THE DAILY RECORD

Tuesday, February 3, 2015 / Volume 107 / Number 22 / $2.00 • Western New York's trusted source for legal and real estate news

Social Media Law

A Good Second Impression: Legal Ethics and Making Public Social Media Private

A number of recent ethics opinions discuss whether a litigant may change the privacy settings on a social media account to make previously-public social media information private.[i] The most recent is the Florida Bar Association's Proposed Advisory Opinion 14-1 (2015).

Although the opinions are cautious and caveats abound, they generally hold that a party, whether in litigation or before litigation has begun, may change privacy settings on a social media account to make public information private. However, a party may not spoliate relevant, or potentially relevant, evidence or violate any statutory, regulatory or other obligation regarding preservation of information.

Unfortunately, this considered guidance is being muddled by suggestions that making public content private may be "concealing" evidence or "obstructing" access thereto in violation of Rule of Professional Conduct 3.4(a). This position is not well-founded. It implies disclosure duties not found in Rule 3.4(a), ignores social media practicalities and defies common sense.

By SCOTT MALOUF
Daily Record Columnist

What does Rule 3.4 require?

The relevant portion of New York's version [ii] of Rule 3.4(a) states that a lawyer shall not:

(1) suppress any evidence that the lawyer or the client has a *legal obligation* to reveal or produce;

(3) conceal or knowingly fail to disclose that which the lawyer *is required by law to reveal;*

[Emphasis added]

Rule 3.4(a) does not impose an independent duty to volunteer all relevant information; it merely prohibits concealing potential evidence a lawyer has a legal obligation to disclose, see *Sherman v. State,* 905 P.2d 355 (Wash. 1995).

New York's comment's on Rule 3.4(a) further clarifies the limits of the rule:

The Rule applies to any conduct that falls within its general terms (for example, "obstruct another party's access to evidence") that is a *crime, an intentional tort or prohibited by rules or a ruling of a tribunal.* An example is "advis[ing] or caus[ing] a person to hide or leave the jurisdiction of a tribunal for the purpose of making the person unavailable as a witness therein."

Comment 1. [Emphasis added]

The rule is not violated because now-private social media information is harder for an opposing party to obtain or identify. Social media information still can be obtained through a document request or a subpoena. A violation occurs when a specific statute, case, rule, order, etc. requires all public social media information to remain publicly-accessible and a litigant makes the subject information or account(s) private.

The likelihood that sweeping public access is required seems remote based upon current case law. Requiring unlimited and unchangeable access to all public social media is similar to making a document request for "all" of a litigant's social media found behind a privacy wall. In each scenario, no limits have been placed upon the breadth of the material covered/sought. The mere existence, and possible utility, of the information is the rationale for the request.

Yet courts generally reject document requests seeking "all" of a litigant's private social media information. Courts require the party seeking private social media information to make a predicate showing of relevance. If that showing is made, then only relevant material need be disclosed. Substituting an unrestricted access standard would upend current case law requiring a showing of relevance.

Unique aspects of social media suggest no violation

An implicit criticism of making social media information private is that any public social media information a litigant makes private necessarily hurts the litigant's case and thus is likely relevant. This argument ignores many innocuous reasons for making a social media account private:

Continued on next page

Continued from previous page

• Unlike static records, social media accounts are living. Data may be created well after suit is filed. Thus, a litigant may wish to change privacy settings to limit exposure of future irrelevant or potentially embarrassing statements (especially those posted by others).

• A user may not have made a conscious, informed choice regarding privacy when signing up for a service. For example, a Facebook user can create an account at age 13.[iii] It is unlikely a 13 year-old will fully consider, or even understand, the implications his privacy settings may have in the future. Further, even seasoned, privacy-minded social media users can be surprised at how much data is public, despite their best efforts to keep it private. A changed privacy setting may merely reflect a better understanding of what data is being shared.

• An individual may wish to change settings to shield information from potential employers or colleges.

• To protect customer lists, an employer may require employees to shield their LinkedIn connections, see *Cellular Accessories For Less, Inc. v. Trinitas, LLC,* 2014 U.S. Dist. LEXIS 130518 (C.D. Cal. September 16, 2014)(LinkedIn settings relevant to whether customer list was a trade secret).

• A student being harassed by others may wish to change settings to prevent cyberbullying. Should counsel representing a harassed student in a school disciplinary matter fear ethical charges related to some ill-defined, potential discovery violation because the harassed student went private?

Additionally, how do we define the scope of the supposed obligation to keep social media accounts public? A litigant may have multiple social media accounts, such as Facebook, LinkedIn, Twitter, Google+, etc. Should all of these accounts remain publicly-available, unchanged, indefinitely? This might make the accounts practically useless, especially for business users who may have invested extensive resources in developing their digital assets.

Common sense suggests no violation

Attorneys routinely issue instructions regarding potential evidentiary issues. We tell a client not to discuss the matter with others. We might instruct a criminal defendant to close the drapes so others cannot observe his activities. It seems incongruous that changing social media privacy settings somehow differs from these common practices.

Takeaways

Despite the arguments above, your best bets in this area are caution and consideration. Understand your client's social media use and how it relates to the case. Review opinions issued by the bar association(s) relevant to your jurisdiction and stay abreast of new opinions and social media practices. Make your second impression count.

Scott Malouf is an attorney who helps other attorneys use social media, text and Web-based evidence. You can learn more about him at his website (www.scottmalouf.com) and follow him on Twitter at @ScottMalouf.

i New York County Lawyers Association Formal Ethics Opinion 745 (2013), North Carolina State Bar Association Formal Ethics Opinion 5 (2014), Pennsylvania Bar Association Opinion 2014-300, Philadelphia Bar Association Professional Guidance Committee Opinion 2014-5, New York State Bar Association Commercial and Federal Litigation Section Social Media Ethics Guidelines (2014), Guideline No. 4.A.

ii The relevant portion of ABA Model Rule 3.4(a) states that a lawyer shall not: unlawfully obstruct another party's access to evidence or unlawfully alter, destroy or conceal a document or other material having potential evidentiary value …

iii www.facebook.com/help/210644045634222