded that the defendants did not sufficiently establish a relevant basis for acquiring the information other than

[35] Tompkins v. Detroit Metropolitan Airport, 278 F.R.D. 387, 388 (E.D. Mich. Jan. 18, 2012) quoting McCann v. Harleysville Ins. Co. of New York, 910 N.Y.S.2d 614, (N.Y. App. Div. 2010).
[36] Id.
[37] No. CIV. A.DKC11-3039, 2013 WL 3877756 (D. Md. July 25, 2013).
[38] Id.
[39] Id. at *2.
[40] Id.
[41] Id.

the "suspicion that they may contain sexually explicit of secually promiscuous content."[42] The court reasoned that allowing defendant access to all of the private emails on the plaintiff's MySpace accounts would "cast too wide a net" for information that could be relevant which would lead to the production of irrelevant information.[43] However, the court did find that defendant was entitled to seek information relating to plaintiff's alleged mental condition via "properly limited requests for production of relevant email communications."[44]

Even with broad pretrial discovery, it is clear that parties are not entitled to mine through the personal affairs of individuals with nothing more than hopes of finding something relevant. Such course of action is unjustifiably intrusive and produces too much irrelevant information. Again, it is best for an attorney seeking social media evidence to serve a narrowly-tailored request upon the opposing party, rather than utilizing alternative, less favorable means.

VI. Social Media Content Providers & Their Responses to Discovery Requests

Obtaining evidence directly from the social media content provider is rarely, if ever, a fruitful endeavor. Rather than attempting to obtain information directly from the social media service, an attorney seeking to uncover the social media exploits of an opposing party should direct the corresponding discovery requests directly to opposing counsel. Without a court order or the opposing party's consent, social media sites are unlikely to respond to any such request. This is most likely because these companies go to great lengths to ensure the protection of their users' private information and risk losing members or facing potential litigation if they were to compromise that trust. Instead, companies like Facebook and Twitter direct opposing parties to acquire the information they seek from one another, choosing to remove themselves from the equation entirely if possible.

[42] Mackelprang, 2007 WL 119149 at *2.
[43] Id. at *7.
[44] Id. at *8.

Although social media content providers have attempted to actively withdraw themselves from the discovery process, in response to the escalating use of social media evidence in litigation they have developed tools that allow users to easily download the information contained within their accounts. For example, Facebook allows users to download their entire account into one file.[45] This makes for a rather simple process to accumulate information that covers the entire span of the user's profile timeline. Although lauded for its simplicity, a commonly overlooked factor of this option is the sheer breadth of what information is included in this material. The downloaded file contains data of all of the user's active session on Facebook (dates, times, devices, IP addresses), a list of ad topics generated based on information mined from your timeline, complete chat histories, and the places you've checked into.[46] Also included are any friend requests sent or received, any friends the user had at any point in time, a list of accounts linked to the Facebook account, and any messages the account sent or received except those that have been previously deleted.[47] While it is clear that this information could be incredibly useful in litigation, the sheer breadth is overwhelming and involves significant activity conducted by third-parties. When a litigant turns over such downloaded information, he or she is also turning over posts, messages, and photos produced by non-parties to the litigation that may have their own privacy concerns. With tools like these available, some courts have disfavored claims of that producing evidence from social media accounts is unduly burdensome.[48]

Services like Facebook provide these tools to prevent users from being forced into turning over their login credentials to another individual. According to Facebook's Terms of Service, users are not permitted to share their password with a third party or allow a third party

[45] Downloading Your Information, https://www.facebook.com/help/131112897028467 (last visited December 3, 2013).
[46] Id.
[47] Id.
[48] See In re White Tail Oilfield Servs., L.L.C., CIV.A. 11-0009, 2012 WL 4857777 (E.D. La. Oct. 11, 2012).

to access their account. Specifically, the terms of service read "You will not share your password (or in the case of developers, your secret key), let anyone else access your account or do anything else that might jeopardize the security of your account."[49] When a litigation storm erupted when employers began delving into the accounts of employees and potential employees, Facebook's Chief Privacy Officer Erin Egan, stated, "[Y]ou should never have to share your password, let anyone access your account, or do anything that might jeopardize the security of your account or violate the privacy of your friends. We have worked really hard at Facebook to give you the tools to control who sees your information."[50] In an era where digital privacy concerns are at an all-time high, Facebook and other social media websites have actively withdrawn from litigation between third-parties. Facebook's stance favoring privacy, however, stands in direct contrast with jurisdictions that have forced individuals to turn over their login credentials to the opposing party.

Moreover, litigants seeking to acquire social media information from the platforms themselves can run afoul of the Stored Communications Act. In Crispin v. Christian Audigier, Inc., for example, the defendants served subpoenas on third-party websites, including Facebook and MySpace, seeking to discover plaintiff's messages and other related content.[51] Although the lower court had denied the plaintiff's motion to quash the subpoenas, the Federal District Court for the Central District of California seemed to rule that the private communications that take place on social media sites are protected from disclosure by third-parties in civil suits whether or

[49] Statement of Rights and Responsibilities, Facebook (last updated Dec. 11, 2012), http://www.facebook.com/legal/terms (last visited December 3, 2013).

[50] John G. Browning, With "Friends" Like These, Who Needs Enemies? Passwords, Privacy, and the Discovery of Social Media Content, 36 Am. J. Trial Advoc. 505, 534 (2013) citing Erin Egan, Protecting Your Passwords and Your Privacy, Facebook (Mar. 23, 2012, 7:32 AM), http://www.facebook.com/notes/facebook-and-privacy/protecting-your-passwords-and-your-privacy/326598317390057.

[51] See Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 968-69 (C.D. Cal. 2010).

not they were disseminated through a public or partially public section of the site.[52] The court reasoned that the social media platforms did fall under the purview of the Act as electronic communication services and that the information sought was electronic storage.[53] Therefore, even though the postings could potentially be displayed to a wide audience, the legislative history of the statute indicated a desire to "protect the electronic communications that are configured to be private, such as private electronic bulletin boards."[54] Although the decision was not clear-cut and the reasoning was a bit murky, the Stored Communications Act in general is a murky piece of legislation that attorneys should seek to avoid.

Attorneys should therefore avoid subpoenaing the social media content provider, and instead seek the information through other avenues, though there are pitfalls there as well.

VII. Ethical Issues of Mining Social Media Accounts

Attorneys have taken various routes in understanding and utilizing the evidence available on social media platforms. It is of no surprise that some attorneys have taken to scrupulous means of acquiring damning evidence against an adversary, while others have held steadfast in their ways by ignoring the websites altogether. As the landscape continues to expand, however, ethics committees and bar associations around the country are currently setting the standards for practicing in an increasingly digital age, and the process has had far-reaching ramifications for all practicing attorneys.

Given the explosive nature of the content and the novel issues it raises, attorneys have clashed with significant ethical issues both in the collection of the evidence and in monitoring their clients' use of social media evidence, which can give rise to spoliation claims. The most

[52] Id. at 991.
[53] Id.
[54] Id. at 979 citing Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 879 (9th Cir. 2002).

significant of these ethical developments is that lawyers are now being held responsible for understanding the technology and its legal implications.

A. Attorneys Have an Ethical Responsibility to Mine Social Networks

Social media evidence has reached a stage where it is too significant to ignore. There is now a wealth of evidence that is easily discoverable and potentially determinative of the outcome of a case. The popularity of social media has reached a point where social media discovery attempts should now be considered a necessity for any practicing attorney, no matter the field, and attorneys that ignore social media evidence can be subjected to charges for ineffective assistance of counsel.[55]

At this point in the digital era, attorneys who fail to search for relevant social media evidence or search improperly cannot shield themselves from liability by claiming a lack of understanding. Social media has become such a key issue that attorneys that do not comprehend the importance of social media evidence, how to discover it, or the social media activity of their clients may be subjected to legal malpractice actions.[56] Although a malpractice claim would only be successful upon a showing that the social media evidence would have made a difference in the outcome of the case, ignoring social media poses too substantial a threat to an attorney's reputation and financial well-being.[57]

In a report filed in May 2012, the ABA Commission on Ethics 20/20 stated that technology "has irrevocably changed and continues to alter the practice of law in fundamental ways. Lawyers must understand technology in order to provide clients with the competent and

[55] See Steven S. Gensler, Special Rules for Social Media Discovery?, 65 Ark. L. Rev. 7, 9 (2012) citing Sashe D. Dimitroff, Social Media and Discovery, in The Role of Technology in Evidence Collection ("Lawyers will be remiss--if they are not so already--who do not consider social media a potential source of discovery."); see also Canedy v. Adams, 2009 WL 3711958 (C.D. Cal. Nov. 4, 2009).

[56] See Frullo v. Landenberger, 814 N.E.2d 1105 (Mass. App. Ct. 2004).

[57] Id. at 1109-110.

cost-effective services that they expect and deserve."[58] The law is a dynamic field, and although the technology is a new phenomenon, the Model Rules of Professional Conduct have long held attorneys responsible for continually updating their legal education. According to Model Rule 1.1, "[a] lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for representation."[59] Specifically, Comment 6 to the Rule, reads: "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…"[60] Staying "abreast" involves understanding technology's effect on legal research and conducting discovery.[61] "These tasks now require lawyers to have a firm grasp on how electronic information is created, stored, and received."[62] According to the Ethics Commission, "a lawyer would have difficulty providing competent legal services in today's environment without knowing how to use email or create an electronic document."[63]

In the digital era, it is not surprising that courts are progressively placing duties on attorneys to effectively use technology for the benefit of their clients. At one point in time, using the resources of the internet and technology in general was a competitive advantage. Now,

---

[58] See John G. Browning, Facebook, Twitter, and Linkedin - Oh My! The ABA Ethics 20/20 Commission and Evolving Ethical Issues in the Use of Social Media, 40 N. Ky. L. Rev. 255, 259 (2013) citing ABA Comm'n on Ethics 20/20 Introduction and Overview 4 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.authcheckdam.pdf.

[59] ABA Model Rules of Prof'l Conduct R. 1.1 (as amended Aug. 2012).

[60] Id. at cmt. 6.

[61] ABA Comm'n on Ethics 20/20 Introduction and Overview 4 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/20120508_ethics_20_20_final_hod_introdution_and_overview_report.authcheckdam.pdf (last visited December 3, 2013).

[62] Id.

[63] ABA Comm'n on Ethics 20/20, Report to the House of Delegates 6 (Aug. 2012), http://www.americanbar.org/content/dam/aba/administrative/ethics_2020/2012_hod_annual_meeting_105a.authcheckdam.pdf (last visited December 3, 2013).

however, it has become mandatory practice.[64] Attorneys must understand how to use technology and must actively convey that knowledge to their clients once litigation has begun. It is also becoming increasingly clear that attorneys must also know how to look for this information without being charged with ethics or conduct violations which can be a tricky endeavor given recent ethics rulings from several jurisdictions.

B. Ethically Mining Social Media Websites

Given the significance and growth of social media, attorneys must understand the proper procedures for discovering the relevant evidence contained therein. The Rules of Professional Conduct currently delineate what an attorney can and cannot do when communicating with adversaries and third parties. These rules are being tested by communications that take place via social media platforms, and ethics commissions from multiple states have reached drastically different conclusions as to what constitutes proper behavior on social media.

The Model Rules of Professional Conduct have been adopted in some form in every state except for California. Under the Model Rules of Professional Conduct, specifically Rule 8.4, a lawyer who engages in conduct involving dishonesty or misrepresentation can be the subject of a professional misconduct action.[65] Specifically, a lawyer cannot "engage in conduct involving dishonesty, fraud, deceit or misrepresentation."[66] Given the focus of the rule on intentional deception, it would appear that an attorney sending a friend request to an individual without anything more would be free from any potential claims. After all, the individual receiving the request is free to decline it and maintain exclusive control of their information. However, this is not always the case because at least one ethics committee has ruled that the attorney's hidden agenda is controlling. While it may seem illogical to equate a simple friend request with acts of

[64] John G. Browning, Facebook, Twitter, and Linkedin - Oh My! The ABA Ethics 20/20 Commission and Evolving Ethical Issues in the Use of Social Media, 40 N. Ky. L. Rev. 255, 261-62 (2013)
[65] See Model Rules of Prof'l Conduct 8.4.
[66] Id.

fraud and deceit, divergent holdings make it unclear whether an attorney has to disclose why that individual is receiving the request at issue or be at risk for not disclosing a material fact.

The Model Rules provide another potential trap for attorneys delving into the digital world in search of treasure. Model Rule 4.2 prohibits any communication between an attorney and an adversary known to be represented by another attorney without consent.[67] While it may seem clever to work around this rule by involving the assistance of third-party investigators, Rules 5 and 8.4 force attorneys to shoulder the blame for communications made for those working under them. It is important to note, however, that separate rules exist for employees of the government or prosecutors who may be permitted to act in undercover investigations to discern information. Investigations on social networking websites require the same analysis as traditional undercover investigations, but with some new twists, especially regarding the propriety of friend requests.

It seems clear that a Facebook request would fall under the type of communication prohibited by the aforementioned rules regarding communications with a represented adversary. But this should not stop an attorney from performing social media due diligence to determine if the opposing party has publicly available information such as blogs or other postings that could be accessed without communicating directly with the opposing party. Obviously if an attorney were to discover pertinent information after running an adversary's name through the search engines available on Google or Facebook, no ethics violations could be raised. These individuals are putting the information out there for the entire world to view so in the eyes of the rules governing attorneys it is all fair game, as should be the case. Additionally, according to at least one state's ethics committee, the simple fact that an attorney has to register on the website or create a profile to access the information does not prevent that information from being

[67] See Model Rules of Prof'l Conduct 4.2.

considered public.[68] If, however, the targeted individual has set up a network or private profile with the very intention of preventing people from viewing his or her profile, then any deceitful act of attempting to acquire this information through misrepresentations could potentially open the lawyer up to ethics violations.

According to the Philadelphia Committee on Legal Ethics, any Facebook friend request sent to a third party, even if sent from an honest personal account, is deceptive and in violation of Rule 8.4 unless that friend request discloses the attorney is seeking to find information relevant to an ongoing case.[69] According to the committee, an attorney acts deceptively by failing to advise the targeted third party of "a highly material fact, namely, that the third party who asks to be allowed access to the witness's pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness."[70] Although the attorney attempted to argue that viewing the individual's Facebook profile directly compared to the legal and ethical practice of videotaping an individual in public, the court found little solace in this comparison because in this case the attorney had to first request permission of the targeted individual to access the desired information.[71] The committee stated that deceptively seeking to access the individual's Facebook profile was similar to the attorney wearing a disguise and sneaking into the individual's home.[72] Rather than taking the Facebook request at face value, the committee instead chose to focus on the attorney's hidden intent in making the request even though the individual had the power to refuse the request and therefore block any type of investigation.[73]

---

[68] See Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02 (2009).
[69] Id.
[70] Id. at 2.
[71] Id.
[72] Id.
[73] Id.

The San Diego County Bar Association's Legal Ethics Committee ruled similarly when it determined that a lawyer may not ethically make ex parte friend requests to represented third parties.[74] The Committee held that under no circumstances may an attorney friend request a represented party's profile, but that attorney may send a request to an unrepresented individual only after disclosing the true nature of the request, i.e. that the request is for litigation purposes.[75] Although the attorney was free to access publicly shared information, a line had to be drawn to prevent attorneys from "intruding on the attorney-client relationship of opposing parties and surreptitiously circumventing the privacy even of those who are unrepresented."[76]

Viewing the same issue in a completely opposite manner, the New York City Committee on Legal Ethics held that no ethical violations occur if an attorney uses a truthful, personal account to send a friend request to an unrepresented third party.[77] Unlike the Philadelphia Committee, the New York City Committee found that no material misrepresentations were being made because the account contained only truthful information about the attorney and the targeted individual had the choice to allow this stranger access to his or her personal information.[78] According to his committee, an attorney cannot be found to violate Model Rule 4.1 unless that attorney uses a false profile or some form of false information to access the individual's account.[79]

The Philadelphia Bar Professional Guidance Committee also reiterated the belief that these same principles apply to an agent of that attorney who uses a social media account to friend the opposing party. The Committee determined that an attorney acts deceptively if he or she

[74] See San Diego Ctny. Bar Ass'n Legal Ethics Comm. Op. 2011-2, 1 (2011).
[75] Id.
[76] Id.
[77] See N.Y. City Bar Ass'n Comm. on Prof'l & Judicial Ethics, Formal Op. 2010-2 (2010).
[78] Id.
[79] Id.

uses a third-party investigator to acquire information from someone using a friend request.[80] Although the court recognized that the investigator did not dupe the opposing party into accepting the friend request in any way besides sending the invite, deception could be found in that the investigator chose to omit "a highly material fact, namely, that the third party who asks to be allowed access to the witness's pages is doing so only because he or she is intent on obtaining information and sharing it with a lawyer for use in a lawsuit to impeach the testimony of the witness."[81] This ruling is directly in line with the Philadelphia Committee's prior ruling as again an emphasis was placed on the hidden intent of the attorney.

It is clear that even though most jurisdictions have adopted similar rules of professional conduct, the application of those rules varies and attorneys seeking social media discovery must be wary of the precedent established in their jurisdictions before taking any course of action.

C. Maintaining Social Media Evidence: Claims for Spoliation

With the inadvertent click of a mouse years of relevant evidence can be permanently deleted. When electronic data is involved in litigation, an attorney should take affirmative steps to ensure that the evidence is neither destroyed nor altered in any way. With litigation either ongoing or pending, there is a real danger that the adversaries may remove damning content from their accounts to better serve their needs. No matter how damning or embarrassing the evidence may be, attorneys are strictly prohibited from destroying evidence.[82] When this evidence is deleted it can give rise to spoliation claims, as exemplified by two recent cases from New Jersey and Virginia.

[80] See Phila. Bar Ass'n Prof'l Guidance Comm., Op. 2009-02 (2009).
[81] Id. at 3.
[82] See Mod. Rules Prof. Cond. s. 3.4(a).

In Gatto v. United Air Lines, Inc., the plaintiff allegedly sustained several injuries as a result of an accident caused by defendant United Air Lines.[83] The plaintiff claimed his injuries left him disabled and severely limited his ability to participate in physical and social activities.[84] During discovery, the defendants sought information relating to the plaintiff's Facebook account and the plaintiff refused.[85] Judge Waldor ordered the plaintiff to release the information, and the plaintiff acquiesced by changing his password to allow the defendants access to his account.[86] The plaintiff, however, deactivated his account shortly thereafter and all of the information was permanently lost.[87] The defendants claimed that what information they did acquire from Facebook was contrary to the plaintiff's injury claims as they showed the plaintiff participating in numerous social and physical activities.[88] The court recognized that the plaintiff's Facebook account was relevant to the litigation because plaintiff alleged to have sustained serious injuries that limited his ability to work and engage in certain other physical activities.[89] While spoliation was not an issue in the case, the plaintiff clearly destroyed relevant evidence that could have played a role in the outcome of the case.

If a party to a case purposefully destroys relevant social media evidence, even if acting under the advice of counsel, that party and the responsible attorney will be subjected to spoliation claims and potentially significant sanctions. This was the case in Allied Concrete Co. v. Lester, where the plaintiff company sought access to the defendant's Facebook profile and the photographs contained within it.[90] After the plaintiff acquired a photo that portrayed the defendant in a poor light, the defendant's attorney, through a paralegal, instructed the defendant

[83] Gatto v. United Air Lines, Inc., No. 10-cv-1090, 2013 U.S. Dist. LEXIS 41909 (D.N.J. March 25, 2013).
[84] Id. at *2.
[85] Id.
[86] Id. at *4.
[87] Id. at *5.
[88] Id.
[89] Id. at *7.
[90] 285 Va. 295 (2013).

to "clean up" his Facebook page because "[we don't] want blow ups of other pictures at trial."[91] The defendant then proceeded to delete a significant number of photographs from his profile.[92] Even though these photos were eventually obtained and Lester prevailed at trial, the court ordered sanctions in the amount of $180,000 against Lester and $542,000 against his attorneys.[93]

Besides fines, sanctions for spoliation can include fee-shifting, special jury instructions such as adverse inference charges, outright preclusion of certain evidence or issues, or even the entry of default judgment or dismissal. Although not etched in stone, generally, the duty to preserve evidence begins before litigation, when litigation is likely.[94]

VIII. Issues Arising After the Discovery Phase

While determining the discoverability of social media evidence is a daunting task in and of itself, it is also a prelude to a much larger battle. Attorneys must still get this type of evidence admitted if they wish to use it at trial. This evidence must therefore withstand the evidentiary rules concerning 403 balancing, hearsay, and the best evidence rule. This can prove difficult given the nature of social media. Some courts have expressed the view that evidence taken from social media accounts possesses no more evidentiary uncertainty than written documents, given that written documents and signatures can be easily forged.[95] Other courts have taken a harder look at just how easily social media postings and profiles can be manipulated, requiring the proponent of the evidence to establish not only that the postings came from the individual's account, but that they were in fact specifically created by that individual.[96] Either way, a

[91] Id. at 302.
[92] Id.
[93] Id. at 303.
[94] See Pension Comm. of the Univ. of Montreal Pension Plan v. Banc of America Securities, LLC, 685 F. Supp 2d 456, 461 (S.D.N.Y. 2010).
[95] See In re F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005).
[96] See State v. Eleck, 130 Conn. App. 632, 23 A.3d 818 (2011)

competent attorney will want to fully understand the steps required to properly authenticate this increasingly popular evidence if that attorney wants to realize the full benefit of such material.

Under the Federal Rules of Evidence, and similar state-specific evidence rules, to admit evidence, a litigant must establish that the evidence is (1) relevant, (2) authentic, and (3) not subject to being excluded under the hearsay rules. Under Federal Rule of Evidence 901(b) evidence can be authenticated by "[t]estimony that a matter is what it is claimed to be," or by the "[a]ppearance, contents, substance, internal patterns, or other distinctive characteristics taken in conjunction with circumstances."[97] Electronically stored information, specifically, can be authenticated under Rule 901(b)(4) if the producing party has supporting evidence that shows the "contents, substance, internal patterns, or other distinctive characteristics" of the evidence.[98]

Getting social media evidence admitted into court does not require authentication by a representative of the social media service provider.[99] Messages or postings can be authenticated through the testimony of the individual who authored the postings. The easiest way to properly authenticate social media evidence, however, is to obtain an admission from the account holder. This can be done through deposition testimony or a notice to admit. If for some reason this is not possible, and the circumstantial evidence of distinguishing characteristics is not sufficient, the proponent of the evidence can hire an e-discovery expert to electronically trace the postings. This alternative, however, can prove quite time-consuming and significantly expensive.

The evidentiary issues surrounding the authentication and admissibility have been best represented in criminal cases.[100] In Griffin v. State, for example, the state attempted to use printouts from the MySpace page of the defendant's girlfriend by having a police officer

[97] FED. R. EVID. 901(b).
[98] FED. R. EVID. 901(b)(4).
[99] See Dockery v. Dockery, No. 22009-01059-COA-R3-CV, 2009 WL 348662 (Tenn. Ct. App. Oct. 29, 2009).
[100] See generally Commonwealth v. Williams, 456 Mass. 857 (2010); People v. Lenihan, 911 N.Y.S.2d 588 (Sup. 2010); People v. Clevenstine, 891 N.Y.S.2d 511 (N.Y. 2009).

authenticate the pages.[101] The postings on the profile allegedly contained threats to eyewitnesses of the murder.[102] The court recognized that "anyone can create a fictitious account and masquerade under another person's name or can gain access to another's account by obtaining the user's username and password."[103] Even though the profile from which the evidence was taken contained the girlfriend's correct birthday, location, and photographs, the court found that the state failed to lay a proper foundation for admitting the evidence because there was a possibility that the profile was created by a third party or was hacked by someone at the time of the postings.[104] According to the court, there was too great of a potential for abuse or manipulation to admit the evidence.[105] The court also laid out several alternative methods the state could have taken to properly authenticate the postings, including asking the individual if she did in fact create the profile and subsequent postings, examining the individual's laptop and internet history, and contacting the social media website directly.[106]

Some courts, however, focus on the user's social media profile and its degree of customization or individualization as a means for authenticating the evidence at issue. Distinguishing Griffin, the Court of Criminal Appeals of Texas recently utilized "circumstantial indicia of authenticity" to admit disputed MySpace postings.[107] Those indicia included photographs of the appellant displaying his unique, gang-related tattoos, a registered email address that included a nickname the appellant was known to go by, and revealing messages to other MySpace users.[108] Affirming the lower court's admittance of the evidence, the court reasoned that this evidence "taken as a whole with all of the individual, particular details

[101] 419 Md. 343, 348 (2011).
[102] Id.
[103] Id. at 352.
[104] Id. at 357.
[105] Id.
[106] Id. at 363-64.
[107] See Tienda v. State, 358 S.W.3d 633, 647 (Tex. Crim. App. 2012).
[108] Id. at 642-45.

considered in combination" was enough to conclude that the MySpace pages did indeed belong to the appellant.[109] This reasoning was consistent with that displayed by the lower court, which ruled:

> "The inherent nature of social networking websites encourages members who choose to use pseudonyms to identify themselves by posting profile pictures or descriptions of their physical appearances, personal backgrounds, and lifestyles. This type of individualization is significant in authenticating a particular profile page as having been created by the person depicted in it. The more particular and individualized the information, the greater the support for a reasonable juror's finding that the person depicted supplied the information."[110]

Getting social media evidence properly authenticated and subsequently admitted at trial can be incredibly difficult if the proper precautions are not taken. Attorneys must be wary of these evidentiary hurdles, even if it appears obvious that the individual was responsible for publishing the postings or creating the account. The authentication of such evidence is another concern that practicing attorneys must familiarize themselves with in order to properly represent their clients in the digital era.

IX. How to Handle Social Media Issues

With new websites popping up every day, the rise of social media is more of a revolution than a fad. Lawyers in all fields must better equip themselves to deal with the issues that arise from their clients' use of these social mediums to better serve them in whatever endeavor. While it would be unethical to advise a client to delete their social media presence, an attorney must also be proactive and warn a client that opposing counsel is entitled to this type of evidence if it is relevant to the issues at hand. Forewarning a client that this is a likely possibility will ease the potential invasive feelings of having someone dig through one's online identity. Social media evidence cannot be ignored, but at the same time raises numerous ethical considerations. This

[109] Id. at 645.
[110] See Tienda v. State, 05-09-00553-CR, 2010 WL 5129722 (Tex. App. Dec. 17, 2010) aff'd, 358 S.W.3d 633 (Tex. Crim. App. 2012).

dichotomy can create a fine line around which attorneys must tread lightly whenever social media evidence could come into play.

For those attorneys seeking to uncover social media evidence from opposing parties, the best route is to be as specific as possible in a narrowly-tailored discovery request. An attorney who notifies the opposing party that he or she is searching only for content that is relevant to the case at hand will better serve that attorney if complications or objections are raised down the line. Additionally, rather than attempting to acquire the specified party's login credentials, the simpler and more preferred route is to have that party use the tools already available to download and then turnover the relevant information. This way less of an invasion occurs as the opposing party remains in control of his or her account and the parties can avoid potential clashes with the Stored Communications Act. Individuals are more apt to turn over information in their exclusive control rather than letting multiple individuals peruse through their online accounts, especially when their login credentials may include a password that is attached to accounts on different websites not relevant to the litigation, such as banking or retail websites. Furthermore, a narrowly-tailored request directed at specific information has a much greater opportunity of withstanding any objections under the current discovery rules.

In terms of acquiring the information outside the procedural guidelines of the discovery rules, an attorney should proceed with caution. If the information is posted to a public profile, it is fair game and an attorney can, and should, extract the postings for relevant evidence. If, however, the information can only be found on a private account, an attorney should look to its local or state bar association or similar ethics committees for guidance. Unless these committees have specifically ruled on the issues, the private account is better accessed through more formal discovery methods.

Finally, given the constant flow of the digital world, lawyers must stay abreast of what is going on in the social landscape and how courts are responding. Technology and social media are rapidly advancing and a website that was not on the scene a year ago could become the next social-media goldmine. An attorney who fails to keep-up could jeopardize their client's case and their own professional well-being under the developing rules of attorney conduct. Navigating the social media minefield may seem daunting, especially for attorneys who do not quite comprehend the services. Because of social media's explosion, however, it is a necessary evil for any attorney.

X. Remaining Issues

Because social media platforms are constantly evolving and changing the ways people communicate, it seems that no hardline rules can be drafted that will fully encompass the mass of evidence drawn from these accounts. Therefore, courts will continually have to confront new and often complicated issues that will arise from the popularity of these platforms. Already, several prominent issues remain unresolved but may prove arduous to deal with in the near future.

With the continual push for increased social interaction, one question that probably cannot be answered with an exact definition is what exactly constitutes a social media account. While sites like Facebook and Twitter clearly fall into this category, a line has not yet been drawn for other, less socially-focused content providers such as retail outlets like Amazon or gaming services like Steam or Xbox Live. It remains unclear whether a discovery request seeking a litigant's social media account information obligates that litigant to turn over the credentials to these types of platforms. Amazon operates primarily as a retail agent but allows users to publish communications through reviews or other comments. Gaming communities also contain significant communications that could prove valuable for opposing counsel. If a party

claims extreme emotional distress but has been routinely and jubilantly participating in social gaming, opposing counsel would surely like access to any online communications that may divulge the true state of the complaining party's mentality. More and more websites and online platforms are offering some form of social interaction for users to accompany their primary services. It is unclear whether these websites must be categorized as social media accounts for discovery purposes.

Similarly, courts may have to define the scope of what constitutes a "document" for social media purposes. In general, the discovery rules, both federal and often state, refer to discovery and relevancy of a document. Rather than determining the relevancy of an entire collection of letters or other writings, the relevancy standard is generally applied on a document-by-document basis. While one letter or journal entry may be relevant, the rest of the collection may not be. Courts have not determined what constitutes a document when social media evidence comes into play. A post on Facebook, a single "Tweet" on Twitter, or even a blog entry can all constitute a document, but the issue become whether a collection of posts or blogs from a single day, hour, or month also constitute a document. While it may not appear to be that significant of an issue, it comes into play when determining what a party should have to turn over in response to discovery requests and whether that party has the right to black-out or hide certain postings surrounding a post relevant to the issue at hand.

Additionally, courts will have to eventually deal with the potential consequences of allowing counsel complete to a party's social media accounts if this trend were to continue. By forcing an individual to turn over his or her login credentials, the integrity of that social media account can be compromised, either purposefully or unintentionally. In today's society, it is no secret that some individuals take great pride in their social media profiles and expend countless

hours building a reputation or achieving certain feats in their online arenas. By submitting to a court order to turn over all login credentials, these individuals could be placing their online profiles at significant risk as a single accidental click could damage their online persona or even career. While integrity would ensure that nothing is done purposefully or vindictively, reparations such as sanctions may not be enough to repair a damaged profile, especially given the importance social media places on an online reputation.

Another issue that has not yet taken center stage but surely has the potential to, involves a website's terms of service and potential violations of the Computer Fraud and Abuse Act, an already muddied piece of legislation that has seen its fair share of criticism. Under the Act an individual can be subject to significant criminal or civil liability for fraudulently accessing a computer "without authorization."[111] Additionally, if an attorney were to create a fake account to access an individual's information the attorney would most likely be violating that service's terms of service for providing false information, which would again have the potential of running afoul of the Act. Whether an attorney could face culpability for attempting to access the social media accounts of an opposing party is unclear, but the broad and murky language of the act should put attorneys on notice that improper actions in the digital world are often not clearly defined but strictly punished.

Given the nature of social media and the fact that it can be deleted with the click of a mouse, rather than imposing significant penalties like sanctions or adverse inference charges after the damage has been done, it would be a better practice for all courts to implement litigation holds as soon as possible. This process would mandate that all parties retain social media postings or other electronically stored information that relates to the case at hand. While this

[111] See 18 § 1030(a)(4), (a)(5)(B)(i-v), (g).

process already exists at the federal level, and has been adopted by some state courts as well,[112] it should become uniform practice. This would obviate a great deal of spoliation litigation that currently plagues the courts concerning this type of frequently inflammatory evidence.

One of the often overlooked features of social media is the braggadocio that is often involved in the postings. Opposing parties and courts will currently have to struggle with what is truthful and what is not, because what one sees on social media is not always the entire story. Social norms and general human nature encourage users to post more about the positive occurrences in their lives as opposed to the drab or dreary. "Litigants' internal sentiments do not necessarily manifest in observable form, and therefore emotionally damaged or remorseful litigants would likely not post pictorial evidence of their true feelings on Facebook."[113] This can lead to tricky situations during discovery and at trial. As the Giachetto court recognized, "[t]he fact that an individual may express some degree of joy, happiness, or sociability on certain occasions sheds little light on the issue of whether he or she is actually suffering emotional distress."[114]

Finally, with regard to attorney ethics and the Model Rules of Professional Conduct, courts may have to specifically delineate what kind of speech actions like a "friend request" on Facebook or a "follow" on Twitter represents. While it is clear that an attorney using a false profile to garner information is acting unethically, it has not yet been uniformly established whether using a personal account with true information could constitute deception or a misrepresentation. This type of analysis would hinge on what a friend request or a follow actually means. The ethics committees from New York and Philadelphia have already

[112] See Zubulake v. UBS Warburg LLC, 229 F.R.D. 422 (S.D.N.Y. 2004).
[113] Kathryn R. Brown, Note, "The Risks of Taking Facebook at Face Value: Why the Psychology of Social Networking Should Influence the Evidentiary Relevance of Facebook Photographs," 14 Vand. J. Ent. & Tech. L. 357, 381–82 (2012).
[114] 2013 WL 2897054 at *8.

demonstrated divergent views as to the nature and intent inherent in sending a Facebook friend request. A friend request on Facebook could mean that the individual wants to share in a legitimate social relationship online. It could also mean that upon accepting the request, an individual is granting that new "friend" complete and unfettered access to a bevy of personal information even though the identity of the individual is unknown. It all depends on how the act of sending the request is interpreted and the true meaning behind it. Courts and bar associations must determine whether a friend request, sent from a personal account, can still be deceptive in that it materially misrepresents the relationship the attorney is establishing with the third party or fails to be forthcoming with all the material facts. Each social media platform has its own terminology and methods for allowing users to share information. There are Tweets, posts, blogs, likes, shares, retweets, subscriptions, and favorites, just to name a few. Because it is unclear what these actions communicate to others, courts will continue to struggle with the ethical issues that social media presents.

The creation and commercialization of each new social media platform only creates more issues for the courts to confront. While it remains to be seen how courts will continue to handle these issues, it is clear that the current digital era provides a bevy of information that will continue to be mined for litigation. The only true weapon courts can wield in battling the confrontations that arise is a better understanding of the technology and the platforms being utilized. Just as lawyers must keep abreast of the interplay between technology and the law, the legal system must also be held to the same standard.

XI. Conclusion

Continued advances in technology may eventually force legislatures to draft new rules of discovery specifically tailored to social media, but until then courts will determine these discovery issues using the existing rules of discovery. While this process has allowed courts to

maintain the status quo, attorneys have not been able to successfully escape the effects of the social media blitzkrieg on society. With new rules of conduct and ethics being generated by bar associations in each state, responsible attorneys must understand and adapt to the issues the technology presents. Failure to do so will jeopardize not only their clients' cases but also their standing in the legal community. The social media fervor is not fading, and its rise has forever altered the way people communicate on a daily basis. Both attorneys and the judicial system as a whole will continue to feel its effects and must continue to adapt as the technology progresses and its legal use amplifies.