

DAILY BUSINESS REVIEW

LEGAL

Metadata from social networks can be crucial evidence



by Elisa J. D'Amico and Marc Hirschfeld

From geotags to hash tags, social media has become a primary method of communicating for individuals and businesses, presenting new opportunities as well as legal challenges. For many individuals, staying in touch with friends, family and colleagues involves myriad electronic communication tools, including text messaging and other messaging applications, Facebook, Skype, LinkedIn and email.

Along with the new opportunities come new legal challenges. And while social media users revel in the instant gratification that social media facilitates, far too many do not consider the trail of evidence that their messaging, blogging and posting leaves behind.

Over the past decade, the Internet has evolved from a one-dimensional source of information (the "World Wide Web") to an interactive playground that allows users to contribute to website content with a few keystrokes ("Web 2.0"). The interactive nature of the Web 2.0 platform created the building blocks for social media to facilitate worldwide information-sharing, making

such communication quick, easy, and for the most part, free.

We already know that, while there are many benefits to using social media tools, users can get themselves into trouble if they fail to establish privacy settings on both social media websites and applications. As social media has altered the way people communicate in both their personal and business lives, it has also fundamentally changed the discovery process inherent to legal proceedings in the U.S. as more litigants want a look at the opposing party's online trail.

Most individuals are unaware of the trail of metadata that they generate online when they use social media tools. This metadata trail is comprised of the information concerning a user's visit to a website, such as what smartphone is being used, the user's IP address, and the user's GPS location. Even where users intend to leave information on a social media website, such as a post or a comment, many are unaware how much metadata is actually being left behind.

Social media websites use the metadata left by users to create unique features that are meant to enhance user interaction on the social media

websites. This paperless trail is often created in the most unexpected of circumstances. LinkedIn, for example, lets a user see who viewed their profile, when their profile was viewed, and the geographic location of the viewer. An unsuspecting individual might intend to use LinkedIn to covertly gather information about potential employees or adversaries. This plan is foiled, however, when the LinkedIn user accesses metadata and sees that they are being investigated. Facebook allows users to upload photographs to its website, but also tracks metadata such as which smartphones or cameras were used and the GPS location of the photograph. Foursquare allows users to check in at different locations and continues to track this information over time, offering users “rewards the more times they check in at locations.

The metadata left behind at these websites creates a trail of personal information for the social media website or application to use, including a very detailed picture of each user, their likes and dislikes, travel habits, shopping habits, browsing history, and more.

But the information left behind can also become crucial evidence in litigation.

Discovery requests no longer encompass strictly paper files. Rather, litigants frequently demand emails and electronically-stored files. Text messages were admitted into evidence and discussed at trial in *U.S. v. Finley*, (477 F.3d 250 (5th Cir. 2007)). Tweets were admitted in *People v. Harris* (No. 2011NY080152 N.Y.S.2d (2012)).

In a Middle District of Florida case decided on February 21, *Davenport v. State Farm Mutual Auto Insurance Co.* (No. 3:11-cv-632-J-JBT), the plaintiff was ordered

to produce “all photographs added to any social networking site ... since the date of the subject accident that depict the Plaintiff, regardless of who posted the photograph.”

Many social media tools have built-in controls that limit the collection and dissemination of social media metadata. But individuals need to educate themselves about the use of such controls when engaging in social media activity. This is especially true in an environment where litigants become more creative in their use of social media evidence as offensive litigation weaponry.

By making an effort to understand the technology behind it, we all will be able to maximize the benefits and efficiencies that social media generates while minimizing the exposure of personal information that it disseminates.

Elisa J. D’Amico is a litigation associate in the Miami office of K&L Gates, focusing on commercial disputes, electronic discovery, creditor rights and bankruptcy-related matters. She can be reached at elisa.damico@klgates.com.

Marc Hirschfeld is president of Precision Legal Services. He assists attorneys with collection, processing and production of electronic discovery materials and provides consulting services to create defensible e-discovery strategies. He can be reached at marc@plsdata.com.