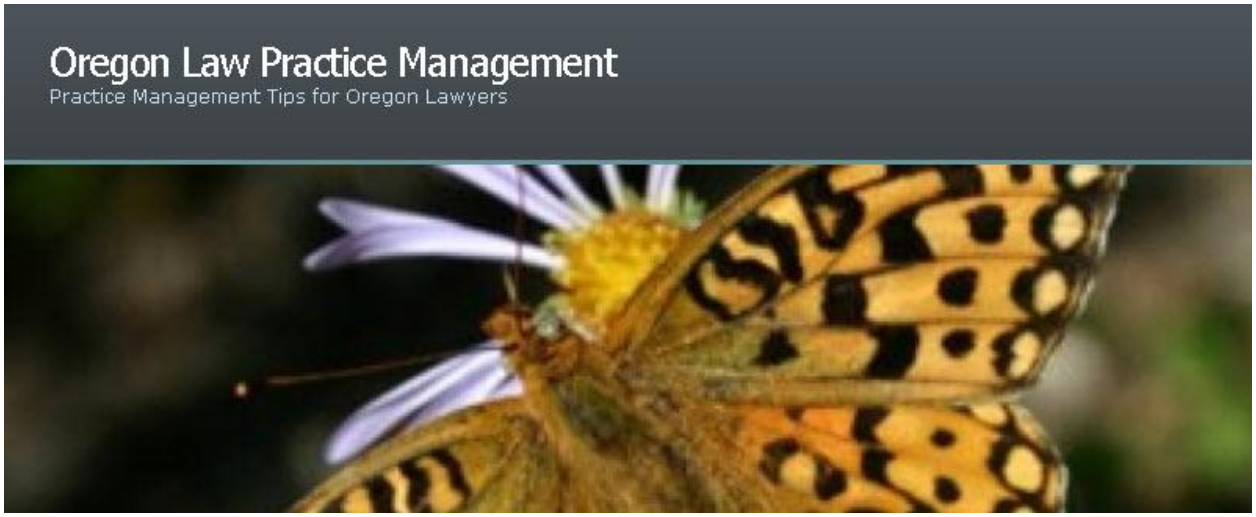

Best of: Ethical Traps in Cyberspace

Earlier this month, I had the opportunity to attend the ABA Annual Meeting in San Francisco. The CLE programming was excellent. In a later post, I will blog about Solo Day 2010. Today I want to share some tips from Ethical Traps in Cyberspace, sponsored by the Section of Labor and Employment Law. The Cyberspace panel featured Michael Z. Green, Paul R. Klenck, Carole Levitt, Mark Risk, and Julie Totten. Here are the highlights (some of which I live-tweeted during the conference):

Discovery

- Beware of "friending" witnesses on social networking sites in preparation for litigation. Such contact may be deceptive if the purpose or nature of the connection is not made clear. The same may hold true if the lawyer asks a third party to make the contact. See Philadelphia Bar Association Professional Guidance Committee Opinion 2009-02 (March 2009).
- If an individual communicates with his or her lawyer using a work computer, the communications may or may not be protected by attorney-client privilege: Scott v. Beth Israel Med. Ctr (no privilege in using work computer); Stengart v. Loving Care Agency, Inc. (e-mails sent via personal Yahoo! account on company laptop protected by attorney-client privilege.)
- Serving a subpoena duces tecum on social media Web sites to obtain personal information of users is not permitted under the Stored Communications Act, 18 USC § 2701(a)(1). Crispin v. Audigier. Lawyers seeking social media content should rely on traditional discovery methods directed to the specific parties involved.
- Employers are specifically prohibited from obtaining unauthorized access to their employees' password-protected Web sites under the SCA. See Konop v. Hawaiian Airlines, Inc. and Pietrylo v. Hillstone Restaurant Group.
- The Internet Archive can be used to retrieve old Web pages.

Counseling Clients

- Ask potential clients and witnesses about their use of social media; review social media content as needed.
- Caution clients about posting anything related to their case, particularly content that may reflect on their character or credibility. It may be best for the client to discontinue use of social media altogether.
- Warn your client that opposing counsel or someone connected to opposing counsel may attempt to independently access the client's profile or "friend" the client. Even if this does not occur, social network postings may be within the scope of a traditional discovery request.
- Be sensitive to spoliation of evidence issues, for example: if a client changes a pre-existing social network page, is this equivalent to altering a "document?" What about changing privacy settings or deactivating or removing an account altogether? Would the result be different if the profile was preserved before it was removed or changed?

Social Media Policies

- Provide guidance on both employer-sanctioned and personal use of social media, in particular how personal use may affect the employer or the employee's professional standing.
- Remind employees that anonymity on the Web doesn't exist.
- All employees should respect the intellectual property of others and avoid posting content that is defamatory or inappropriate. Using social media to "fire back," harass, or negatively engage others can come back to haunt the employee and employer.
- Additionally, lawyers and legal support staff should follow ethical parameters: protect client confidentiality, avoid giving legal advice, and use disclaimers as needed.
- Social media policies should be drafted to encompass emerging technology and reviewed regularly.
- PolicyTool is a good place to start if you need to craft a social media policy.

Internet Marketing for Lawyers

- Good judgment is essential when using social media.
- Marketing via the Internet should comply with ethical rules regarding advertising, solicitation, and the unauthorized practice of law:
    - Real-time electronic contact is specifically prohibited by ABA Model Rule 7.3(a).
    - Web sites and blogs should specifically state the jurisdictional limits of the attorney's practice to avoid UPL issues.
    - Content *should be* current, accurate, and subject to substantiation.
    - Content *should not create* false expectations.
- Jurisdictions vary. Know the rules of your specific state(s).

Facebook and MySpace

- Review your privacy settings, checking all sections and subsections. Perform this review on a regular basis, as social media providers change settings frequently.
- As with any Web site, use strong passwords or better yet, a pass phrase, and change it from time-to-time.

- Take control of what "friends" or "friends of friends" may post about you, especially when tagging you in photographs.
- Limit use of games or third party applications that access your personal profile.
- "Friending" judges before whom you appear is probably best avoided. In Florida, judges are specifically prohibited from "friending" lawyers who appear before them to avoid the appearance of impropriety: Florida Supreme Court Judicial Ethics Advisory Committee Opinion Based on: Florida Canon 2B.

LinkedIn

- Use of LinkedIn's "specialties" may be problematic. Research your jurisdiction. If necessary, use a disclaimer or leave this area of your profile blank.
- Also proceed cautiously with regard to client recommendations. Since all LinkedIn recommendations must be approved by the user, use this opportunity to correct any content that may run afoul of the rules. For example, it may be necessary to ask the client to add disclaiming language or delete content that constitutes an inappropriate comparison.

Ethical Traps in Cyberspace was an engaging program. Kudos to the top-notch panel members: Michael Z. Green, Paul R. Klenck, Carole Levitt, Mark Risk, and Julie Totten.

Originally published August 16, 2010 at
http://oregonlawpracticemanagement.wordpress.com/2010/08/16/best-of-ethical-traps-in-cyberspace/