New York Law Journal
E-Discovery
WWW.NYLJ.COM
An ALM Publication
VOLUME 256—NO. 65
MONDAY, OCTOBER 3, 2016

Social Media Investigations: Digging Deep, Or Just Scratching The Surface?

BY DANIEL M. BRAUDE AND DANIEL E. LUST

© ISCTOCK

Time and again, defendant corporations find themselves settling cases at inflated valuations simply to avoid the costs to preserve, review and produce substantial amounts of electronically stored information (ESI). In contrast, individual plaintiffs with very few documents to produce, if any, have been sitting back and relaxing throughout discovery.

This is changing as defendants increasingly use social media to turn the tables on plaintiffs. A well-known example involved the surviving husband in a wrongful death case in Virginia who shared a picture of himself on Facebook in which he was drinking a beer and wearing a t-shirt that read "I ♥ Hot Moms." His attorney instructed him to delete this picture, but not before it was spotted and retained by defense counsel, ultimately resulting in an adverse inference instruction to the jury and a fine of more than $700,000. *Allied Concrete v. Lester*, 285 Va. 295, 302 (2013).

Defendants can and should use photos, tweets, vines, snaps, emojis and whatever else can be pulled from a plaintiff's social media trail to potentially discredit the plaintiff and demonstrate that alleged damages are not based in reality. But are defense attorneys today properly digging through social media postings, or are they just scratching the surface?

New York's Social Media Authority

The creation of Facebook in 2004 kicked off the social media boom.

DANIEL M. BRAUDE, *a partner in Wilson Elser's New York and White Plains offices, is co-chair of the firm's e-discovery practice and serves as an adjunct professor at Pace University School of Law.* DANIEL E. LUST *is an associate in the White Plains office and focuses on general liability and transportation litigation.*

But it was not until September 2010 that New York courts dipped a toe into the treacherous social media waters and addressed the issue of discoverability. In *Romano v. Steelcase*, 30 Misc.3d 426 (Sup. Ct. Suffolk County, 2010), the court granted access to the plaintiff's complete Facebook and MySpace accounts, including private and deleted content, following production by defendants of public postings from both accounts that depicted the plaintiff's "active lifestyle" in contradiction to her claims:

> [W]hen 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….

In some situations, unfettered access to the private portion of a social media account could be characterized as a "fishing expedition." Yet, in *Romano*, the court focused on the existence of contradictory materials and determined that the defendants' right to discovery, specifically their need for materials hidden behind privacy settings, far outweighed the plaintiff's relative privacy interest. Two months later, the Appellate Division in *McCann v. Harleysville Ins. Co. of N.Y.*, 78 A.D.3d 1524 (N.Y. App. Div. 4th Dep't. 2010), articulated the standard that a party seeking social media content must establish "a factual predicate with respect to the relevancy of the evidence." Under this standard, access will likely be granted to a plaintiff's protected content where a defendant establishes a "factual predicate" by producing material found on "public" portions of social media platforms that sufficiently contradicts the nature and character of the plaintiff's claims or testimony.

Gaps in Social Media Authority and Guidance

The lasting impact from *Romano* and *McCann* is the commentary on plaintiff's diminished privacy interest and the application of the "factual predicate" standard to social media, respectively. This authority remains relevant and is still cited across courts in New York and around the country. See *Forman v. Henkin*, 134 A.D.3d 529, (N.Y. App. Div. 1st Dep't. 2015); *Breton v. City of New York*, 2016 WL 2897848 (Sup. Ct. New York Cty 2016); *Higgins v. Koch Dev.*, 2013 WL 3366278 (S.D. Ind. 2013); *Keller v. Nat'l Farmers Union Prop. & Cas. Co.*, 2013 WL 27731 (D. Mont. 2013). However, the rapid pace of innovation in social media has caused these 2010 opinions and their progeny to become outdated.

Compared to 2010, the current social media landscape is almost unrecognizable, with many notable platforms, including Instagram, LinkedIn, Twitter and Snapchat, gaining prominence over the past several years. In addition, the very definition of "social media" has been blurred as quasi-social and third-party mobile apps, such as Waze (a GPS app) and Venmo (a digital payment app), have developed followings. This begs the question of whether these platforms fall within the social-media-specific "factual predicate" standard.

A larger question looms: Should demonstration of a factual predicate through social media material on one platform permit access to private material on other platforms? To date, New York courts have largely treated individual accounts as discrete locations on which data can be stored. Is this a workable approach in light of "linking" functionality where users on one platform simultaneously post identical content across multiple platforms? The intermingling of accounts creates a scenario where courts will likely treat a plaintiff's social media content as consisting of a single portfolio of material rather than discrete and unrelated accounts.

Rapid innovation also has caused a lack of guidance regarding counsel's ethical obligations. Snapchat's process for viewing another user's postings provides a unique example. Traditional platforms such as

Facebook, Instagram, LinkedIn and Twitter offer publicly accessible landing pages for each user's profile while indicating whether certain content is accessible only to that user's "friends." This does not exist on Snapchat. Also, there is no traditional access ("friend") request where *mutuality* exists through an option to approve or deny the request. Instead, one's Snapchat postings can be viewed only by those that *unilaterally* "add" that user, a novel functionality not covered by the Social Media Ethics Guidelines of the Commercial and Federal Litigation Section of the New York State Bar Association, June 9, 2015. Once this "adding" occurs, the owner of the added account automatically receives a notification that he or she has been "added" by a certain user.

Could "adding" another user on Snapchat be considered an unethical communication with a person represented by counsel? The answer to this question *appears* to be no. A 2010 opinion of the New York State Bar Association's Committee on Professional Ethics (Formal Opinion No. 843), explicitly allowed an attorney to view publicly accessible portions of an opposing party's account. In addition, the American Bar Association's Standing Committee on Ethics and Professional Responsibility (Formal Opinion No. 466) explained in 2014 that LinkedIn's analogous page-view notification feature was not an impermissible communication, but only an innocuous communication between LinkedIn and the user. If this Snapchat "add" feature were deemed per se unethical, it would run contrary to these opinions. In fact, it would entirely prohibit viewing a user's publicly available content despite that user's lack of an expectation of privacy. This issue, among other social media-related ethical issues, has remained unanswered while Snapchat has grown into one of the most popular platforms. In any event, it is difficult to think that ethical guidance will be able to keep pace with social media's expansion.

Digging Deep

In contrast to the early days of Facebook, an individual's social media content is likely to be spread across multiple platforms. It is not enough to focus on Facebook and merely take screenshots from an easily identified account. This approach may overlook treasure troves of metadata, possibly pinpointing when and where a plaintiff visited a particular location, not to mention entire social media accounts that are not easily identified. In addition, the general population has increasingly implemented privacy settings and restricted access exclusively to approved "friends" or "followers." It also remains possible that some plaintiffs' attorneys may still follow the approach taken by counsel in *Lester v. Allied Concrete*, or at least recommend tweaks to their clients' privacy settings. Regardless, a proper social media investigation and forensic collection, which should be conducted early and often, will still frequently uncover useful material on anyone who maintains even a modest online presence.

In today's world, uncovering probative social media material requires much more than "Googling" a plaintiff's name and crossing your fingers. Attorneys must know the right questions to ask during discovery. This is not limited to straightforward questions about name-brand platforms such as Facebook and Twitter, but includes questioning designed to uncover the use of lesser-known platforms and third-party mobile apps or to confirm ownership of accounts using pseudonyms or misleading profile usernames.

A proper investigation does not stop with a plaintiff's accounts, but extends to friends and relatives whose profiles may not be hidden behind privacy settings. It is no longer enough to merely understand the law. Counsel today must develop a thorough understanding of a wide variety of social media platforms and third-party apps, or associate with one who does, especially when technology develops at a lightning pace and where fads come and (Pokémon) go in the blink of an eye.