STATE LEGISLATION OF SOCIAL MEDIA;

Could They – Would They – Should They?

Presented to the Kentucky Legislative Research Commission

House Chamber, Capitol Building

Frankfort, Kentucky

June 13, 2012

By Stuart Adams

Stuart Adams Law Office, P.S.C.

Louisville, Kentucky

LinkedIn	http://www.linkedin.com/in/stuartadams
Facebook	http://www.facebook.com/stuartadams.law
Twitter	http://twitter.com/StuartAdamsLaw
SociaLies blog	http://socialies.wordpress.com/

In many ways, social media has crept up on all of us, including individuals, businesses, and legislative bodies, like the proverbial barge coming down the river. One may be casually sailing back and forth, having seen the silhouette of the new thing appearing on the horizon up river from us, but tend to ignore it since it seemed so far away and insignificant. Some may choose to ignore it, hoping it will go away or change course before we might have to deal with it. Others, who have more experience with risk management, or who simply like to keep a sharp lookout for potential threats, might immediately start to assess the danger of what they see on the horizon, and take measures to be better prepared to deal with whatever may come their way.

We already know, thanks to the various companies monitoring the avalanche of social media networks, such as comscore.com, that "The average American spent 32 hours per month on the Internet in 2010. Persons ages 45-54 set the high bar averaging more than 39 hours online each month." http://bit.ly/fhksFQ An updated report from the end of 2011 showed that social networking sites then reached 82 percent of the world's online population, representing 1.2 billion users around the world and "social networking activity has more than tripled in the last few years." http://bit.ly/MtfZMH

The purpose and scope of this post is not to pontificate on whether a state legislature should attempt to insert itself into any of the issues mentioned below. It is intended to serve as a starting point for discussion and modest reference[1] to a few of the current issues with potential relation to social media.

Social Media Issues for Lawyers

Lawyers, let alone legislators who may be lawyers, have their own set of ethical, malpractice, and business ROI issues revolving around social media. The number of issues created or impacted by the ongoing development of social media is likewise expanding at a rate previously unknown in the field of legal ethics. Fortunately, we do have some baseline guidance.

Since many social media channels take the form of, or are similar to Web pages, essentially all of the Web-based ethical issues we've known about for over a decade will typically apply to them. In some cases, these old issues are "complicated" by the substantially more interactive nature of social media, and in particular, by the user-generated content not present in the older, static Web site design. Already present and continuing to grow is the issue of content generated by artificial intelligence engines.

Many of the Web-related ethics issues revolve around whether or not they were the result of unilateral actions of a client or other third party, for whom the attorney is not responsible, or involved an attorney's effort to circumvent the rules. "While the Internet did not create the ability of third parties, such as clients, to make statements that a lawyer could not ethically make, it certainly has increased the ease with which such statements can be made and, as a result, the difficulty that lawyers face in policing them, if policing they need do.[2]

A lawyer may not "induce" or "assist" (both somewhat subjective terms) in improper advertising, according to ABA Model Rule of Professional Conduct 8.4(a). Thus,

---

[1] To help those interested in reading "source material," which may be ever-changing and available from multiple sources, I've tried to include a link to the online version I read. To avoid those long URL's however, I have sometimes used the bitly™ (http://bit.ly/) URL shortener, and have not included the "last accessed" verbiage at the end of each cite.

[2] Hricik, David, Communication and the Internet: Facebook, Email and Beyond, Working Paper, Mercer University - Walter F. George School of Law, December 2009
http://ssrn.com/abstract=1557033

encouraging a client or “friend” to post a comment anywhere (ex. on client's blog to the effect that prospective class action plaintiffs should join a lawsuit the lawyer or lawyer’s firm has filed) would seem to be inappropriate at best.

What about comments or other material that would not otherwise comply with the ethics rules binding lawyers, which are posted on a lawyer’s blog or Web site by a third party, but not induced by the lawyer? At least one bar association has stated that a lawyer “should review the website to insure that there is nothing on it that would constitute any other violation of the advertising Rules….”[3] In other words, it appears you have to keep your own house clean after the visitors leave.

Additionally, you may sometimes have to suggest others clean up their house. South Carolina and Ohio[4] have said lawyers should “counsel” their clients to correct anything on the client’s pages that would be so incorrect or inappropriate as to constitute a problem if the lawyer posted it. The client’s First Amendment rights would seem to be at stake here, but these rulings appear limited thus far, at least, and have not been extended to non-client third party sites.

The ethical “trials” and tribulations of the legal profession, with regard to social media mistakes, continues to gain publicity from all quarters, including the American Bar Association itself.

> • A Chicago immigration lawyer posted an ad on Craigslist seeking a secretary and asking for measurements and photos. In a follow-up e-mail, the lawyer said one of the job requirements would be — sexual interaction with me and my partner. The disciplinary penalty is pending.
>
> • A Florida lawyer called a judge an evil, unfair witch on his blog. He was reprimanded in April 2009.
>
> • A Tampa lawyer listed four lawyers who weren‘t licensed in Florida as attorneys on the website for his law firm. He was suspended for 90 days.[5]

Although the primary purpose of this paper is not to deal in depth with these issues, the “SOCIAL MEDIA FOR LEGAL PROFESSIONALS” references section at the end contains several articles dealing in detail with them. The following, however, is a partial listing of the basic ethics issues related to lawyers being involved, or in some cases, refusing to utilize social media tools.

- links from the lawyer's social media platform to third party Web sites (Is this an "endorsement" or contain "otherwise unethical" content?)
- links from third party Web sites to a Web site operated by the lawyer

---

[3] Pa. B. Ass"n Comm. on Legal Eth. & Prof. Resp. 2007-13 (Dec. 2007).
[4] S.C. B. Op. 99-09 (1999) http://bit.ly/lhkucr; S.Ct. Ohio Bd of Comm’rs on Grievances and Discipline Op. No. 2004-7 (Aug. 6, 2004) http://bit.ly/jMiBQa
[5] Debra Cassens Weiss “Ethics Officials Seeing More Cases from Lawyers" Online Foibles” May 11, 2010 http://www.abajournal.com/news/article/ethics_officials_seeing_more_cases_from_lawyers_online_foibles/

- links from a social media channel (ex. Twitter, LinkedIn, Facebook profile, or blog, to the lawyer's Web site, or providing a way (ex. listing the phone number, e-mail address, or response widget) to contact the lawyer via law firm contact information. ("Solicitation" or violation of multi-state practice rules?)
- posts by clients in response to one by the lawyer
- posts by the lawyer in response to one by a client or other third party
- "endorsement" language posted by a client or other third party
- posting information which exposes confidential information about the lawyer, client, witness, leaving a trail of your investigation (ex. trial strategy), etc.
- posting information which could reasonably be interpreted as legal advice
- posting information that is false (ex. out of date) or misleading (ex. jurisdictionally inapplicable)
- posts of material by third parties on their own Web sites (or social media pages controlled by them) that would violate the lawyer's rules of ethics, if they had been posted by the lawyer
- inadvertent creation of an attorney-client relationship
- disqualification from representation due to receipt of information from an adverse party (So you thought the Facebook post raised a hypothetical issue?)
- use of (personally or through inducing another) deceptive practices to gather evidence (Are you really my Facebook friend?)
- professional competence, or lack thereof, in using social media properly as a tool, while avoiding pitfalls (I didn't realize I could find that out….)

Social Media ROI and Crisis Management 101 for Lawyers

Aside from ethical and malpractice concerns, lawyers who simply want to get some return on investment from time and resources devoted to social media can follow some basic rules. Ken Hardison has posted a nice article outlining some basic mistakes to avoid:

- Mistake # 1 Copying what every other lawyer is doing in their market
- Mistake # 2 Not Having a Unique Selling Proposition (USP)
- Mistake # 3 No Consistency in Marketing Message
- Mistake # 4 No Marketing Plan
- Mistake # 5 Not Tracking Your Marketing
- Mistake # 6 Lack of Follow-Through
- Mistake # 7 Not Getting Everyone in Your Firm on Board with the Marketing Plan and Goals[6]

[6] Ken Hardison "The 7 Fatal Mistakes Lawyers Make In Marketing Their Practices" 2009 PILMMA.org http://www.legalmarketingblog.com/uploads/file/The_Seven_Fatal_Mistakes_Lawyers_Make.pdf

Sharlyn Lauby has also provided a nice set of guidelines for those who have found themselves in a social media mess, without the benefit of a PR firm. Her suggestions include:

- Assemble a team of trusted employees who are willing to work round the clock (it won't be for long – just a few days at most) to help you evaluate the situation and possibly respond
- Assess the situation online by harnessing the tools that are publicly available, such as Google Search, Blogs, Technorati, Twitter Search and Who's Talkin.' Also watch RSS feeds to the online publications of both mainstream and industry media sources.
- Track these sources constantly to see what and how the situation is developing. Watch the "attacker's" website or blog as well. They may change their tune or consumers may react negatively and post comments about it on their site.

Then assess the situation:

- Trend the volume of response and the type of consumer reaction over time: Is it growing or waning? Is it supportive or negative? How is this changing over time?
- Identify what your target audience's reaction is. This will determine your response. Remember: your response could validate that there is an issue and may further perpetuate a negative situation.
- If consumers are silent on the situation, continue to monitor but don't respond publicly. Assess the need to respond on an ongoing basis – hourly, twice daily, daily, etc.
- If consumers are demanding a response, be sure that the initial upswell of outrage has passed and that the issue is, in fact, continuing. The online audience is fickle – if something more interesting breaks in the news, they may abandon your issue to move on to something more "important."
- When responding, be sure to really listen and determine what consumers want – do they just want an apology/acknowledgment or do they demand change? Be sure to address these things in your response.
- DO NOT RESPOND too quickly, too thoroughly, in too much of a 'corporate' tone or via a press release posted on your website (as the sole response mechanism). These tactics are typically not well-received in the social media landscape.[7]

Countermeasures can even be found on sources like Wikipedia, which posts the following suggestions on how organizations should handle social media problems, such as those caused by pretexting and other forms of social engineering attacks:

- Organizations must, on an employee/personnel level, establish frameworks of trust. (i.e., When/Where/Why/How should sensitive information be handled?)
- Organizations must identify which information is sensitive and question its integrity in all forms. (i.e., Social Engineering, Building Security, Computer Security, etc.)

[7] Sharlyn Lauby "5 Steps for Successful Social Media Damage Control" July 9, 2009 Mashable http://mashable.com/2009/07/09/social-media-damage-control/

- Organizations must establish security protocols for the people who handle sensitive information. (i.e., Paper-Trails for information disclosure and/or forensic crumbs)
- Employees must be trained in security protocols relevant to their position. (e.g., employees must identify people who steer towards sensitive information.) (also: In situations such as tailgating, if a person's identity cannot be verified, then employees must be trained to politely refuse.)
- An Organization's framework must be tested periodically, and these tests must be unannounced.
- Insert a critical eye into any of the above steps: there is no perfect solution for information integrity.[8]

The Policy on Policies

An ever popular issue for debate in both the private and public sector revolves around the extent to which, if any, an employer should impose a social media/social networking policy upon employees. Some have opted to encourage their employees to engage in daily, if not hourly social networking in order to enhance marketing efforts, interact with customers, to monitor reputation of the employer, as well as to conduct business intelligence expeditions to see what the competition is up to.

Most studies indicate a majority of employers still impose some sort of ban on external social networking, at least while employees are on the job. North Carolina appears to have been an "early-adapter" in this regard.

> "…Bev Perdue distributed North Carolina's first state government social media policy and online tutorial to state agencies and departments on Dec. 23. The announcement was made via the Governor's Office Twitter page and the documents can be downloaded on Perdue's Facebook page."
>
> "Social networking is not the next big thing. It's here now, and state government must stay current if we are to be fully transparent and accountable to the public," said Perdue. "I encourage all state agencies to take advantage of social media to increase communication and interaction with the citizens of North Carolina."[9]

The military seems to have attacked social media as an acceptable target and typically ranks at the top of government agencies using social media as a variety of tools.

> The U.S. Army, Navy and National Guard have all established official profiles at the online sharing platform Pinterest, whose user demographic is estimated to be eighty percent female."

---

[8] Wikipedia "Social Engineering Security" http://en.wikipedia.org/wiki/Social_engineering_(security)
[9] Casey Mayville "North Carolina Issues Policy for Government Social Media Usage" December 23, 2009 http://www.govtech.com/pcio/North-Carolina-Issues-Policy-for-Government.html

> "The U.S. military is wasting no time "pinning" its interests to one of the fastest growing social networking sites on the Internet.[10]

Other countries have likewise readily adopted social media, including policies, and according to at least one article published by Gartner, "The Best Government Social Media Guidelines So Far Come from New Zealand:"

> "I am always quite critical with governments as they come out with social media policies and guidelines that are full of good intention but usually fail to meet the intended goal of stimulating its use by erring too much on the side of risk management and institutional presence."
>
> I love the passive-active-engaged approach.
>
> Your organization doesn't have to jump in boots and all on the first day. You can start with a passive involvement and move through to becoming more active and finally fully engaged with the audiences you have identified.
>
> Passive: One of the first things your organization can do in social media is simply to listen. What's being said about you? […]
>
> Active: Once you've listened for a while and understand the tone and concerns of a social media community, you can begin becoming more active. You can post links to information to help people answer questions they have, or you can actively correct an inaccuracy on a blog, forum or a wiki […]
>
> Engaged: Finally, your organization can become fully engaged. You can set up a group on a social networking site and regularly introduce content for discussion, or you can establish a Twitter profile and begin contributing and actively posting and answering questions.
>
> This looks so reasonable and yet it is not what most guidelines say, as they try to urge organizations to establish a presence even without any clear understanding of their audience's expectations.[11]

A series of references is listed at the end of this article on social media training and policies for government employees.

---

[10] Luke Fretwell "U.S. Military Leads Government Adoption of Pinterest" February 9th, 2012 http://fedscoop.com/u-s-military-leads-government-adoption-of-pinterest/

[11] Andrea Di Maio "The Best Government Social Media Guidelines So Far Come from New Zealand" December 1, 2011 http://blogs.gartner.com/andrea_dimaio/2011/12/01/best-government-social-media-guidelines-so-far/

Employer Scrutiny of Employee Social Media Activities

One of the hottest topics in social media litigation and legislation is certainly the result of an ongoing battle between employers and employees in the private and government sectors, over employer scrutiny of the social media postings and profiles of both candidates and employees. The scrutiny extends to requiring employment candidates to turn over passwords to their social media accounts as a condition precedent to moving up the ladder from candidate to employee, and likewise has extended from activities while on the job to after-hours and post employment postings in a variety of settings.

In deference to a part of the title of this paper, and getting right to the point of the "could they – would they," I submit the following quote, excerpted from the JDSupra blog:

> *In response to press reports that employers are increasingly demanding that employees and job applicants disclose their login information for Facebook and other social media sites, state and federal legislatures have jumped into action, with Maryland recently becoming the first state to expressly prohibit the practice.*
>
> *A number of states are poised to follow Maryland. Currently, California, Illinois, Massachusetts, Michigan, Minnesota, New Jersey, and Washington have bills in the pipeline that seek to ban employers from requesting confidential login information as a condition of employment, and these bills appear to be attracting broad, bipartisan support.*
>
> *The new Maryland law, which will go into effect on October 1, 2012, prohibits employers from requesting employees' social media passwords. The law applies to "employers" – broadly defined as any person engaged in a business, industry, profession, trade or other enterprise in Maryland, as well as units of Maryland state and local government – and their respective representatives and designees, and even employers that are based outside Maryland but that have employees located in Maryland will need to comply with the statute.* (Lawmakers Rush to Ban Employers From Demanding Facebook Passwords Morrison & Foerster Social Media Newsletter Vol. 3, Issue 3 June 2012 excerpted in JDSupra Socially Aware: The Social Media Law Update -- Vol. 3, Issue 3 -- June 2012 http://bit.ly/LwOi99)

Earlier this year, the U.S. House of Representatives rejected a proposed amendment that would have added the following paragraph to the Federal Communications Commission Process Reform Act of 2012:

> "Nothing in this Act or any amendment made by this Act shall be construed to limit or restrict the ability of the Federal Communications Commission to adopt a rule or to amend an existing rule to protect online privacy, including requirements in such rule that prohibit licensees or regulated entities from mandating that job

> applicants or employees disclose confidential passwords to social networking websites."[12]

The defeated effort would have given the Federal Communications Commission the power to stop employers from asking job applicants for their password to Facebook and other social networking sites. While this would seem to be a green flag for more state legislative bodies to start drafting, the following warning should be heard, perhaps substituting the word "legislation" for "technology:"

> "The decision to embrace social media technology is a risk-based decision, not a technology-based decision. It must be made based on a strong business case, supported at the appropriate level for each department or agency, considering its mission space, threats, technical capabilities, and potential benefits."[13]

The "free speech" issue of employer and government involvement in social media could easily provide fuel for a seminar by itself.[14] This will presumably be a topic for legislatures and courts for some time to come. Perhaps the most recent social media conflagration has revolved around ownership of social media contacts, accounts, and content.

Password Please

As referenced above, many employers encourage employees to use social media networks to spread the good word about the employer's business. In doing so, those employees who understand the social aspect of social media, may very well develop a substantial database of "friends," "followers," and social media posts (a/k/a "content") they have developed either on or off the clock. While some cases revolve around what is done at the traditional workplace, more and more virtual employees and home-based bloggers are providing an increasing amount of a the marketing material for businesses.

When an employee leaves, he or she has been sometimes known to want to continue to use the database and content generated during tenure with a former employer. A number of pieces of litigation have been filed in the last few years over ownership of the social media accounts, passwords, contacts, and content. Several articles are referenced at the end of this document under the heading "Employer vs. Employee Ownership of Social Media Accounts, Contacts, Content, etc."

---

[12] Sarah Jacobsson Purewal "Facebook Password Amendment Rejected by Congress" PCWorld, March 29, 2012
http://www.pcworld.com/article/252837/facebook_password_amendment_rejected_by_congress.html

[13] "Guidelines for Secure Use of Social Media by Federal Departments and Agencies," v1.0 Issued By: ISIMC - Effective Date: 09.17.2009 cio.gov
http://www.cio.gov/Documents/Guidelines_for_Secure_Use_Social_Media_v01-0.pdf

[14] Brian Heaton Social Media Usage Becoming a Free Speech Question for Governments May 17, 2011 govtech.com
http://www.govtech.com/policy-management/Social-Media-Free-Speech-Question.html

You Can't Take it With You

Employers are not the only ones concerned with ownership of social media accounts. Have you ever thought what happens to your social media content, contacts, and other aspects of your online life when you die or become permanently disabled? Well, some heirs have tried to argue their entitlement to delve into the area and a recent article in the Courier Journal, indicates this may be a source of both legislation and litigation in many states for years to come.[15]

I Admonish You

One of the most costly social media problems for the judiciary, and for taxpayers, is the ongoing battle in the court system between judges and lawyers who attempt to get jurors to play by the same rules in as they did in a pre-social media era. Now that essentially everyone seems to be "wired" at all times, it seems there are accounts on almost a daily basis about some major civil or criminal trial that has been derailed because a juror, witness, lawyer, or even a judge has broken the rules. There are numerous cases of jurors doing their own research via smart phone from the jury room during deliberations. Some jurors polled after such an incident claimed they felt it their duty to conduct research into areas not fully presented by the lawyers or the court. This is despite repeated admonitions from the bench to the contrary.

The mindset of the public these days has resulted in all sorts of guidelines and policies but the problem remains and may be growing. Bailiffs have been instructed to confiscate anything electronic from jurors, and even from those in the cheap seats at trials, in order to prevent improper dissemination of information that could cause a mistrial. While some courts blog from the bench or allow bloggers in court, others have a strict policy against it. The question remains, however, whether there should be legislation, in addition to the powers of contempt held by the courts, in order to ensure that justice is done, without the unauthorized assistance of the social media networks.

I Admonish You Again

One final "admonition" comes from one of the first e-mails I received the day I wrote this article. LinkedIn® advised me, after they learned that approximately 6.5 million hashed LinkedIn passwords were posted on a hacker Web site:

> We are working hard to protect you, but there are also steps that you can take to protect yourself, such as:
>
> •Make sure you update your password on LinkedIn (and any site that you visit on the Web) at least once every few months.

[15] Michael Avok "Is Facebook part of your estate? Some states are adopting laws on digital assets" 3/17/2012 Courier Journal http://www.courier-journal.com/apps/pbcs.dll/article?AID=2012303170067

•Do not use the same password for multiple sites or accounts.

•Create a strong password for your account, one that includes letters, numbers, and other characters.

•Watch out for phishing emails and spam emails requesting personal or sensitive information.[16]

No matter how secure you feel and no matter how sophisticated your knowledge of social media, technology, and security, there are folks out there who are probably better than you and inclined to take advantage of what you've got. That includes doing so by pretexting, phishing, and an ever increasing, and increasingly devious variety of techniques to get you to volunteer your Visa password and PIN number, or some other bit of information they can use to their advantage. Heed the warnings and enjoy the ride.

[16] "Taking Steps to Protect Our Members," LinkedIn® posted 6/7/2012
http://blog.linkedin.com/2012/06/07/taking-steps-to-protect-our-members/

ADDITIONAL REFERENCES

Social Media for Legal Professionals

Stuart Adams "Social Media 101 for Lawyers: What You Need to Know About it to Build Your Business and Stay Out of Trouble" May 19, 2010 presentation paper for the Louisville Bar Association

Stuart Adams and Constance Ard Your Space is My Space presentation paper for the 2009 Kentucky Bar Association Annual CLE Update

Stuart Adams Who is the Most Popular Lawyer Now? Social Media Ethics Issues for Lawyers presentation paper for the 2011 Kentucky Bar Association Annual CLE Update

Stuart Adams "Social Media and the Future of the Legal Profession" SocialLies blog June 17, 2011

Stuart Adams Judicious Blogging SocialLies blog October 23, 2009

Social Media Training and Policies for Government Employees

Dannielle Blumenthal "10 Social Media Safety Tips for Government Employees" GovLoop.com 6/24/ 2011 http://www.govloop.com/profiles/blogs/10-social-media-safety-tips

Margaret DiBianca Social-Media Policies: Ethical Issues for Court Employees 9/27/2011 LexisNexis http://www.lexisnexis.com/community/labor-employment-law/blogs/labor-employment-commentary/archive/2011/09/27/social-media-policies-ethical-issues-for-court-employees.aspx

Grant Gross "Gartner Predicts Huge Rise in Monitoring of Employees' Social Media Use" PCWorld.com 5/29/2012 http://www.pcworld.com/businesscenter/article/256420/gartner_predicts_huge_rise_in_monitoring_of_employees_social_media_use.html

Harrison "Social Media Policies a Thorny Issue for Companies and Employees" TMCnet 9/26/2011 http://www.tmcnet.com/topics/articles/222407-social-media-policies-thorny-issue-companies-employees.htm

Justin Herman "Using Social Media in Government" howto.gov 6/4/2012 http://www.howto.gov/social-media/using-social-media

Alain Lemay “Who not to follow on Twitter! - A guide for public sector employees” 6/5/2011 GovLoop.com http://www.govloop.com/profiles/blogs/who-not-to-follow-on-twitter

Casey Mayville “North Carolina Issues Policy for Government Social Media Usage” 12/23/2009 http://www.govtech.com/pcio/North-Carolina-Issues-Policy-for-Government.html

Steve Townes “Utah Creates Social Media Guidelines for Employees Who Blog, Tweet, Etc.” govtech.com 10/6/2009 http://www.govtech.com/policy-management/Utah-Creates-Social-Media-Guidelines-for.html

Employer vs. Employee Ownership of Social Media Accounts, Contacts, Content

Stephanie Rabiner “More Employers Asking for Facebook Passwords” 3/21/2012 FindLaw http://blogs.findlaw.com/free_enterprise/2012/03/more-employers-asking-for-facebook-passwords.html

Steven Harmon “California poised to bar employers from peeking into private information on social media sites” 5/3/2012 SiliconValley.com http://www.siliconvalley.com/ci_20534489/california-bar-employers-peeking-into-private-data-social-media-password

Saul Ewing “Governor O'Malley Signs Maryland Law Prohibiting Employers from Seeking Access to Personal Social Media Information; Other States Considering Similar Bans” 5/2/2012 JD Supra http://www.jdsupra.com/post/documentViewer.aspx?fid=44c481c2-896b-4630-83a6-e999b3cc8a13

Amy Eve Maremont vs. Fredman Design Group - MEMORANDUM OPINION AND ORDER - re: Accessing An Employee's Social Media Account Without Bad Intent US Dist Ct for Northern Dist of Ill. 12/7/2011http://pub.bna.com/lw/10c07811.pdf

John Mello “Facebook Password Requests from Employers Raise Ire of Lawmakers” 3/25/2012 PCWorld.com http://www.pcworld.com/article/252521/facebook_password_requests_from_employers_raise_ire_of_lawmakers.html

Sarah Purewal Facebook Password Amendment Rejected by Congress 3/29/2012 PCWorld http://www.pcworld.com/article/252837/facebook_password_amendment_rejected_by_congress.html

Unfair Competition & Trade Secrets

Hays Connie & William Leahy "Can 'Friends' Be Trade Secrets?" 5/2/2012 Competition & Trade Secrets Counsel blog http://www.unfaircompetitiontradesecretscounsel.com/trade-secrets-1/can-friends-be-trade-secrets/

Shawn Tuma "Are LinkedIn Contacts Trade Secrets?" 10/18/2011 Shawn E. Tuma blog http://shawnetuma.com/2011/10/18/are-linkedin-contacts-trade-secrets/

Estates –Ownership of Decedent's Social Media Accounts

Michael Avok "Is Facebook part of your estate? Some states are adopting laws on digital assets" 3/17/2012 Courier Journal http://www.courier-journal.com/apps/pbcs.dll/article?AID=2012303170067

Cyber-bullying

Andrew Chow "Facebook Threat Gets NJ Girl, 14, Arrested" 1/7/2012FindLaw Blotter http://blogs.findlaw.com/blotter/2012/01/facebook-threat-gets-nj-girl-14-arrested.html

Additional Articles and Resources

Stuart Adams, "Social Media Glossary" 6/8/2012 SociaLies blog http://bit.ly/L3iCbV http://www.juristechnology.com/Glossary - Social Media ver 6-7-2012.pdf

Stuart Adams, "Best Practices – Tips on Social Networking; Cutting Through the Smoke and Mirrors" SociaLies blog http://socialies.wordpress.com/tips-on-social-networking-best-practices/

Stuart Adams, "Employer Ownership of Employee Social Media Accounts; The War Continues" January 5, 2012 http://socialies.wordpress.com/2012/01/05/employer-ownership-of-employee-social-media-accounts-the-war-continues/

Stuart Adams, "Social Networking Threatens Another Jury Verdict" SociaLies blog January 30, 2010 http://socialies.wordpress.com/2010/01/30/social-networking-threatens-another-jury-verdict/

Bob Ambrogi, "Rules of Conduct for Social Networking," Legal Blog Watch, May 14, 2009 http://legalblogwatch.typepad.com/legal_blog_watch/2009/05/my-entry.html

Dannielle Blumenthal “10 Social Media Safety Tips for Government Employees” 6/24/ 2011 GovLoop.com http://www.govloop.com/profiles/blogs/10-social-media-safety-tips

Margaret DiBianca “Social-Media Policies: Ethical Issues for Court Employees” LexisNexis 9/27/2011 http://www.lexisnexis.com/community/labor-employment-law/blogs/labor-employment-commentary/archive/2011/09/27/social-media-policies-ethical-issues-for-court-employees.aspx

Grant Gross “Gartner Predicts Huge Rise in Monitoring of Employees' Social Media Use” PCWorld.com 5/29/2012 http://www.pcworld.com/businesscenter/article/256420/gartner_predicts_huge_rise_in_monitoring_of_employees_social_media_use.html

Erin Harrison “Social Media Policies a Thorny Issue for Companies and Employees” TMCnet 9/26/2011 http://www.tmcnet.com/topics/articles/222407-social-media-policies-thorny-issue-companies-employees.htm

Justin Herman “Using Social Media in Government” howto.gov 6/4/2012 http://www.howto.gov/social-media/using-social-media

C.C. Holland, “Mind the Ethics of Online Networking” Law.com, November 6, 2007 http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=900005558317

Alain Lemay “Who not to follow on Twitter! - A guide for public sector employees.” GovLoop.com 6/5/2011 http://www.govloop.com/profiles/blogs/who-not-to-follow-on-twitter

Casey Mayville “North Carolina Issues Policy for Government Social Media Usage” govtech.com 12/23/2009 http://www.govtech.com/pcio/North-Carolina-Issues-Policy-for-Government.html

“Report of the South Carolina Bar Young Lawyers Division Social Media Task Force” November 2009 http://www.scbar.org/public/files/docs/Report.pdf

Amy Spach, "The Ethical Pitfalls of Online Social Networking," Law Marketing Portal, March 3, 2008 http://www.lawmarketing.com/pages/articles.asp?Action=Article&ArticleCategoryID=13&ArticleID=731

Ken Strutin, “Social Media and the Vanishing Points of Ethical and Constitutional Boundaries,” 31 Pace L. Rev. 228 (2011) http://digitalcommons.pace.edu/plr/vol31/iss1/6

Steve Townes “Utah Creates Social Media Guidelines for Employees Who Blog, Tweet, Etc.” 10/6/2009 govtech.com http://www.govtech.com/policy-management/Utah-Creates-Social-Media-Guidelines-for.html

Federal Legislation Impacting Various Aspects of Social Media

There are numerous federal laws impacting social networking. Here are a few of the more significant ones.

CAN-SPAM Act of 2003: The full name of the Act is “Controlling the Assault of Non-Solicited Pornography And Marketing Act of 2003.” The Act established the first national standards for sending commercial e-mail and required the Federal Trade Commission (FTC) to enforce its provisions. The Act defines a "commercial electronic mail message" as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service (including content on an Internet website operated for a commercial purpose)." It preempts state anti-spam laws that do not deal with fraud and it exempts "transactional or relationship messages."

Communications Decency Act (“CDA”): The Act, 47 U.S.C. §230(c)(1), was Title V of the Telecommunications Act of 1996. It was an early attempt by Congress to regulate pornographic material and has been interpreted to say that operators of Internet services are not to be construed as publishers, and therefore not legally liable for the words of third parties who use their services.

Computer Fraud and Abuse Act (“CFAA”): The Act, 18 U.S.C. §1030, prohibits intentionally accessing a computer without permission when damage or impairment of data results.

Gramm–Leach–Bliley Act: The Act, (Pub.L. 106-102, 113 Stat. 1338) also known as the Financial Services Modernization Act of 1999 encourages the organizations covered by the GLB to implement safeguards against pretexting and provides limited privacy protections against the sale of customers’ private financial information.

Health Information Technology for Economic and Clinical Health Act (“HITECH”): The Act (Public Law 104-191) was enacted as part of the American Recovery and Reinvestment Act of 2009. Subtitle D of the HITECH Act addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

Stored Communications Act (“STA”): The Act, 18 U.S.C. §2701, provides for both criminal and civil penalties for a person who "intentionally accesses without authorization a facility through which an electronic communication service is provided or… intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorize access to a wire or electronic

communication while it is in electronic storage in such system." The STA was enacted as Title II of the Electronic Communications Privacy Act.

USA PATRIOT Act ("Patriot Act"): The Act, Public Law 107–56, was a response to the terrorist attacks of September 11th, dramatically reduced restrictions in law enforcement agencies' gathering of intelligence within the United States; expanded the definition of terrorism to include domestic terrorism, expanded the Secretary of the Treasury's authority to regulate financial transactions, and particularly those involving foreign individuals and entities.