The Implications of the Social Media Revolution on Discovery in U.S. Litigation

By Jonathan E. DeMay
Jonathan E. DeMay is a partner in the New York office of Condon & Forsyth LLP and principally focuses on representing clients relating to major aviation accidents, commercial transactions, products liability, aircraft financing transactions, aircraft hull damage claims, and general aviation. He frequently counsels clients about electronic discovery and social media issues. DeMay can be reached at jdemay@condonlaw.com.

TIP
Seek discovery of social media via narrowly tailored discovery requests directed at the user, coupled with requests for authorizations to obtain relevant records from the social media site, rather than serving a subpoena directly on the social media provider without user consent.

We are in the midst of what has been described as a social media revolution. This revolution is changing the way individuals,[1] companies,[2] and governments[3] organize, navigate, and share information, as well as the very nature of privacy.[4] The explosive growth of social media, coupled with the continuing transition from the use of desktop and laptop computers to increasingly powerful mobile devices, has provided virtually instantaneous and constant access to an increasingly interconnected digital world and, correspondingly, increased litigation risk.

Facebook, YouTube, and Twitter, three of the most popular social media sites, provide examples of the growth of social media. Facebook was launched on February 4, 2004, from a Harvard University dorm room and has since grown into one of the most influential companies in the world. The breadth of Facebook is staggering. It has over 500 million active users—50 percent of whom log on daily. Users send approximately four billion messages per day via Facebook Messages and upload more than three billion photos per month. More people play games on Facebook than on Xbox 360, PlayStation 3, and Wii combined.[5] YouTube, an online video community founded in February 2005, has more than two billion videos viewed and hundreds of thousands of videos uploaded per day. Twitter, a social networking and microblogging site founded in March 2006, has approximately 200 million registered accounts, and 110 million "tweets" per day.[6]

Other social media sites include Myspace, LinkedIn, Habbo, Flickr, Friendster, Digsby, Orkut, Bebo, Hi5, and FourSquare. The rise and fall of Myspace underscores the volatility of social media. Launched in January 2004, Myspace was the world's largest social network until its user growth stagnated and it was overtaken by Facebook. It now has approximately 63 million unique users—about half of its audience from one year ago and representing a loss of 10 million visitors from January to February 2011 alone.[7]

Despite its inherent fluidity, it is increasingly clear that social media has fundamentally changed the way many individuals live their lives and companies conduct business. In this environment, issues relating to the use of social media have increasingly arisen during litigation.[8] In some instances, it may even level the playing field relating to electronic discovery. Typically, companies generate far more traditional electronically stored information than do individuals. As a result, corporate defendants in U.S. litigation generally bear a disproportionate amount of the costs and risks associated with electronic discovery when compared with a typical individual plaintiff. Social media provides parties with the opportunity to obtain information about which they would most likely be unaware if pursued only from more traditional sources of discovery. In smaller, personal injury-type cases, social media is more likely to be a boon to defendants than to plaintiffs. One easily could envision a plaintiff posting photographs or comments on a social media site that prove damaging to his or her claims, for example, a personal injury plaintiff posting photographs from an adventure vacation despite claims of severe and permanent injuries that have confined the plaintiff to bed. In contrast, social media may be more beneficial to plaintiffs in litigation arising from a wrongful death case, where it is less likely that a decedent will have posted a photograph or comment that will materially affect the lawsuit and more likely that a company employee has made adverse, disparaging, or out-of-context statements that might negatively affect the company's defense.

This article provides an overview of the case law addressing the discoverability of social media to assist practitioners in pursuing that discovery. While the law relating to the discoverability of social media is still developing with trends and issues continuing to emerge, the case law provides guidance to a party seeking such discovery. This article examines some of the more significant decisions[9] before setting forth general guidelines to follow when pursuing discovery from social media sites.

The Case Law of Social Media Discoverability

Mackelprang v. Fidelity National Title Agency of Nevada, Inc.[10] In this case, the court addressed a discovery dispute relating to a plaintiff's two Myspace.com Internet accounts. The dispute arose in the context of a lawsuit in which the plaintiff claimed, inter alia, sexual harassment and emotional distress during the course of her employment, including coercion to engage in sexual relations with a company vice president under threat that if she did not do so, her husband would be fired from his position at the same company.

The court addressed the defendant's motion to compel production of e-mail communications on the two Myspace

Published in *The Brief*, Volume 40, Number 4, Summer 2011.

accounts that allegedly had been set up by the plaintiff.[11] One Myspace account allegedly identified the plaintiff as a 39-year-old single female who did not want children. The other Myspace account allegedly identified the plaintiff as a 39-year-old married woman who loved her six children.

The defendant had served a subpoena on Myspace.com to produce all records for the accounts, including private e-mails between the plaintiff and other persons. Myspace.com had produced "certain 'public' information" relating to the accounts but declined to produce private e-mails from either account absent "a search warrant or a letter of consent to production by the owner of the account."[12] Thereafter, the defendant sent a letter and a consent and authorization for private messages to the plaintiff requesting that she execute the authorization for the defendant to obtain the private messages from her two Myspace accounts. The plaintiff refused to execute the authorization because she claimed the information sought was irrelevant and that the request violated her privacy.

The defendant argued that the plaintiff was a willing participant in the alleged sexual communications and conduct and that she used one of the Myspace accounts to facilitate these types of relationships. In its motion to compel, the defendant offered to stipulate that any private Myspace messages that were produced would be subject to a protective order to protect any privacy interests.

In denying the defendant's motion to compel, the court noted that the defendant had "no information" relating to the identities of the persons with whom the plaintiff had exchanged e-mails or about the content of those e-mails. The court also noted that the Myspace accounts were opened after the plaintiff had left the defendant's employment, and that even if one of the Myspace accounts contained sexually related e-mail messages between the plaintiff and others, this evidence would not be admissible to support the defendant's defense that its prior alleged sexual conduct was welcomed by the plaintiff.[13] The court stated that the defendant was engaged in a "fishing expedition" with nothing more than suspicion that the e-mails could contain sexually explicit content.[14] As such, the court found that the defendant's suspicion that the plaintiff's Myspace private e-mail messages could contain sexually explicit or promiscuous content failed to demonstrate a relevant basis for their production.[15]

The court also rejected the defendant's argument that it was entitled to production of the Myspace private e-mail messages because they could contain statements by the plaintiff and witnesses about the subject matter of the lawsuit, including other potential causes of her alleged severe emotional distress. The court found that seeking a release for all private e-mails on the plaintiff's Myspace accounts "cast too wide a net" for information that could be relevant—and that this could result in the production of irrelevant sexually explicit or promiscuous e-mail communications between the plaintiff and third persons.[16] (Although not requested by either party, the court also declined to conduct an in camera review to determine if the e-mails contained relevant information.[17]) However, the court found that the defendant was entitled to seek information relating to the plaintiff's alleged mental condition via "properly limited requests for production of *relevant* email communications," such as private Myspace messages that contain information relating to her sexual harassment allegations or that discuss her alleged emotional distress and its causes.[18]

EEOC v. Simply Storage Management, LLC.[19] In this case, the court addressed whether two claimants were required to produce Internet social networking site profiles and other communications from their Facebook and Myspace accounts in the context of a workplace sexual harassment claim, including allegations of severe emotional distress. The court framed the "main challenge" of the case as defining "appropriately broad limits—but limits nevertheless—on the discoverability of social communications in light of a subject as amorphous as emotional and mental health, and to do so in a way that provides meaningful direction to the parties."[20]

The court found the appropriate scope of relevance to be "any profiles, postings, or messages (including status updates, wall comments, causes joined, groups joined, activity streams, blog entries)" and social networking site applications for the claimants for the relevant time period that related to "any emotion, feeling, or mental state," as well as any communications that related to "events that could reasonably be expected to produce a significant emotion, feeling, or mental state."[21]

The court also found that third-party communications to the claimants should be produced if the communications put the claimants' communications into context.[22] In addition, the court found that photographs of a claimant during the relevant time period and posted on a claimant's profile generally will be discoverable "because the context of the picture and the claimant's appearance may reveal the claimant's emotional or mental status. On the other hand, a picture posted on a third party's profile in which a claimant is merely 'tagged,' is less likely to be relevant. In general, a picture or video depicting someone other than the claimant is unlikely to fall within the definition set out above."[23]

In so finding, the court did not attach great significance to the possibility that the discovery of the claimants' social networking sites could reveal private information that embarrassed them.[24] The court noted that a person's expectation that his or her communications be kept private was not a legitimate basis for shielding those communications from discovery. It stated that privacy and confidentiality concerns could be addressed by an appropriate protective order.[25] The court further stated that any privacy concern was outweighed by the fact that, inter alia, the claimants had already shared the information with at least one other person through private messages or with a larger number of people through postings.[26] In this regard, the court noted that "□'Facebook is not used as a means by which account holders carry on monologues with themselves.'□"[27]

Bass v. Miss Porter's School.[28] This case involved a lawsuit arising out of a student's suspension from school as the result of cheating on an exam. The court addressed the defendants' request for production seeking documents about a plaintiff's alleged teasing and taunting via text messages and Facebook, and documents concerning communications between the plaintiff and "anyone else" relating to the allegations in the amended complaint. The plaintiff objected to the requests on several grounds, including that the requests sought documents that were irrelevant and not reasonably calculated to lead to the discovery of admissible evidence.

The plaintiff subsequently served a subpoena on Facebook to obtain records from her former Facebook account, to which she claimed she had lost access before commencing her lawsuit. Thereafter, the plaintiff and Facebook reached a stipulated agreement that Facebook would release "reasonably available data" from the plaintiff's Facebook profile. The court then ordered the plaintiff to produce all documents from Facebook that were relevant to the defendants' discovery requests and to provide to the court a complete set of the documents provided to the plaintiff by Facebook for in camera review. The plaintiff provided the court with 750 pages of Facebook wall postings, messages, and photographs, only 100 pages of which had been produced to the defendants.

In reviewing the documents from Facebook, the court noted that there was no "meaningful distinction" between the documents produced and those withheld from production, and stated:

> Facebook usage depicts a snapshot of the user's relationships and state of mind at the time of the content's posting. Therefore, relevance of the content of Plaintiff's Facebook usage as to both liability and damages in this case is more in the eye of the beholder than subject to strict legal demarcations, and production should not be limited to Plaintiff's own determination of what may be "reasonably calculated to lead to the discovery of admissible evidence."[29]

The court ordered the plaintiff to disclose the previously nondisclosed portion of the Facebook documents to the defendants.[30]

Crispin v. Christian Audigier, Inc.[31] In this case, the court addressed a lawsuit against various licensees relating to the use of a plaintiff's artwork. The defendants had served subpoenas duces tecum on several third parties, including Media Temple, Inc.,[32] Facebook, and Myspace, Inc. The subpoenas directed to Media Temple, Facebook, and Myspace sought basic subscriber information as well as all communications with various entities, including the defendants. The plaintiff moved to quash the subpoenas on three grounds, the most significant of which was that the Stored Communications Act (SCA)[33] prohibited third-party Internet providers from disclosing the type of electronic communications sought by the defendants. The magistrate judge found that the SCA did not apply because (1) the third-party businesses were not electronic communication service (ECS) providers as defined in the statute, (2) it only precludes voluntary disclosure by ECS providers and not disclosure compelled by subpoena, and (3) it precludes only the disclosure of communications held in "electronic storage" by the ECS provider and the materials were not in electronic storage within the meaning of the statute.[34] The plaintiff moved the district court to reconsider the magistrate judge's decision that Media Temple, Facebook, and Myspace are not subject to the SCA.

In considering the plaintiff's motion, the district court closely examined the SCA. The SCA was enacted in 1986 as part of the Electronic Communications Privacy Act[35] "□'because the advent of the Internet presented a host of potential privacy breaches that the Fourth Amendment does not address.'□"[36] The SCA prevents providers of communication services from disclosing private communications to certain types of entities and individuals. It limits the government's ability to compel a provider to disclose information in its possession about its customers and subscribers. Furthermore, it limits the right of an Internet service provider to divulge information about customers and subscribers to the government voluntarily.

The SCA distinguishes between an ECS provider and a remote computing service (RCS) provider, which are subject to different standards of care. An ECS provider is defined as "□'any service which provides to users thereof the ability to send or receive wire or electronic communications.'□"[37] An ECS provider cannot "□'knowingly divulg[e] to any person or entity the contents of a communication while in electronic storage by that service.'□"[38]

An RCS is defined as "□'the provision to the public of computer storage or processing services by means of an electronic communications system.'□"[39] An RCS provider cannot "□'knowingly divulg[e] to any person or entity the contents of any communication which is carried or maintained on that service.'□"[40] Furthermore, the RCS provider cannot disclose "the content of any communication received by electronic transmission that is carried or maintained on its service for a customer or subscriber 'solely for the purpose of providing storage or computer processing services to [the] subscriber or customer, if the provider is not authorized to access the contents of [the] communications for purposes of providing . . . services other than storage or computer processing.'□"[41]

In reviewing the plaintiff's motion, the district court rejected the defendants' argument that the plaintiff lacked standing to move to quash the subpoenas served on the third parties.[42] The court also rejected the defendants' argument that the SCA explicitly permitted service of a subpoena duces tecum.[43] The court stated that the SCA established a "complex scheme" by which a "governmental entity can, after fulfilling certain procedural and notice requirements, obtain information from an RCS provider via administrative subpoena or grand jury or trial subpoena."[44] It allows a government entity to obtain "information from an ECS provider only pursuant to criminal warrant if the communication has been held by the provider for fewer than 180 days."[45] "In all other cases, the governmental entity can obtain information from an ECS provider using the

subpoena procedures set forth in § 2703(b)."[46] The court noted that the statute "does not mention service of a civil subpoena duces tecum."[47]

The district court next considered whether the subpoenas should be quashed pursuant to the SCA. To make this determination, it examined whether social media providers fall within the ambit of the SCA and, if so, whether the information sought by the subpoenas (i.e., private messages and postings) is electronic storage within the meaning of the SCA. The court noted that the parties had only provided "minimal facts" about Media Temple, Facebook and Myspace. The court found that Media Temple, Facebook, and Myspace provided private messaging or e-mail services and, therefore, such services constitute ECSs.[48]

The court found authority relating to private bulletin board services (BBS) to be relevant to its analysis.[49] In this regard, the court found that the SCA definition of an ECS provider was "intended to reach a private BBS," but also found that case law "[u] nquestionably" required that a BBS be "restricted in some fashion"; a "completely public" BBS is not afforded protection under the SCA.[50] The information submitted by the parties established that Facebook wall postings and Myspace comments are "not strictly 'public,' but are accessible only to those users plaintiff selects."[51]

With respect to Media Temple's webmail service and Facebook's and Myspace's private messaging, the district court found that the entities operated as ECS providers.[52] The messages, if not yet opened, were considered to be in electronic storage because they are "temporary, intermediate storage" within the meaning of 18 U.S.C. § 2510(17)(A). If, however, the messages had been opened and retained by the plaintiff, the three entities were considered RCS providers supplying storage services.[53]

The district court noted that the determination whether Facebook and Myspace were ECS or RCS providers as to Facebook wall and Myspace comments presented "a distinct and more difficult question."[54] The court noted that "the difficulty in interpreting the statute is 'compounded by the fact that the [SCA] was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like [Facebook and Myspace]. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.' As the Ninth Circuit further observed, 'until Congress brings the laws in line with modern technology, protection of the Internet and websites such as [these] will remain a confusing and uncertain area of the law.' □"[55]

The district court stated that there is no temporary, intermediate step for postings or comments on a social networking site, as there is no point where, for example, a Facebook wall posting needs to be opened. As a result, a Facebook wall posting or a Myspace comment cannot be protected as a form of temporary, immediate storage. However, the court found that the postings, once made, were stored for backup purposes. The court concluded that Media Temple, Facebook, and Myspace are ECS providers—and Facebook and Myspace are ECS providers in regard to wall postings and comments, and that such communications are in electronic storage.[56] Alternatively, the court found that Facebook and Myspace are RCS providers in regard to the wall postings and comments. In so finding, the court noted that the number of users who could view the stored message is of no legal significance and that, in the context of the RCS definition, "it does not matter that the stored Facebook wall postings and MySpace comments are available to hundreds or thousands of approved users."[57]

The district court then quashed the Media Temple subpoena and the portions of the Facebook and Myspace subpoenas that sought private messaging. As to the portions of the subpoenas seeking Facebook wall postings and Myspace comments, the district court concluded that the factual record was insufficient for a determination whether access to the postings and comments was sufficiently restricted. The district court vacated this portion of the magistrate judge's ruling and remanded it for further evidentiary development.[58]

McCann v. Harleysville Insurance Co. of New York.[59] In this case, the New York State appellate court, in a perfunctory decision, addressed two appeals arising from lawsuits relating to injuries allegedly sustained in a motor vehicle accident. In each appeal, the defendant challenged the trial court's order denying its motion to compel, inter alia, "an authorization for plaintiff's Facebook account."[60] The defendant argued that the information was relevant to whether the plaintiff sustained a serious injury in the accident. The appellate court was not persuaded, stating that the defendant had failed to establish a factual predicate relating to the relevancy of the evidence but rather "sought permission to conduct 'a fishing expedition' into plaintiff's Facebook account on the mere hope of finding relevant evidence."[61] The defendant, however, was not prohibited from seeking discovery of the plaintiff's Facebook account at a future date.[62]

Romano v. Steelcase Inc.[63] In this case, the defendant sought an order allowing it access to the plaintiff's current and historical Facebook and Myspace pages and accounts, including all deleted pages. The defendant argued that the plaintiff had posted information on these sites that was factually inconsistent with the plaintiff's claims about the extent and nature of her injuries. The plaintiff claimed she had sustained permanent injuries that prevented her from participating in certain activities and also impacted her enjoyment of life. The defendant contended that publicly accessible Facebook and Myspace pages revealed that the plaintiff enjoyed an active lifestyle and traveled during the time period she claimed she was limited by her injuries. The defendant attempted to question the plaintiff relating to her Facebook and Myspace accounts at her deposition without success and, thereafter, served discovery requests seeking "authorizations to obtain full access to and copies of Plaintiff's current and historical records/information on her Facebook and MySpace accounts."[64] The plaintiff did not provide

the defendant the requested authorizations.

The trial court noted that the SCA "prohibits an entity, such as Facebook and MySpace from disclosing . . . information without the consent of the owner of the account."[65] The court interpreted the permissible scope of discovery under New York Civil Practice Law and Rules Section 3101 as requiring "full disclosure of all non-privileged matter which is material and necessary to the defense or prosecution of an action."[66] The court added that it had "broad discretion" in determining what is material and necessary and that this standard is interpreted liberally, requiring disclosure of "any facts" relating to the controversy that will assist in the preparation for trial.[67]

The trial court found the requested information material and necessary.[68] The court stated that it appeared that the plaintiff was "smiling happily" in a photograph outside of her home despite her claim that she had sustained permanent injuries and was "largely confined to her house and bed."[69] The court found that because public portions of the social networking sites contained material that was contrary to her claims and deposition testimony, there was a reasonable likelihood that private portions of her sites might contain further relevant information relating to her activities and enjoyment of life.[70] The court concluded that preventing the defendant from accessing the plaintiff's private postings on Facebook and Myspace would be inconsistent with the liberal disclosure policy in New York and also would condone the plaintiff's attempt to "hide relevant information behind self-regulated privacy settings."[71]

The court also found that this disclosure would not violate the plaintiff's right to privacy because a user of social media does not have a reasonable expectation of privacy about the information the user posts or shares.[72] After reviewing, inter alia, the Facebook privacy policy, which advised that security measures for the website were not "perfect or impenetrable" and that personal information posted or shared on the site "may become publicly available," the court concluded that

> when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings. Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist. Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. As recently set forth by commentators regarding privacy and social networking sites, given the millions of users, "[i]n this environment, privacy is no longer grounded in reasonable expectations, but rather in some theoretical protocol better known as wishful thinking."[73]

The court further found that the defendant's need for access to the information outweighed any privacy concerns raised by the plaintiff and granted the defendant access to the plaintiff's "current and historical Facebook and MySpace pages and accounts, including all deleted pages and related information."[74] It likewise required the plaintiff to provide the defendant a "properly executed consent and authorization as may be required by the operators of Facebook and MySpace, permitting said Defendant to gain access to Plaintiff's Facebook and MySpace records, including any records previously deleted or archived by said operators. . . ."[75]

McMillen v. Hummingbird Speedway, Inc.[76] In this case, the plaintiff sought damages for personal injuries allegedly sustained when he was involved in a rear-end collision during a stock car race. He alleged "possible permanent impairment, loss and impairment of general health, strength, and vitality, and inability to enjoy certain pleasures of life."[77] During discovery, defendant Hummingbird sought information about any social networking sites the plaintiff used, as well as his associated user names, log-in names, and passwords. The plaintiff responded by stating that he had Facebook and Myspace accounts but objected to providing his user names and log-in information, which he maintained were confidential.

The defendant reviewed the public portion of the plaintiff's Facebook account and discovered comments about a fishing trip and attending the Daytona 500 race in Florida. Thereafter, the defendants moved to compel the production of the plaintiff's user names, log-in names, and passwords, arguing that the plaintiff's social media accounts could contain further evidence that could impeach or contradict his disability or damages claims.

The trial court evaluated the motion under Pennsylvania state discovery rules, under which "nearly any" relevant materials are discoverable. The plaintiff argued that the court should recognize that communications shared with one's private friends on social network sites are confidential and protected from disclosure. The court noted that Pennsylvania had not adopted a "□'social network site privilege'□" and that Pennsylvania law generally disfavors privileges. The court stated that a new privilege would not be recognized unless it was established: "1.) that his communications originated in the confidence that they would not be disclosed; 2.) that the element of confidentiality is essential to fully and satisfactorily maintain the relationship between the affected parties; 3.) community agreement that the relationship must be sedulously fostered; and 4.) that the injury potentially sustained to the relationship because of the disclosure of the communication outweighs the benefit of correctly disposing of litigation."[78]

In evaluating the plaintiff's social media site privilege claim, the court stated:

> Facebook, MySpace, and their ilk are social network computer sites people utilize to connect with friends and meet new people. That is, in fact, their purpose, and they do not bill themselves as anything else. Thus, while it is conceivable that a person could use them as forums to divulge and seek advice on personal and private matters, it would be unrealistic to expect that such disclosures would be considered confidential.[79]

Thereafter, the court examined the Facebook privacy policy and found that Facebook users are "put on notice that

regardless of their subjective intention when sharing information, their communications could nonetheless be disseminated by the friends with whom they share it, or even by Facebook at its discretion. Implicit in those disclaimers, moreover, is that whomever else a user may or may not share certain information with, Facebook's operators have access to every post."[80] After examining the Myspace privacy policy, the court found that Myspace operators have similar access to a user's content or conduct. As such, the court concluded that the "complete access" provided to Facebook and Myspace operators defeated the plaintiff's claim that his communications were confidential.[81] Furthermore, the court found that the relationships fostered through social media are "basic friendships," which do not depend on confidentiality, and that any relational harm resulting from disclosure of social media content is "undoubtedly outweighed" by the benefit of correctly disposing of litigation.[82]

The court noted that the plaintiff had alleged significant injuries and that the publicly accessible portion of his Facebook page revealed posts that the defendants contended showed that the plaintiff was exaggerating his injuries. The court found it reasonable to assume that the plaintiff may have had additional observations about his travels and activities in private posts not otherwise available to the defendants and gaining access to them could refute the plaintiff's claims.[83] Accordingly, the court found that "[w]here there is an indication that a person's social network sites contain information relevant to the prosecution or defense of a lawsuit . . . access to those sites should be freely granted."[84] Accordingly, the court ordered the plaintiff to produce his Facebook and Myspace user names and passwords and to preserve existing information and posts on these social media accounts.[85]

Conclusion

While case law addressing the discovery of social media—like social media itself—is still developing, there are a number of guidelines that are helpful when pursuing discovery from social media sites. First, an attorney should not attempt to gain access to a social network account (e.g., by "friending" a plaintiff or defendant) under false pretenses, either directly or via an agent.[86] Second, it generally is not advisable to seek social media discovery by subpoena served directly on the social media provider without user consent. Instead, if a party in civil litigation seeks the discovery of social media, it generally is preferable to do so via discovery requests directed at the user coupled with requests for written authorizations to obtain the relevant records from the social media site. Third, the discovery requests should be narrowly tailored to seek information and documents relevant to the lawsuit. Fourth, a court is more likely to find the social media relevant and properly discoverable if publicly accessible portions of the party's social media accounts are inconsistent with its allegations in the complaint or in its discovery responses or testimony. In this regard, it often is helpful to locate the party's social media accounts and create screen shots of the accounts in the early stages of the case to help identify, preserve, and develop information about any inconsistencies. A number of social media aggregator websites (e.g., Spokeo) can assist a party with the process of identifying a person's social media accounts. Fifth, if a party objects to discovery requests relating to social media accounts on privacy grounds, the party seeking the discovery should be willing to enter into a confidentiality agreement to lessen any privacy concerns of the court. Also, as a practical matter, a party should try to determine how many persons have access to the "private" portion of the social media account. For example, if a plaintiff limits access to his or her Facebook account to Facebook "friends," any privacy concerns will be diminished if the plaintiff has 600 such friends who can view the plaintiff's postings.

Endnotes

1. As of September 2009, approximately 73 percent of online U.S. Internet users aged 12 to 17 used social media. *See* Amanda Lenhart et al., *Social Media and Young Adults*, PEW INTERNET, Feb. 3, 2010, www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx (last visited May 16, 2011). It would be a mistake, however, to assume that social media use is limited to young adults. As of May 2010, 47 percent of Internet users aged 50 to 64 used social media, and 26 percent of Internet users aged 65 and over used social media—a growth of 88 percent and 100 percent, respectively, from the prior year. *See* Mary Madden, *Older Adults and Social Media*, PEW INTERNET, Aug. 27, 2010, www.pewinternet.org/Reports/2010/Older-Adults-and-Social-Media.aspx (last visited May 16, 2011).

2. As of 2010, approximately 56 percent of Fortune 500 companies had a corporate Facebook account, and approximately 60 percent had a corporate Twitter account. *See* Nora Ganim Barnes, *The Fortune 500 and Social Media: A Longitudinal Study of Blogging, Twitter and Facebook Usage by America's Largest Companies*, UMASS-DARTMOUTH CENTER FOR MARKETING RESEARCH, www.umassd.edu/cmr/studiesandresearch/bloggingtwitterandfacebookusage/ (last visited May 16, 2011).

3. *See, e.g.*, Gary Strauss & Mimi Hall, *State Department Taps Twitter to Reach Iranians*, U.S.A. TODAY, Feb. 15, 2011, www.usatoday.com/news/world/2011-02-15-statetwitter15_ST_N.htm (use of Twitter by U.S. State Department to communicate directly with Iranians); J. David Goodman, *World Leaders Cheer but Remain Wary*, N.Y. TIMES, Feb. 11, 2011, www.nytimes.com/2011/02/12/world/middleeast/12global.html (noting that a number of governments made statements about the Egyptian revolution via Twitter).

4. *Cf.* City of Ontario, Cal. v. Quon, 130 S. Ct. 2619, 2629 (2010) ("Rapid changes in the dynamics of communication and information transmission are evident not just in the technology itself but in what society accepts as proper behavior.").

5. *See* David Gelles, *Facebook's Grand Plan for the Future*, FT MAGAZINE, Dec. 3, 2010, www.ft.com/cms/s/2/57933bb8-fcd9-11df-ae2d-00144feab49a.html.

6. *See* Oliver Chiang, *Twitter Hits Nearly 200M Accounts, 110M Tweets per Day, Focuses on Global Expansion*, FORBES, Jan. 19, 2011, http://blogs.forbes.com/oliverchiang/2011/01/19/twitter-hits-nearly-200m-users-110m-tweets- per-day-focuses-on-global-expansion/.

7. *See* Michael Arrington, *Amazingly, MySpace's Decline Is Accelerating*, TECHCRUNCH, Mar. 23, 2011, http://techcrunch.com/2011/03/23/amazingly-myspaces-decline-is-accelerating/.

8. *See, e.g.*, United States v. Phaknikone, 605 F.3d 1099, 1101 (11th Cir. 2010) (addressing whether district court properly admitted a criminal defendant's Myspace profile page, subscriber report, and photographs); United States v. Fumo, 639 F. Supp. 2d 544, 555 (E.D. Pa. 2009) (addressing juror use of Twitter, Facebook, and personal web page during criminal trial); Pietrylo v. Hillstone Restaurant Group, No. 06-5754, 2008 WL 6085437, at *1 (D.N.J. July 25, 2008) (addressing company managers allegedly obtaining improper access to an employee's private Myspace group).

9. Although not addressed in this article, a number of other decisions address the discoverability of social media. *See, e.g.*, Barnes v. CUS Nashville, LLC, No. 3:09-cv-00764, 2010 WL 2265668, at *1 (M.D. Tenn. June 3, 2010) (magistrate judge proposed creating a Facebook account to view nonparty Facebook photographs and related comments in camera); Ledbetter v. Wal-Mart Stores, Inc., No. 06-cv-01958, 2009 WL 1067018 (D. Colo. Apr. 21, 2009) (addressing subpoenas served on Facebook, Myspace, and Meetup.com); Viacom Int'l Inc. v. YouTube Inc., 253 F.R.D. 256, 259 (S.D.N.Y. 2008) (addressing motion to compel YouTube and Google to produce electronically stored information and documents in context of copyright action).

10. No. 2:06-cv-00788, 2007 WL 119149 (D. Nev. Jan. 9, 2007).

11. In this opinion, the court interchangeably refers to the defendant or defendants. For purposes of simplicity, this article refers to the defendant.

12. *Id.* at *2.

13. *See id.* at *6.

14. *See id.* at *2, *6.

15. *Id.*

16. *Id.* at *7.

17. *Id.* at *8.

18. *Id.*

19. 270 F.R.D. 430 (S.D. Ind. 2010).

20. *Id.* at 434.

21. *Id.* at 436.

22. *Id.*

23. *Id.* The court defined tagging as "the process by which a third party posts a picture and links people in the picture to their profiles so that the picture will appear in the profiles of the person who 'tagged' the people in the picture, as well as on the profiles of the people who were identified in the picture." *Id.* at n.3.

24. *See id.* at 437.

25. *Id.* at 434.

26. *Id.* at 437.

27. *Id.* (quoting Leduc v. Roman, 2009 CanLII 6838 (Can. Ont. Sup. Ct. Feb. 2, 2009)).

28. No. 3:08cv1807, 2009 WL 3724968 (D. Conn. Oct. 27, 2009).

29. *Id*. at *1.

30. *Id.* at *2.

31. 717 F. Supp. 2d 965 (C.D. Cal. 2010).

32. Media Temple, Inc., is a web hosting and virtualization service provider. It provides businesses with services to host websites, e-mail, business applications, and other Internet content. *See* Media Temple, About Us, http://mediatemple.net/company/about.php (last visited May 16, 2011).

33. 18 U.S.C. §§ 2701–2712.

34. 717 F. Supp. 2d at 969–70.

35. 18 U.S.C. §§ 2510–2522.

36. 717 F. Supp. 2d at 971 (quoting Quon v. Arch Wireless Operating Co., 529 F.3d 892, 900 (9th Cir. 2008)).

37. *Id.* at 972 (quoting 18 U.S.C. § 2510(15)).

38. *Id.* (quoting 18 U.S.C. § 2702(a)(1), (b)).

39. *Id.* (quoting 18 U.S.C. § 2711(2)).

40. *Id.* (quoting 18 U.S.C. § 2702(a)(2)).

41. *Id.* (quoting 18 U.S.C. § 2702(a)(2)).

42. *Id.* at 973, 976.

43. *Id.* at 974–76.
44. *Id.* at 974–75.
45. *Id.* at 975.
46. *Id.*
47. *Id.*
48. *See id.* at 980.
49. *Id.* □50. *Id.* at 981.
51. *Id.* at 980.
52. *Id.* at 987.
53. *Id.*
54. *Id.* at 988.
55. *Id.* (quoting Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002)). In *Konop*, the plaintiff, a Hawaiian Airlines pilot, commenced a lawsuit against Hawaiian Airlines, alleging that it had accessed his secure website without authorization, disclosed its contents, and took other actions in violation of the federal Wiretap Act, the SCA, and the Railway Labor Act. 302 F.3d at 872. The plaintiff had created and maintained the website where he posted bulletins critical of Hawaiian Airlines and its officers, as well as the Air Line Pilots Association. The plaintiff controlled access to the website and created a list of people eligible to access it. A Hawaiian corporate officer obtained access to the website by use of two users authorized by the plaintiff to access it. The plaintiff claimed that Hawaiian thereafter retaliated against him due to the positions he articulated on the website. The Ninth Circuit Court of Appeals addressed whether Hawaiian Airlines violated the SCA based upon the manner in which the corporate officer accessed the plaintiff's website and, inter alia, reversed the district court's grant of summary judgment because the Ninth Circuit assumed that neither individual who provided access to the Hawaiian corporate officer was a "user" of the website within the meaning of the SCA at the time the corporate officer gained access. *Id.* at 880.
56. *Id.* at 982, 989.
57. *Id.* at 990.
58. *See id.* at 991.
59. 78 A.D.3d 1524 (N.Y. App. Div. 2010).
60. *Id*. at 1524.
61. *Id.* at 1525.
62. *Id.*
63. 907 N.Y.S.2d 650 (N.Y. Sup. Ct. 2010).
64. *Id.* at 653.
65. *Id.* at 652.
66. *Id.*
67. *Id.*
68. *Id.* at 654.
69. *Id.*
70. *Id.*
71. *Id.* at 655.
72. *Id.* at 655–56.
73. *Id.* at 657 (quoting Dana L. Fleming & Joseph M. Herlihy, *What Happens When the College Rumor Mill Goes Online? Privacy, Defamation and Online Social Networking Sites*, 53 B.B.J. 16 (Jan.-Feb. 2009)).
74. *Id*.
75. *Id.*
76. No. 113-2010 CD, 2010 WL 4403285 (Pa. Com. Pl. Sept. 9, 2010).
77. *Id*. at *1.
78. *Id.* at *2.
79. *Id.*
80. *Id.* at *3.
81. *Id.*
82. *Id.* at *3–4.
83. *Id.* at *4.
84. *Id.*
85. *Id.*
86. *See* New York City Bar Comm. on Prof. Ethics, Formal Op. 2010-2 (2010) ("Obtaining Evidence from Social Networking Websites").