REGENT UNIVERSITY
LAW REVIEW

Volume 22 **2009–2010** **Number 1**

THE LEGAL IMPLICATIONS OF SOCIAL NETWORKING

Sharon Nelson
John Simek
Jason Foltin[*]

INTRODUCTION

The world has embraced social networking with a fervor rarely seen. Even lawyers, though always slower than the general public to adopt new technology, are increasingly utilizing social networking sites, both for marketing purposes and as a source of evidence.

Unknowingly, they have all dropped into what the military might call a "hot zone." Perils await on all sides, and lawyers are poorly armed. Only recently have we begun to wake up to the dangers of social networking and its ethical implications for lawyers.

Let's take a look at social networking from 10,000 feet and consider some recent statistics.

In April 2009, Facebook announced that it had over 200 million active users worldwide.[1] In the same month, Twitter, the new kid on the social networking block, reached over 14 million users in the United States.[2] LinkedIn claims over 48 million members worldwide[3] and Plaxo over 40 million.[4] MySpace, once the 800-pound gorilla of this new world,

---

[*] Authors Sharon Nelson, Esq. and John Simek are the President and Vice President of Sensei Enterprises, a computer forensics and information technology company in Fairfax, Virginia. John Simek, EnCE, CCE, is a Certified Handheld Examiner, Certified Novell Engineer, Microsoft Certified Professional + Internet, Microsoft Certified Systems Engineers, NT Certified Independent Professional, and Certified Internetwork Professional. Author Jason Foltin is a paralegal with Sensei Enterprises.

[1] Facebook Timeline, http://www.facebook.com/press/info.php?timeline (last visited Nov. 19, 2009).

[2] Posting of Nick O'Neill to Social Times, http://www.socialtimes.com/2009/04/twitter-14-million/ (Apr. 7, 2009, 09:00 EST) (citing March Data is Live on Site Analytics!, http://blog.compete.com/2009/04/07/march-data-live/ (Apr. 7, 2009)).

[3] LinkedIn, About Us, http://press.linkedin.com/about (last visited Nov. 19, 2009).

[4] Plaxo Company Overview, http://www.plaxo.com/about (last visited Nov. 19, 2009).

has fallen from favor with Internet users.[5] Still, according to TechCrunch, it has an impressive 125 million users globally.[6] These networks are rapidly becoming a part of everyday life to an increasing number of people, but if any of the sites listed above are unfamiliar to you, just take a look at their Wikipedia entries.[7]

Texting and blogging are often included as part of the social networking phenomenon. We will discuss them here from time to time, as there is such interconnection among all these technologies.

This alluring new world has demonstrated many pitfalls. Initially, very few people used the privacy settings that were available to them.[8] They simply left them at the default settings, meaning that everything they posted was wide open to anyone.[9] And let's face it, if your "friend" on Facebook chooses to cut and paste elsewhere some very unseemly language you posted, your privacy settings are all for naught. Additionally, the terms of use, which most people do not read, give the sites enormous power over how your postings may be used. It is enough to give a cautious person a serious case of the willies.

Compounding the dangers, social networks have begun to attract, in a major way, folks who want to use them to spam, to control bot networks, to attract Internet users to sites which will download malware, and even to use photos of your family and friends to peddle their products. Imagine the surprise of the husband who found a photo of his wife in a Facebook "hot singles" ad, with her image used without her knowledge or consent.[10] The advertiser had merely lifted her attractive photo from a Facebook page.[11]

Hackers have shown increasing interest in these sites as well (never a good omen for sites that once seemed fairly innocent). By using the

---

[5] *See* Posting of Michael Arrington to TechCrunch, MySpace Is in Real Trouble If These Page View Declines Don't Reverse, http://www.techcrunch.com/2009/05/18/myspace-is-in-real-trouble-if-these-page-view-declines-dont-reverse/ (May 18, 2009).

[6] Posting of Michael Arrington to TechCrunch, Facebook Now Nearly Twice the Size of MySpace Worldwide, http://www.techcrunch.com/2009/01/22/facebook-now-nearly-twice-the-size-of-myspace-worldwide/ (Jan. 22, 2009).

[7] Wikipedia, Facebook, http://en.wikipedia.org/wiki/Facebook (last visited Nov. 19, 2009); Wikipedia, LinkedIn, http://en.wikipedia.org/wiki/LinkedIn (last visited Nov. 19, 2009); Wikipedia, MySpace, http://en.wikipedia.org/wiki/MySpace (last visited Nov. 19, 2009); Wikipedia, Plaxo, http://en.wikipedia.org/wiki/Plaxo (last visited Nov. 19, 2009).

[8] *See, e.g.*, Sophos, *Facebook Members Bare All on Networks, Sophos Warns of New Privacy Concerns*, Oct. 2, 2007, http://www.sophos.com/pressoffice/news/articles/2007/10/facebook-network.html.

[9] *See id.*

[10] Culture Smith Consulting, Husband Speaks Out on Seeing Wife in Facebook Dating Ad, http://www.culturesmithconsulting.com/husband-speaks-out-on-seeing-wife-in-facebook-dating-ad/ (July 29, 2009) (citing Video Post: *Husband Sees Wife on Singles Facebook Ad* (ABC 13 July 29, 2009), http://cfc.wset.com/videoondemand.cfm?id=45551).

[11] *Id.*

sites' features that allow the downloading of content from third-party sites, the networks have left huge security holes for hackers to exploit.[12]

Because social networking is so new, the barrage of tales involving missteps has taken on the force of an avalanche in the last couple of years. Let's take a look at social networking through the prism of the law.

I. COURTS WRESTLE WITH SOCIAL NETWORKING

The news flashes have come fast and furious in the last two years, so much so that it is truly impossible to keep up with them all, though they assault us nearly every night on the evening news, or their online counterparts.

In the most egregious case on record, a woman sitting on a British jury in a sexual assault and child abduction case polled her friends on Facebook to see which way she should vote.[13] One wants to ask in exasperation, "What in the world was she thinking?" But this is the world in which we live, and we take our jurors as we find them.

For example, Pennsylvania State Senator Vincent Fumo complained in his post-verdict appeal of conviction that a juror used Twitter, Facebook, and blogs to post information about the trial during deliberations.[14] The court rejected the complaint in its ruling on Fumo's post-trial motion.[15]

> The Twitter message at issue simply stated, "This is it . . . no looking back now!"
>
> The Court finds that such a comment could not serve as a source of outside influence because, even if another user had responded to Wuest's Twitter postings (of which there was no evidence), his sole message suggested that the jury's decision had been made and that it was too late to influence him. Moreover, Wuest's comment caused no discernible prejudice. It was so vague as to be unclear. Wuest raised no specific facts dealing with the trial, and nothing in his comment directly referred to the trial or indicated any disposition toward anyone involved in this suit. Finally, there is no evidence that he discussed any of these matters with any of his fellow jurors. Hence, the Court declines to grant the motion on this ground.[16]

---

[12] Brian Krebs, *Hackers' Latest Target: Social Networking Sites*, WASH. POST, Aug. 9, 2008, at D1, *available at* http://www.washingtonpost.com/wp-dyn/content/article/2008/08/08/AR2008080803671.html.

[13] Daily Mail Reporter, *Juror Dismissed After Asking Facebook Friends How She Should Vote on Trial*, MAIL ONLINE, Nov. 25, 2008, http://www.dailymail.co.uk/sciencetech/article-1089228/Juror-dismissed-asking-Facebook-friends-vote-trial.html.

[14] United States v. Fumo, No. 06-319, slip op. 115, 116–17, 125, (E.D. Pa. Jun. 17, 2009), *available at* http://www.paed.uscourts.gov/documents/opinions/09d0710p.pdf.

[15] *Id.* at 128.

[16] *Id.* at 117 (alteration in original) (citation omitted).

With respect to the juror's Facebook postings, the court found that they were in the nature of general status updates which revealed nothing of substance and he did not appear to receive any outside information because of them; thus, there was no prejudice.[17] And though Wuest had posted on his moribund blog that he was on jury duty, he offered no further information, nor did he receive any comments to the blog post.[18]

In conclusion, the court found that "despite violating the [c]ourt's admonition against discussing the details of the trial, Wuest was a trustworthy juror who was very conscientious of his duties. There was no evidence presented by either party showing that his extra-jury misconduct had a prejudicial impact on the [d]efendants."[19]

It is noteworthy in this case that the court clearly finds that this juror violated the court's orders.[20] He "skates," however, and only because the court found that his misconduct had no prejudicial impact.[21] It is all too easy to imagine a case where there might be considerable prejudicial impact from this sort of misconduct.

Consider the following hypothetical facts: There are a number of social networkers who are simply addicted to posting the events of their lives. If they are prone to tell the world that they had a decaf skim latte in the morning and which TV shows they are watching at night (along with which brand of popcorn), the allure of posting about a juicy trial is surely going to be too much to resist.

Another misbehaving juror in Arkansas posted eight tweets during a trial which resulted in a $12.6 million dollar verdict.[22] Stoam Holdings and its owner Russell Wright were accused of running a Ponzi scheme.[23] During the trial, the juror's tweets included one that said, "oh and nobody buy Stoam. Its [sic] bad mojo and they'll probably cease to [e]xist, now that their wallet is 12m lighter."[24]

This could have been very bad "mojo," indeed, for the juror and the trial, but the Court found "that the tweets were [merely] in bad taste,

---

[17] *Id.* at 121–22.

[18] *Id.* at 125, 127.

[19] *Id.* at 127–28.

[20] *Id.* at 122.

[21] *Id.*

[22] Jon Gambrell, *Appeal Claims Juror Bias in 'Tweets' Sent During $12 Million Case*, LAW.COM, Mar. 16, 2009, http://www.law.com/jsp/article.jsp?id=1202429071686.

[23] *Id.*

[24] *Id.*

but not improper."[25] It is questionable whether other courts might have treated that offense so lightly.

Consider a recent case in which Miami-Dade Circuit Judge Scott Silverman dismissed a civil fraud lawsuit after declaring a mistrial when Chief Executive Officer Yizhak Toledano took advantage of a bench conference to text Chief Financial Officer Gavin Sussman, who was on the witness stand.[26] After being alerted by a spectator, Judge Silverman questioned Toledano and Sussman, who admitted to the texting.[27] The judge then had the offending text messages read aloud and made part of the record.[28]

In his order dismissing the case, Judge Silverman wrote that the texting

> "was underhanded and calculated to undermine the integrity of this court and the legal process . . . . Regretfully, plaintiff through its unacceptable conduct has reached into the [C]ourt's quiver of sanctions, drawn the bowstring taut and aimed the arrow at the heart of its own case. This [C]ourt has justifiably released the string."[29]

The judge also awarded attorney fees and costs to the defense.[30]

So what do we do with these devices? Some courts, like the United States District Court for the Eastern District of Virginia, ban the entry of cell phones entirely.[31] This practice is, to put it very mildly, not likely to be popular with attorneys or jurors. It is curious, in this electronic age, that this court still insists that attorneys bring paper calendars to court with them to schedule hearings and trial dates rather than use their smartphones. It seems quite deliciously antiquated for an otherwise very modern court.

The United States District Court for the Southern District of New York is experimenting with an interim rule whereby attorneys may bring in pre-authorized electronic devices, though jurors, witnesses, and observers are still required to leave such devices behind.[32]

---

[25] Tresa Baldas, *For Jurors in Michigan, No Tweeting (or Texting, or Googling) Allowed*, LAW.COM, July 1, 2009, http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202431952628&slreturn=1&hbxlogin=1.

[26] Deborah C. Espana, *Judge Tosses Fraud Suit After Witness Is Texted by Boss During Trial*, LAW.COM, Aug. 17, 2009, http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202433074669.

[27] *Id.*

[28] *Id.*

[29] *Id.*

[30] *Id.*

[31] Sharon Nelson & John Simek, *Three Strikes and You're Out: Judges Talk About Technology in the Courtroom*, LAW PRAC., July–Aug. 2005, at 24, 25.

[32] Katherine A. Helm, Op-Ed, *Courtrooms All Atwitter*, NAT'L L.J. (New York City), Aug. 10, 2009, at 34.

Some states are bringing down the hammer. Michigan acted decisively in making a Supreme Court rule banning the use of any electronic communications devices, such as iPhones and BlackBerrys, while in the jury box or during deliberations.[33]

It is difficult, during a trial of any length, to keep cell phones out of the hands of jurors. As a society, we have become accustomed to using them to stay in touch with family members and to receive important communications from employers. Arguably, if jury members are allowed to have smartphones in the jury box, they can be easily distracted. This would likely be just as true in the jury deliberation room. Perhaps we can ban the use of cell phones in those two places, but can we really forbid access to cell phones during breaks or in the evenings?

A veritable smorgasbord of policies exists. New Jersey permits jurors to bring cell phones inside, provided that they remain off during trial.[34] One Alaska court requires jurors to check their cell phones with the bailiff at the start of deliberations, while Malheur County, Oregon, and the United States District Court for the Western District of Louisiana ban jurors' cell phones outright.[35]

Some courts, like the one in Ramsey County, Minnesota, have issued a new policy prohibiting jurors from bringing any wireless communication device to court. In Ramsey County, a court declared two mistrials after jurors used cell phones during deliberations, in violation of a court order.[36]

The court in Multnomah County, Oregon, has a jury instruction specifically addressing electronic devices and activities: "Do not discuss this case during the trial with anyone, including any of the attorneys, parties, witnesses, your friends, or members of your family. 'No discussion' also means no emailing, text messaging, tweeting, blogging or any other form of communication."[37]

The instruction also warns jurors about Internet searches:

> In our daily lives we may be used to looking for information on-line and to "Google" something as a matter of routine. Also, in a trial it can be very tempting for jurors to do their own research to make sure they are making the correct decision. You must resist that temptation for our system of justice to work as it should.[38]

---

[33] Anita Ramasastry, *Why Courts Need to Ban Jurors' Electronic Communications Devices*, FINDLAW.COM, Aug. 11, 2009, http://writ.news.findlaw.com/ramasastry/20090811.html.

[34] *Id.*

[35] *Id.*

[36] *Id.*

[37] *Cell Phone Policies/Instructions for Jurors*, JUR-E BULL. (Nat'l Ctr. for State Courts, Ctr. for Jury Studies, Williamsburg, Va.), May 1, 2009, http://www.ncsconline.org/WC/Publications/KIS_JurInnJurE05-01-09.pdf.

[38] *Id.*

Another instruction was issued on April 21, 2009, by an Arkansas judge, who said,

> [D]uring your deliberations, please remember you must not provide any information to anyone by any means about this case. Thus, for example, do not use any electronic device or media, such as the telephone, a cell or smart phone, Blackberry, PDA, computer, the Internet, any Internet service, any text or instant messaging service, any Internet chat room, blog, or website such as Facebook, My[]Space, YouTube or Twitter, to communicate to anyone any information about this case until I accept your verdict.[39]

Similar instructions have reportedly been given to jurors by judges frustrated by the misuses of these new technologies.[40]

As always, technology has leap-frogged over our current rules and procedures and we are struggling to catch up. Different courts have played with different rules. Some simply have bailiffs monitor the courtroom, putting the kibosh on any attempt to utilize a smartphone in the courtroom.

The National Center for State Courts has been collecting cell phone policies and related instructions for jurors—notable for the fact that these are all over the map![41] We have clearly identified the problem, but we certainly have not standardized a solution.

Reporters are also caught up in the frenzy. A United States District Judge allowed a reporter to tweet about court proceedings during a trial of six gang defendants in Kansas.[42] He felt it opened the legal process to the public.[43]

In July 2009, a court order in Florida went in the opposite direction. The reporters were given a temporary press room while covering a trial.[44] They were permitted to bring in their "cellular phones, BlackBerries, iPhones, Palm Pilots, and other similar electronic devices as long as they agree[d] in writing to not email, text message, twitter,

---

[39] Ride the Lightning: Web 2.0 Jury Instructions in Arkansas, http://ridethelightning.senseient.com/2009/05/web-20-jury-instructions-in-arkansas.html (May 8, 2009, 07:00 EST) (original alterations omitted).

[40] *See, e.g.,* People v. Jamison, No. 8042/06, 2009 WL 2568740, at *6 (N.Y. Sup. Ct. Aug. 18, 2009).

[41] *See Cell Phone Policies*, *supra* note 37.

[42] LarrysWorld.com, Twitter in the court: Federal Judge Gets It, http://www.pcanswer.com/2009/03/09/twitter-in-the-court-federal-judge-gets-it/ (Mar. 9, 2009).

[43] *Id.* (citing Roxana Hegeman, *Twitter Boosts Public Access to Federal Courtrooms*, FOXNEWS.COM, Mar. 6, 2009, http://www.foxnews.com/wires/2009Mar06/0,4670,CourtroomTweets,00.html).

[44] Order Regarding Media Conduct and Electronic Equipment Access, United States v. UBS AG, No. 1:09-cv-20423-ASG (S.D. Fla. July 9, 2009), *available at* http://www.flsd.uscourts.gov/viewer/viewer.asp?file=/cases/pressDocs/109cv20423_106.pdf.

type or otherwise use those devices inside any courtrooms within this District."[45]

Obviously, it is a jungle out there. As the old saying goes, "if you know the rules of one court, you know the rules of one court."

II. LAWYERS AND JUDGES WHO HAVE FALLEN INTO THE TAR PIT

You might read the preceding section and think, "Gosh, who would do something like that?" It appears, however, that lawyers and judges are no different. Consider some of the following examples.

A Texas judge recounts a case in which a lawyer requested a continuance due to the death of her father.[46] The lawyer's recent Facebook statuses told a different story, however, speaking of a week filled with drinking and partying.[47] Strangely, her story in court did not match her Facebook posts.[48] Another lawyer posted a complaint about the same judge's court on Facebook, prompting the judge to send the lawyer a good-natured Facebook barb of her own.[49] The judge also recalls cases in which lawyers were "on the verge of crossing, if not entirely crossing, ethical lines" with their online complaints about clients or opposing counsel, and once had to warn a family member that her online boasts about how much money she expected to win in a tort suit might hurt her case.[50]

Here is a cautionary tale of a lawyer who seems to have forgotten the rules of engagement. A child was injured at an Old Navy store (a subsidiary of Gap, Inc.) on a clothing rack and a lawsuit ensued in federal court based on diversity jurisdiction.[51] The plaintiffs deposed the Gap's General Liability Claims Manager via video deposition on the chain of custody of the clothing rack.[52] The witness was in Sacramento, California, the defense attorneys were in Fort Lee, New Jersey, and the *pro hac vice* attorney was in Southfield, Michigan.[53] The deponent and the *pro hac vice* attorney "were only visible from the 'chest up'" and their hands were not visible.[54] Can you see where this is going? Before the

---

[45] *Id.*

[46] Molly McDonough, *Facebooking Judge Catches Lawyer in Lie, Sees Ethical Breaches*, A.B.A. J., July 31, 2009, http://www.abajournal.com/news/facebooking_judge_catches_lawyers_in_lies_crossing_ethical_lines_abachicago/.

[47] *Id.*

[48] *Id.*

[49] *Id.*

[50] *Id.*

[51] Ngai v. Old Navy, No. 07-5653 (KSH) (PS), 2009 WL 2391282, at *1 (D.N.J. July 31, 2009).

[52] *Id.*

[53] *Id.*

[54] *Id.*

deposition, the two sent eleven text messages between themselves.[55] During the one hour and twelve minute deposition, the attorney and client exchanged five more text messages.[56] Then came one of those moments that make the virtuous smile. The *pro hac vice* attorney inexplicably sent a text to the *plaintiffs'* attorney saying, "[you are] doing fine," thus hoisting himself on his own petard.[57] Suspecting (do you think?) that something fishy was afoot, the plaintiffs' attorney requested that the *pro hac vice* attorney preserve his text messages from the deposition.[58]

When all was said and done, the essence of the argument against producing the text messages was that they were protected by the attorney-client privilege.[59] The court did indeed find that the text messages made before the deposition were privileged,[60] but the text messages sent during the course of the deposition were not.[61] The court stated that the *pro hac vice* attorney violated Federal Rule of Civil Procedure Rule 30 by texting during the deposition.[62] The court equated the conduct with passing notes to the client that included instructions "intended to influence the fact finding goal of the deposition process."[63]

Had it not been for the *pro hac vice* attorney sending a text to the plaintiffs' attorney, no one would likely have known of this impermissible (and ethically questionable) conduct. It will be a sad day for our system if deposing attorneys need to include a "no texting" provision to deposition admonitions.

In another case, a California lawyer (non-practicing) was suspended for blogging about a trial while serving as a juror.[64] The lawyer had been warned not to discuss the case, orally or in writing,[65] but he apparently knew better, as egotistical individuals always seem to. "Nowhere do I recall the jury instructions mandating [that] I can't post comments in my blog about the trial[.]"[66] He then proceeded to describe the judge and the

---

55 *Id.*

56 *Id.*

57 *Id.* (alteration in original).

58 *Id.*

59 *Id.* at *2.

60 *Id.* at *4.

61 *Id.*

62 *Id.* at *4 (citing FED. R. CIV. P. 30(c)).

63 *Id.*

64 Martha Neil, *Calif. Lawyer Suspended Over Trial Blogging While Serving as Juror*, A.B.A. J., Aug. 4, 2009, http://www.abajournal.com/news/calif._lawyer_suspended_over_trial_blog_while_serving_as_juror/.

65 *Id.*

66 *Id.*

defendant in an insulting manner.[67] Because of his misconduct, the appellate court reversed the felony burglary conviction.[68] The California Bar disciplinary authorities were not amused and his law license was suspended for forty-five days.[69]

Let us not assume the judiciary is immune to the temptations of the technological world. On April 1, 2009, the North Carolina Judicial Standards Commission publicly reprimanded a district court judge for making Facebook posts about a child custody and support hearing being tried before him.[70] During the hearing, which lasted from September 9 to September 12, 2008, the judge and the attorney for the defendant became Facebook "friends" and conversed online about the case, with topics ranging from when the case would be settled to whether one of the parties had engaged in an affair.[71]

The judge also used Google to research the plaintiff's business website, which had not been offered into evidence.[72] The judge never disclosed this outside research to the parties or their counsel.[73] On October 14, the judge disqualified himself from the case and his order was vacated.[74] The North Carolina Judicial Standards Commission concluded that the "[j]udge['s] actions constitute[d] conduct prejudicial to the administration of justice that brings the judicial office into disrepute."[75] The judge promised to familiarize himself with the Code of Judicial Conduct and avoid committing such infractions again.[76]

III. WHY GO WHERE DANGER LURKS EVERYWHERE?

For the lawyers, social networking provides a new venue for marketing and at a lawyer's favorite price—free.[77] What can they accomplish on these social networks that have such appeal?

1. They can establish themselves as having expertise in a particular area of law.[78]

---

[67] *Id.*

[68] *Id.*

[69] *Id.*

[70] Ryan Jones, *Judge Reprimanded for Discussing Case on Facebook*, THE-DISPATCH.COM, June 1, 2009, http://www.the-dispatch.com/article/20090601/ARTICLES/905319995/1005?Title=Judge-reprimanded-for-discussing-case-on-Facebook.

[71] *Id.*

[72] *Id.*

[73] *Id.*

[74] *Id.*

[75] *Id.*

[76] *Id.*

[77] Susi Schuele, *Social Networking for Lawyers: The Lawyer's Guide to Making Friends*, GPSOLO, June 2009, at 40, 41.

2. They can gather followers if they provide consistently valuable content.[79]

3. They can create an online network, and sometimes, they can move that network offline.[80]

4. They may attract reporters, who are known to use and quote blogs on a regular basis.[81]

5. They may receive speaking invitations, leading to business opportunities.[82]

6. They can follow what others in their field are doing and emulate them whenever good ideas crop up.[83]

7. They can simply follow those who give out good information, helping to keep themselves current in their area of practice.[84]

8. They can start up conversations with those in their target markets.[85]

9. Most of all, "there is gold in them thar hills," which deserves its own section of this Article, as social networking sites so often offer up gold nuggets of evidence.[86]

IV. SOCIAL NETWORKING AS EVIDENCE

The legal world took notice when, on February 20, 2009, the Ontario Superior Court of Justice permitted a defendant to cross-examine a plaintiff in a tort suit about his private Facebook profile.[87] The Court

---

[78] *Id.*

[79] *See id.*

[80] *See id.* at 42.

[81] *See* Andrew Updegrove, *The Profession: Essentials of Creating a Successful Legal Blog*, BOSTON B.J., May–June 2007, at 16, 17.

[82] Diane Levin, *Only Connect: The Impact of Blogging on the Field of ADR*, DISP. RESOL. MAG., Summer 2009, at 24, 25–26.

[83] *See id.* at 26.

[84] *See id.*

[85] *See* Schuele, *supra* note 77, at 43.

[86] *See infra* text and accompanying notes 87–108.

[87] Tariq Remtulla, *Canada: Facebook Not So Private? Ontario Court Finds Facebook Profile Discoverable*, MONDAQ, Mar. 23, 2009, http://www.mondaq.com/article.asp?articleid=76332.

noted that it was "reasonable to infer that his social networking site likely contain[ed] some content relevant to the issue of how [the plaintiff] has been able to lead his life since the accident."[88]

There is also the famous case where a woman claiming serious injuries after a car accident was confronted by photos of her skiing in the Swiss Alps.[89] Whoops.

In another case, a woman lost a custody battle after sexually explicit comments on her boyfriend's MySpace page came to light.[90] And in yet another instance, a husband lost credibility after describing himself on MySpace as "single and looking."[91]

In criminal cases, social networking sites often come into play. In 2007, Jessica Binkerd was sentenced to five years and four months in prison after she drove under the influence of alcohol and was involved in a crash that resulted in the death of her passenger.[92] Her attorney anticipated that she would get probation, but she was sentenced to prison after evidence from her MySpace page showed her wearing an outfit with a belt that had plastic shot glasses on it.[93] Other photos showed her holding a beer bottle and wearing a shirt advertising tequila.[94] As her attorney put it, even though the outfit was part of a Halloween costume, the photos were all the judge talked about, saying that she had learned no lesson and showed no remorse.[95]

In 2008, two weeks after being charged with drunk driving in an accident that seriously injured a woman, Joshua Lipton made the foolish decision to show up at a Halloween party in a prisoner costume with the label "Jail Bird" on his orange jumpsuit.[96] Someone posted the photo on Facebook and the prosecutor made effective use of the photo of this young man partying while his victim was recovering in a hospital.[97] The judge called the photos "depraved" and sentenced him to two years in prison.[98]

---

88 *Id.*

89 Shannon Kari with Matthew Coutts, *Facebook Postings Not Serious: Defence*, NAT'L POST, Feb. 12, 2008, *available at* http://www.financialpost.com/news-sectors/technology/story.html?id=302023.

90 Vesna Jaksic, *Litigation Clues Are Found on Facebook*, NAT'L L.J. (New York City), Oct. 15, 2007, at 1.

91 *Id.*

92 *Id.* at 7.

93 *Id.*

94 *Drinking, Driving, and Facebook Don't Mix*, CBS NEWS, July 18, 2008, http://www.cbsnews.com/stories/2008/07/18/tech/main4272846.shtml.

95 Jaksic, *supra* note 90, at 7.

96 *Drinking, Driving, and Facebook Don't Mix*, *supra* note 94.

97 *Id.*

98 *Id.*

In another sentencing hearing, Matthew Cordova found himself with a five-year prison sentence in Arizona.[99] He had pled guilty to aggravated assault with a gun.[100] At the hearing, his attorney tried to portray him as a peaceful man who had found religion, yet the prosecution had a MySpace picture of Cordova holding a gun which he posted comments about.[101]

In 2009, Raul Cortez was found guilty of murder.[102] He might not have been sent to death row, however, without the gang signs and colors displayed on his MySpace page being introduced in court.[103]

The police often use social networking sites in their investigations, while prosecutors check the sites of gang members, who regularly discuss their activities on their social networking sites.[104] Happily, they are often dumb enough to provide great fodder for criminal investigations.[105]

Many divorce attorneys have reported to the authors that, whenever they get a new case, they Google all the parties (including their own client) and also check their social networking sites. In one such case in which the authors were involved, a well-groomed woman who portrayed herself as a "soccer mom" was undone by explicit photos of herself that she had posted online looking to "hook up" with men.[106] Dad got custody.[107]

In another case the authors handled, a wife learned of her husband's infidelity because she talked to his lover on his Facebook page.[108] Though the wife had no access to the page, one of her friends did.

It should now be a matter of professional competence for attorneys to take the time to investigate social networking sites. You must pan for gold where the vein lies—and today, the mother lode is often online.

---

[99] Erica Perez, *Getting Booked by Facebook*, MILWAUKEE J. SENTINEL, Oct. 3, 2007, at 9A, *available at* http://www.redorbit.com/news/technology/1087625/getting_booked_by_facebook/index.html.

[100] *Id.*

[101] Jaksic, *supra* note 90, at 7.

[102] Jay Gormley, *MySpace and Facebook Becoming Evidence in Court*, CBS11TV.COM, Feb. 3, 2009, http://cbs11tv.com/local/MySpace.Facebook.Evidence.2.926231.html.

[103] *Id.*

[104] *See* Jaksic, *supra* note 90, at 7.

[105] *Id.*

[106] Sharon D. Nelson & John W. Simek, *Adultery in the Electronic Era: Spyware, Avatars and Cybersex*, WYO. LAW., Dec. 2008, at 1, 1–2, *available at* http://wyomingbar.org/pdf/barjournal/barjournal/articles/Cybersex.pdf?-session=wybar_user:C6319D2B1890131606osFDE6E8B4.

[107] *Id.*

[108] *Cf.* Ride the Lightning, Social Networks: An Avalanche of Evidence, http://ridethelightning.senseient.com/2009/03/social-networks-an-avalanche-of-evidence.html (Mar. 10, 2009, 14:42 EST).

V. HOW MIGHT LAWYERS MANAGE TO GET THEMSELVES TAKEN TO THE WOODSHED?

Apart from some of the courtroom and litigation antics referenced earlier, these areas of conduct may cause an attorney a great deal of trouble:

1. They shill for themselves, which not only backfires as a marketing target, but may violate state ethical rules regarding lawyer advertising.[109]

2. They deliberately or inadvertently form an attorney-client relationship.[110]

3. They drink a glass of wine or two or six and say or do something unwise online.

4. They treat their online conduct as trivial, without the recognition that what you do online may-well live forever. The authors have been told by people who have contacted representatives of Twitter that the company has every tweet that has ever gone out.[111]

5. They fail to realize that they may be divulging client confidences. Even though only their "friends" may have access to their Facebook page, those "friends" may shoot off posts to anyone they wish.

6. They do not properly investigate the privacy settings and therefore expose their online conduct where they may not mean to.

7. They mix their personal and professional online conduct together—not always a wise move. Think, for instance, of a fifty–year-old lawyer who has a child who is her friend on Facebook.

---

[109] *See* MODEL CODE OF PROF'L RESPONSIBILITY DR 2-101(A) (1983) ("A lawyer shall not, on behalf of himself . . . use or participate in the use of any form of public communication containing a . . . self-laudatory . . . statement or claim.").

[110] *See* MODEL CODE OF PROF'L RESPONSIBILITY DR 2-104(A)(4) (1983) (individualized legal advice may bar future employment); MODEL RULES OF PROF'L CONDUCT R. 1.2 annot. at 37 (2003) (unofficially advising pro se litigants is common but disfavored).

[111] *See* Posting of Marshall Kirkpatrick to ReadWriteWeb, Confirmed: Twitter Is Saving All Your Tweets, After All, http://www.readwriteweb.com/archives/confirmed_twitter_is_saving_all_your_tweets_after.php (Sept. 25, 2009, 11:05 PST).

The child posts inebriated photos of her mom at her birthday celebration. Mom would have known better—the daughter may not.

8. They get online when they are angry and say something defamatory.

9. They do not proofread and they look like idiots, which is counter-productive to their marketing efforts.

10. They talk about their colleagues, their bosses, their adversaries and their clients, potentially unleashing a perfect storm of unethical conduct.

11. They use deceit to bypass the privacy settings of a social networking site. As an example, an attorney may try to inveigle a third-party into "friending" someone on Facebook in order to gain access to an opposing party's Facebook page.

VI. SOCIAL NETWORKING: AN E-DISCOVERY AND RECORDS MANAGEMENT NIGHTMARE[112]

Even if you haven't caught what some have deemed "the Twitter bug," some within your firm likely have.[113] And what are they saying, when sending their "tweets" via Twitter?[114] Everyday comments like "[w]alking the dog[]" and "[w]hen did I get so darn fat[.]"[115] But they are also saying "the Smith, Smith, and Smith law firm is EVIL" and naming names.[116] They might also be saying, "We're working on a case that's going to put Acme Corporation in a stock market tailspin."[117]

If you have a "pish posh" reaction to Twitter, you might want to rethink that feeling.[118] "From the *National Law Journal*: 'Beware, Your 'Tweet' on Twitter Could Be Trouble[.] Subheader: Latest networking craze carries many legal risks."[119]

---

[112] Adapted from Sharon D. Nelson & John W. Simek, *Capturing Quicksilver: Records Management for Blogs, Twittering and Social Networks*, WYO. LAW., June 2009, at 1, *available at* https://www.wyomingbar.org/pdf/barjournal/barjournal/articles/Twitter.pdf [hereinafter *Capturing Quicksilver*].

[113] *Id.* at 1.

[114] *Id.*

[115] *Id.*

[116] *Id.*

[117] *Id.*

[118] *Id.*

[119] *Id.* (quoting Tresa Baldas, *Beware: Your 'Tweet' on Twitter Could Be Trouble*, NAT'L L.J. (New York City), Dec. 22, 2008, at 6).

"[I]s a tweet done on firm resources a 'record' for purposes of retention requirements and ESI preservation/production?"[120] Perhaps . . . or perhaps not. Much of this remains unsettled ground.[121]

"If you find that scary, you're not alone."[122] For a while, record managers no doubt thought they had the universe pretty well covered with e-mail and company-approved programs.[123] After a while, some of them caught up with instant messages.[124] But Twitter, blogs, and social networks have given almost everyone a Goliath-sized headache.[125] Whether you are thinking in terms of your own law firm or your clients, you must now consider these new technologies.[126]

They bedevil records management ("RM") in particular.[127] The minute RM catches up to technology, technology leapfrogs ahead with something else to cause consternation.[128]

Douglas Winter, who heads the electronic discovery unit at Bryan Cave, describes tweets as being no different from letters, e-mail, or text messages: they can be damaging and discoverable, which could be especially problematic for companies that are required to preserve electronic records, such as the securities industry and federal contractors.[129] Yet another compliance headache is born.[130]

Tom Mighell of the electronic discovery company Fios suggests that we may find a post from a proud employee that says: "[O]ur disc brakes are fine. I'm an engineer on that product. We test to 5x tolerance on the label, so you can be rougher on them than you think. Don't worry."[131] As Tom points out, after that post, "[y]ou've got potential product liability in 140 characters."[132]

---

[120] *Id.*

[121] *Id.*; *see also* Therese Craparo & Anthony J. Diana, *United States: The Next Generation of E-Discovery: Social Networking and Other Emerging Web 2.0 Technologies*, MONDAQ, Aug. 4, 2009, http://mondaq.com/article.asp?articleid=84000 (discussing the "developing legal landscape" concerning Web 2.0 technologies).

[122] *Capturing Quicksilver*, *supra* note 112, at 1.

[123] *Id.*

[124] *Id.*

[125] *Id.*

[126] *Id.*

[127] *Id.*

[128] *Id.*

[129] *Id.* at 1–2 (quoting Baldas, *supra* note119, at 6).

[130] *Capturing Quicksilver*, *supra* note 112, at 2.

[131] *Id.*; Kim S. Nash, *Text Messaging, Facebook Can Get You in Legal Trouble*, PC WORLD, Nov. 6, 2008, http://www.pcworld.com/businesscenter/article/153418/text_messaging_facebook_can_get_you_in_legal_trouble.html.

[132] *Capturing Quicksilver*, *supra* note 112, at 2.

Twitter is by no means alone.[133] There is also Yammer, and present.ly[134] (no, that's not a typo)—and surely many more to come. Enterprise versions are just beginning to emerge, and companies are now faced with the dilemma of developing policy to govern them.[135]

A. Blogs

As blogs have exploded in popularity over the last few years, so have corporate security concerns.[136] Not only might employees disclose trade secrets or divulge insider information on their blogs, but misuse of blogs could also lead to wrongful termination or harassment suits.[137]

There should, of course, be a company policy about blogging at work or about work.[138] Many companies sanction blogs. Microsoft has hundreds of them.[139] One case has suggested that employers may have the right to prevent employees from accessing blogs while at work, which may fend off some of the dangers associated with blogging.[140]

If blogs are allowed at work, the company needs to maintain blog archives where retention is mandated under laws or regulations.[141] Blogs do indeed create a "paper" trail, for better or worse.[142] Corporate blogging and individual employee blogging present different challenges: one clearly speaks for the corporation,[143] while the other may or may not, depending on the circumstances.[144]

Enterprise blogs require security, authentication, and audit trails.[145] Likewise, it should be possible to search them, issue reports, etc.[146] Control over enterprise blogs can be appliance-based, an enterprise application, or through software as a service ("SaaS").[147]

---

[133] *Id.*

[134] *Id.*; *see* Yammer: About, https://www.yammer.com/about/about (last visited Nov. 19, 2009); Present.ly - Tour, https://presentlyapp.com/tour (last visited Nov. 19, 2009).

[135] *Capturing Quicksilver*, *supra* note 112, at 2.

[136] *Id.*

[137] *Id.*

[138] *Id.*

[139] *Id.*; *see* Microsoft Community Blogs Search Results, http://www.microsoft.com/communities/blogs/PortalHome.mspx (click "Go") (last visited Nov. 19, 2009) (listing various blogs).

[140] *Capturing Quicksilver*, *supra* note 112, at 2 (citing Nickolas v. Fletcher, No. 3:06-CV-00043 KKC, 2007 WL 1035012, at *1, 9 (E.D. Ky. Mar. 30, 2007)).

[141] *Id.*

[142] *Id.*

[143] *Id.*

[144] *Id.*

[145] *Id.* at 3.

[146] *Id.*

[147] *Id.*

Audit trails should capture all changes, including new posts, changed or deleted posts, and comments and discussion.[148] They should capture context, including who posted/commented, what posts are read, and what posts are trackbacked.[149]

One wit has suggested a very simple corporate blog policy: "Just try to be smart about it."[150]

B. Social Networks

The lifeblood of many employees is their social networks, including MySpace, Facebook, LinkedIn, and Plaxo.[151] Besides being gigantic timewasters, these sites abound with risks for businesses as most businesses do not monitor their employees' sites.[152] Therefore, all the risks associated with blogs apply here.[153] Some experts believe that companies may be well-advised to use filters to block access to social networking sites at work.[154] At the very least, this action will keep the posts from being company records.[155] In fact, a recent survey conducted by web filter ScanSafe found that seventy-six percent of ScanSafe's clients are indeed blocking access to social networking sites, an astonishingly high percentage.[156] Companies report seeing such sites as both a security risk and a productivity drain.[157] On the other hand, genuine business usage of these sites has grown tremendously[158] and it may be very difficult to allow business usage and forbid personal usage, no matter what a company's policy may say.[159]

A 2008 independent survey commissioned by FaceTime Communications (based in the U.K., but we have no reason to suspect the answers would be much different here) found that roughly eighty

---

148 *Id.*

149 *Id.*

150 *Id.*; Jeremy Zawodny, Yahoo! Employee Blog Guidelines: The Official Version and My Own Advice, http://jeremy.zawodny.com/blog/archives/004725.html (May 31, 2005, 22:35 EST).

151 *Capturing Quicksilver*, *supra* note 112, at 3.

152 *Id.*

153 *Id.*

154 *Id*; *see also* Craparo & Diana, *supra* note 121 (suggesting that companies address the Web 2.0 trend before the issued is forced upon them).

155 *Capturing Quicksilver*, *supra* note 112, at 3.

156 *See* Chuck Miller, *Survey: Social Networks Increasingly Blocked*, SC MAGAZINE, Aug. 19, 2009, *available at* http://www.scmagazineus.com/Survey-Social-networks-increasingly-blocked/article/146833/.

157 *Capturing Quicksilver*, *supra* note 112, at 3.

158 *Id.*; *see also Online Social Networks Go to Work*, MSNBC INTERACTIVE, 2009), http://www.msnbc.msn.com/id/5488683/ (last visited Nov. 19, 2009) (discussing the popularity and benefits of the use of social networking sites at work).

159 *Capturing Quicksilver*, *supra* note 112, at 3.

percent of employees use social networks at work, a statistic that was true of *both* personal and business use.[160] The work-related purposes included professional networking, researching, and learning about colleagues.[161]

As may be obvious, checking the social networking sites of potential employees could be wise, as an employer might get some sense of trouble brewing in the future: a lack of discretion, angry entries, a "TMI" (too much information) proclivity, etc.[162]

Is employer monitoring of social networking sites really happening in the wild?[163] The authors conducted an ad hoc online survey. While everyone said an employer had a right to monitor, no one actually knew of an employer who *was* monitoring personal sites.[164]

C. Toss or Keep?

From our viewpoint, as folks involved in computer forensics, if you don't legally have to keep data and can't think of a reason why you should keep it, toss it.[165] You'll save a fortune if you become embroiled in litigation.[166] Shrinking the data to search will shrink the volume of potentially responsive data that must be reviewed.[167]

Some of the emerging technologies are fluid: comments on blogs, ever-expanding discussions on "wikis," changes on social networking sites, etc.[168] How do you manage something that isn't static and that has multiple authors?[169] Snapshots are one method with risk assessments performed to determine how often snapshots must be taken.[170] Periodic archiving is another possibility, though it is a headache (again) to figure out how to schedule it.[171] Training is helpful—employees need to understand that they are creating "records" when they use these technologies and that they must think before they create records, bearing in mind the risks of the records they create.[172]

---

[160] *Id.*; FACETIME COMMUNICATIONS, THE COLLABORABORATIVE INTERNET: USAGE TRENDS, EMPLOYEE ATTITUDES AND IT IMPACTS, (Oct. 2008), http://www.facetime.com/survey08/summary/.

[161] *Capturing Quicksilver*, *supra* note 112, at 3.

[162] *Id.*

[163] *Id.*

[164] *Id.*

[165] *Id.*

[166] *Id.*

[167] *Id.*

[168] *Id.*

[169] *Id.*

[170] *Id.* at 3–4.

[171] *Id.* at 4.

[172] *Id.*

It's a brave new world, and most corporations and law firms are having a heck of a time dealing with it. It can involve huge costs, business disruptions, public embarrassment, and even legal liability.[173] Management of Web 2.0 records is limited at best, often chaotic, and duplicative.[174] This is a huge challenge for record managers. And ponder this Web 2.0 risk scenario from Michael Cobb:

> Suppose you're the CIO of a company that dominates its market to the point where competitors are grumbling about monopolistic practices. Some of your employees decide to "help" by going on the offensive, denigrating these grumbling competitors in off-site blog posts and wiki entries, tagging negative stories on the Web, posting slanted questions on LinkedIn, fostering criticism on Facebook and so on. Then the company is hit with a lawsuit by its competitors for engaging in an alleged smear campaign. Your general counsel proclaims innocence and tries to limit the scope of discovery, but is compelled by law to agree to hand over all relevant ESI.[175]

Again, interesting. Your opponents will have trolled the Web for data.[176] Can you claim ignorance?[177] Must you produce these off-site communications by your employees?[178] Can you afford not to know about Web 2.0 data?[179] These are questions that are giving CEOs (and their lawyers) recurring nightmares.[180]

VII. PRIVACY, WHAT PRIVACY?

Further compounding these problems is the belief that what a user posts is private and will only be seen by them and their select "friends." Thus, individuals go "hogwild" and provide personal information they might otherwise keep to themselves.

For instance, a Facebook profile can contain a virtual treasure trove of personal information: an individual's name; birthday; political and religious views; contact information; gender; sexual preference; relationship status; favorite books, movies, etc.; educational and employment history; and pictures.[181] As the list of features and applications available to those frequenting social networking sites has

---

[173] *Id.*

[174] *Id.*

[175] *Id.* (quoting Michael Cobb, *Web 2.0 and E-Discovery: Risks and Countermeasures*, SEARCHSECURITY, July 2, 2008, http://searchsecurity.techtarget.com/tip/0,289483,sid14_gci1319551,00.html).

[176] *Capturing Quicksilver*, *supra* note 112, at 4.

[177] *Id.*

[178] *Id.*

[179] *Id.*

[180] *Id.*

[181] James Grimmelmann, *Saving Facebook*, 94 IOWA L. REV. 1137, 1149 (2009).

grown, so too has the depth of information about both who you are and who you know.[182]

Consider for example the all too familiar scenario of a job applicant losing his or her employment offer after the employer finds out that one of their listed interests on Facebook is "smoking blunts."[183]

And while the above story may not seem to have far-reaching implications, others expose the darker side of privacy concerns. For instance, someone used personal photographs obtained from a private photo album to blackmail Miss New Jersey 2007.[184] The thought that anyone can dig up private photographs and disclose them to the world at large is enough to send shivers down anyone's spine.

Making matters worse, unbeknownst to the average citizen, courts have been unwilling to recognize a reasonable expectation of privacy for materials people willingly post on the Internet without taking any measures to restrict access to them, or otherwise protect them.[185]

One such cautionary tale is the case of Cynthia Moreno.[186] After a hometown newspaper publicized her online tirade about how much she despised the town in which she had grown up, both she and her family were subjected to a violent barrage of community outbursts.[187] Ms. Moreno then brought suit against the newspaper alleging, among other things, that the newspaper violated her privacy by publishing her online remarks in the newspaper.[188] The court explained that the crucial ingredient for an invasion of privacy claim, the public disclosure of private facts, was missing because Ms. Moreno's "affirmative act made her article available to any person with a computer and thus, opened it to the public eye."[189] As such, the court stated it had no choice but to

---

[182] *See id.* at 1150 (explaining how sending gifts, creating quizzes, utilizing the poke, or playing games through the multitude of Facebook applications can reveal things about a person's knowledge, beliefs, and preferences).

[183] *Id.* at 1165 (citing Alan Finder, *When a Risque Online Persona Undermines a Chance for a Job*, N.Y. TIMES, June 11, 2006, § 1, at 1).

[184] *Id.* (citing Austin Fenner, *N.J. Miss in a Fix over Her Pics*, N.Y. POST, July 6, 2007, at 5, *available at* http://www.nypost.com/p/news/regional/item_u9E3QCTLwd5sD0Wz7Zb0MO).

[185] *See supra* text and accompanying notes 87–150.

[186] Moreno v. Hanford Sentinel, Inc., 91 Cal. Rptr. 3d 858 (Cal. Ct. App. 2009).

[187] *Id.* at 861. Local reaction to the publication was alleged to include "death threats and a shot fired at . . . [Ms. Moreno's] family home." *Id.* The complaint alleged that David Moreno's twenty-year-old family business lost so much money that it was closed, and the family subsequently relocated. *Id.*

[188] *Id.*

[189] *Id.* at 862.

dismiss her invasion of privacy cause of action, even if Ms. Moreno had meant her thoughts for a limited few people on her MySpace page.[190]

Similarly, in *Pennsylvania v. Protetto*, the court held that no expectation of privacy existed with regard to either sexually explicit e-mail messages sent by a man to a fifteen-year-old girl or an electronic chat room conversation between them.[191] Here, the court based its finding on the fact that once sent, the e-mail messages could have been forwarded to anyone, and people often pretend to be someone they are not in a chat room.[192]

Finally, in perhaps the best illustration of the risks associated with posting information about oneself on a social network, the court in *Cedric D. v. Stacia W.* terminated a father's parental rights after viewing his MySpace profile.[193] In so holding, the court found the information posted on his profile highly relevant and determined that it suggested "'his lifestyle was not conducive to one in the best interest of a child.'"[194] As cases like this illustrate, content on an individual's social networking profile may now play a role in establishing criminal or civil liability in court proceedings.[195] More importantly, this case stands for the proposition that users can and will be held accountable for their statements on social networking sites, sometimes with life-altering consequences.[196]

Several different policy interventions have been proposed to "fix" social networks' privacy problems.[197] Some individuals say that perhaps the best policy is to do nothing and allow market forces to establish the

---

[190] *Id.* at 863. Although the court dismissed Ms. Moreno's invasion of privacy claims, the court did allow Ms. Moreno's other cause of action, the intentional infliction of emotional distress, to move forward. *Id.* at 864.

[191] Commonwealth v. Proetto, 771 A.2d 823, 831–32 (Pa. Super. Ct. 2001).

[192] *Id.* at 830. The court analogized

> [s]ending an e-mail or chat-room communication . . . to leaving a message on an answering machine. The sender knows that by the nature of sending the communication a record of the communication, including the substance of the communication, is made and can be downloaded, printed, saved, or in some cases, if not deleted by the receiver, will remain on the receiver's system. Accordingly, by the act of forwarding an e-mail or communication via the Internet, the sender expressly consents by conduct to the recording of the message.

Id.

[193] Hillel I. Parness, *Toward "Social Networking Law"?*, LANDSLIDE, Mar./Apr. 2009, at 13, 16 (citing Cedric D. v. Stacia W., No. 1 CA-JV 07-0056, 2007 WL 5515319, at *4 (Ariz. Ct. App. Sept. 20, 2007)).

[194] *Id.* (quoting *Cedric D*, 2007 WL 5515319, at *4.).

[195] *Id.*

[196] *See id.* (citing *Cedric D*, 2007 WL 5515319).

[197] *See generally* James Grimmelmann, *supra* note 181, at 1178–1206 (2009) (discussing proposed solutions to privacy problems that likely will or will not be successful).

optimal level of privacy protection.[198] Others have argued for better technical controls or establishing user restrictions.[199] Still others have suggested a strengthened, public-disclosure tort and a right to opt out.[200]

In order for any of these policies to be practical, they must take into account the social dynamics of social networking and attempt to balance the "good" (i.e., reasons an individual joins a social network in the first place) with the "bad" (i.e., the potential privacy risks that can occur).[201] Which one will provide the best solution is a question that only time and trial-and-error will answer.

For the time being, users should not allow themselves to be lulled into a false sense of security; rather, be mindful that the information they provide may be subject to strict scrutiny by potential employers, the legal system, and their peers. In a report released in August 2009, for example, forty-five percent of employers were reported to use social networking sites to research their job candidates.[202] In the end, privacy risks all come down to what and how much users choose to share about themselves. Perhaps when users decide to join a social network they should be given a *Miranda*-like warning, letting them know that what they say can and will be used against them.

A. Not Just a "Minor" Problem: Social Networking and Sexual Predators

From ninety-year-old grandmothers to a brother's annoying eighth grade sister, everyone is catching the social networking bug. On a darker note, cyber criminals have also begun to tap into social networks and turn these sites into their own twisted little playgrounds.[203] Recently, the New York State Attorney General launched a probe into allegations that while Facebook claims to provide a safe online environment, parental complaints of inappropriate and sexually explicit material were allegedly not addressed by Facebook in a timely manner.[204]

---

[198] *See id.* at 1178.

[199] *Id.* at 1184.

[200] *Id.* at 1195–97.

[201] *See id.* at 1206.

[202] *See* Press Release, PRNewswire, Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds (Aug. 19, 2009), http://uncw.edu/stuaff/career/documents/employersusing socialnetworkingsites.pdf.

[203] Sander J.C. Van Der Heide, Note, *Social Networking and Sexual Predators: The Case for Self-Regulation*, 31 HASTINGS COMM. & ENT. L.J. 173, 176–77 (2009) (citing Jessica S. Groppe, Note, A Child's Playground or a Predator's Hunting Ground?—How to Protect Children on Internet Social Networking Sites, 16 COMMLAW CONSPECTUS 215, 215–16 (2007)).

[204] Joseph Spector, *Cuomo Launches Probe of Facebook*, J. NEWS (Westchester County, N.Y.), Sept. 25, 2007, at 1B.

And while Facebook and MySpace have set minimum age restrictions for users at age thirteen,[205] an overwhelming number of social network users are, and will continue to be, minors. The large number of children using social networks combined with the prevalence of illicit behavior poses several legal and moral issues regarding what obligations and duties, if any, social networking sites owe to their users.

Various attempts have been made to regulate social networking sites by requiring age verification of site users to prevent sexual predators from turning these sites into hunting grounds.[206] These attempts, however, "have been largely unsuccessful and have given rise to well-established legal defenses."[207] Most notably, social networks have put up legal roadblocks by arguing that they are either immune from liability under the Communications Decency Act of 1996 ("CDA") or that they owe no duty to protect others from a third-party's criminal or tortious acts.[208] These roadblocks have largely been successful in shielding websites from liability for the criminal and tortious acts of their users, thereby preventing injured parties from seeking recourse from anyone save the offending party.[209]

Two recent major cases highlight these well-established lines of defense that social networking sites typically employ when faced with prototypical sexual predator claims. In the first case, MySpace was sued in June 2006 by a mother and her fourteen-year-old daughter, because the girl had been sexually assaulted by a man whom she met on MySpace.[210] The complaint alleged that the social network provider had been grossly negligent, or at the very least negligent, in failing to prevent sexual predators from communicating with minors on its website.[211]

MySpace's first defense against this claim was that the immunity provided under the CDA barred any claims based on the publication of third-party content.[212] The court rejected and cited as "disingenuous" the

---

[205] Facebook Statement of Rights and Responsibilities, (Aug. 28, 2009), http://www.facebook.com/terms.php?ref=pf; MySpace Terms & Conditions, (June 25, 2009), http://www.myspace.com/index.cfm?fuseaction=misc.terms.

[206] *E.g.*, Michael D. Marin & Christopher V. Popov, Doe v. MySpace, Inc.*: Liability for Third Party Content on Social Networking Sites*, COMM. LAW., Spring 2007, at 3, 3.

[207] *Id.*

[208] *See id.* at 3–5 (citing Communications Decency Act of 1996, 47 U.S.C. § 230 (2006)).

[209] *Id.* at 3.

[210] Doe v. MySpace, Inc., 528 F.3d 413, 416 (5th Cir. 2008).

[211] *Id.* The plaintiff parent asserted claims against MySpace for "fraud, negligent misrepresentation, negligence, and gross negligence." *Id.*

[212] *See id.* In its pertinent part, the CDA provides that "[n]o provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1)

Plaintiffs' attempts to circumvent CDA immunity by arguing that their claims were not against MySpace as a publisher but rather were claims for failing to implement any safety measures.[213] Seeing through this artful pleading, the court held that the underlying bases of the plaintiffs' claims were predicated on MySpace's publication of third-party information; and thus, CDA immunity applied.[214]

In addition to the statutory immunity of the CDA, the district court found that there was no legal basis for the proposition that social networking websites have any duty to protect users for the actions of third parties.[215] And while exceptions to the general rule exist, none of the special relationship exceptions were found to apply in the case of online social networking.[216] A social network provider's relationship with its users is not one which gives rise to a duty to control their actions; a user is simply one of the hundreds of millions of people who have posted a profile on a website.[217]

Notwithstanding this attenuated relationship, the plaintiffs attempted to apply a novel theory of premises liability to argue that MySpace had a duty to protect its users from sexual predators.[218] The court rejected the argument stating that not only was there no legal basis for the plaintiffs' theory, but also that "[t]o impose a duty under these circumstances for MySpace to confirm or determine the age of each applicant, with liability resulting from negligence in performing or not performing that duty, would of course stop MySpace's business in its tracks and close this avenue of communication."[219]

Likewise, in another recent case, *Doe v. Sexsearch.com*, the plaintiff sued the website provider after he was introduced to and had sex with a fourteen-year-old girl posing as an eighteen-year-old, resulting in criminal proceedings against him.[220] Plaintiff employed a "double-barreled shotgun approach in this case,"[221] alleging a plethora of claims, all of which essentially "boil[ed] down to either (a) Defendants failed to discover that Jane Roe lied about her age . . . , or (b) the contract terms

---

(2006). Moreover, the CDA further articulates that "[n]o cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section." *Id*. at § 230(e)(3).

213 *MySpace*, 528 F.3d at 419–20 (quoting Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 849 (W.D. Tex. 2007)).

214 *Id.* at 420.

215 Doe v. MySpace, Inc., 474 F. Supp. 2d 843, 850–52 (W.D. Tex. 2007).

216 *Id.;* Marin & Popov, *supra* note 207, at 5.

217 Marin & Popov, *supra* note 207, at 5.

218 *Id.; MySpace*, 474 F. Supp. 2d at 851.

219 *Id.*

220 502 F. Supp. 2d 719, 722 (N.D. Ohio 2007).

221 *Id.* at 737.

[were] unconscionable."[222] Unfortunately for the plaintiff, the court determined that he failed to hit a claim upon which liability attached; this was due in large part because the court found that the defendants were immune from liability pursuant to Section 230 of the CDA.[223] The remaining claims were barred either by the Ohio state law or because the contract itself was generally not unconscionable.[224]

In reality, the preceding cases have done nothing to ease the blight of sexual predation occurring with the passive assistance of social networks. They simply reaffirm the fact that social networking sites have been able, thus far, to breathe easy under the auspices of the CDA and demonstrate that attempts to regulate social networks through tort law and legislative action have been for naught. But increasingly negative media scrutiny has caught the nation's attention and appears to be forcing social networking sites into action.[225] This negative national attention pulls at the heart of these social network providers—money. If parents prevent their minor children from using the websites in fear that they may become prey, it means less traffic going through them, which in turn drives down financial profits.

Illinois has recently issued an apparent warning about how far states may be willing to go to prevent online predators from using social networking.[226] The legislation bans all registered sex offenders from using social networking sites during parole.[227] You can see how this has caught the attention of social networks—if banning sex offenders does not work, perhaps the next step is to force these sites to increase and enforce their respective minimum age requirements.

VIII. COPYRIGHT ISSUES

As if there weren't already enough potential legal land mines when it comes to social networking, posting content that infringes on intellectual property rights can figuratively "blow up" in the faces of both users and social network providers.

---

[222] *Id.* at 724. In total, the plaintiff brought fourteen claims against the defendant which included: breach of contract, fraud, negligent infliction of emotional distress, negligent misrepresentation, breach of warranty, deceptive trade practices, unconscionability of contract, and failure to warn. *Id.* at 723–24.

[223] *Id.* at 724–28, 737 (citing 47 U.S.C. § 230 (2006)).

[224] *Id.* at 728–37.

[225] *See, e.g.,* Claire Cain Miller, *Facebook Moves to Improve Privacy and Transprency*, N.Y. TIMES, Aug. 27, 2009, http://bits.blogs.nytimes.com/2009/08/27/facebook-moves-to-improve-privacy-and-transparency/.

[226] *See* H.R. 1314, 96th General Assem., Reg. Sess. (Ill. 2009), *available at* http://www.ilga.gov/legislation/96/HB/09600HB1314enr.htm.

[227] *Id.* at § 3-3-7(a)(7.12).

In years past, social networking sites have usually been off-the-hook when it came to copyright infringement pursuant to the safe harbor provisions of the Digital Millennium Copyright Act ("DMCA"), so long as the provider complied with the "notice and take-down" provisions of the statute.[228] Recent lawsuits, however, brought by copyright owners against YouTube and Google for allegedly infringing on the copyright owner's copyrights, may force changes in the legal landscape of copyright law as it pertains to Internet providers and, specifically, to social networking sites.[229]

First, here is a brief history lesson. In 1998, Congress attempted to bring U.S. copyright law into the twenty-first century by ratifying the DMCA, which created a series of "safe harbors" for certain activities of qualifying Internet Service Providers ("ISPs").[230] Section 512 of the DMCA sets forth the criteria an ISP must meet in order to be afforded protection under the DMCA's safe harbor provision.[231] The DMCA requires that 1) the ISP has no "actual knowledge" that infringing material exists on its sites or 2) be aware of any factual evidence tending to make infringing content apparent and, 3) if aware, the site must promptly remove the infringing content.[232] Additionally, an ISP can receive no pecuniary gains "attributable to the infringing activity."[233] Finally, upon notice by the copyright owner of purportedly infringing content, the ISP must remove the material.[234] As a threshold matter, Section 512(i)(1)(A) of the DMCA requires an ISP to have "adopted and reasonably implemented" a policy informing subscribers of the service provider's right to terminate the access of repeat offenders in appropriate circumstances.[235]

Several cases have highlighted a straightforward application of Section 512(c) and the safe harbor provisions as applied to ISPs. Many of these cases have focused on the burden of the plaintiffs to notify the defendants of the infringing content. In one such case, brought in 2001, a federal district court in California determined that eBay could not be held accountable for its users' copyright infringement because the popular selling site did not have actual or constructive knowledge of the

---

228 *See* Digital Millennium Copyright Act, 17 U.S.C. § 512(c) (2006).

229 *See infra* text accompanying notes 238–246.

230 Lauren Brittain Patten, Note, *From Safe Harbor to Choppy Waters: YouTube, the Digital Millennium Copyright Act, and a Much Needed Change of Course*, 10 VAND. J. ENT. & TECH. L. 179, 188–90 (2007) (citing 17 U.S.C. § 512(c)).

231 *See* 17 U.S.C. § 512(c)(1).

232 *Id.* at § 512(c)(1)(A)(i)–(iii).

233 *Id.* at § 512 (c)(1)(B).

234 *Id.* at § 512 (c)(1)(C).

235 *Id.* at § 512(i)(1)(A).

alleged misconduct.[236] Finding that the website was afforded protection under the auspices of the safe harbor provisions of DMCA, the court granted eBay's request for summary judgment.[237]

Recently, however, several content owners have challenged the protection of Section 512(c) as it pertains to YouTube, a video sharing site. For instance, Viacom has sued YouTube and its parent company Google for copyright infringement, seeking at least one billion dollars in damages.[238] In its complaint, Viacom alleges that YouTube's popularity is built on the website's vast availability of infringing works.[239] Further, Viacom contends that YouTube uses this library of works to increase the amount of traffic drawn to its website.[240] Likewise, a second complaint, filed in May of 2007 by The Football Association Premier League, Ltd., accused YouTube of engaging in copyright infringement for YouTube's gain.[241] The plaintiffs argued that YouTube's ineffective "notice and take-down" mechanism is nothing more than a meaningless attempt to satisfy the requirements of the DMCA.[242] In fact, the plaintiffs complained that not only is it nearly impossible to find all infringing material, but it is also an exercise of futility since YouTube users simply repost the content under a different file name or user name.[243]

In light of these recent lawsuits, some legal experts have commented on the validity of the arguments presented. Some have opined that, if YouTube is serving advertisements according to the kind of videos a user views or searches for, this conduct could amount to a financial benefit attributable to the infringing activities.[244] Under this scenario, YouTube would apparently lose any protection provided through the DMCA's safe harbor provisions and effectively open the company up to legal liability for copyright infringement.[245] Others have argued that these lawsuits against YouTube illustrate the fundamental problems with the DMCA and urge concrete changes through the judicial system.[246] In either case, the outcomes of these cases could reshape the

---

[236] *See* Hendrickson v. eBay, Inc., 165 F. Supp. 2d 1082, 1093 (C.D. Cal. 2001).

[237] *Id.* at 1094, 1096 (citing 17 U.S.C. § 512(c) (2006)).

[238] Complaint for Declaratory and Injunctive Relief and Damages at 5, Viacom Int'l, Inc. v. YouTube, Inc., 540 F. Supp. 2d 461 (S.D.N.Y. 2008) (No. 07 CV 2103).

[239] *Id.* at 3.

[240] *Id.* at 2–5.

[241] Class Action Complaint at 2, Football Ass'n Premier League, Ltd. v. YouTube, Inc., 633 F. Supp. 2d 159 (S.D.N.Y. 2009) (No. 07 CV 3582).

[242] *See id.* at 4, 13, 21–23, 29.

[243] *Id.* at 28–30.

[244] *E.g.*, Kevin Fayle, *Understanding the Legal Issues for Social Networking Sites and Their Users*, FINDLAW.COM, (2007), http://technology.findlaw.com/articles/00006/010966.html.

[245] *See id*.

[246] *See* Patten, *supra* note 230, at 209–10.

legal obligations of social networking sites, the services they provide, and the business models used.

More certain, though, is the assertion that individual users should always keep in mind that existing laws apply equally to their online and offline conduct. Thus, each time a user posts content on a social network, whether it is text, graphics, photos, etc., the same copyright laws apply and the same risk of liability attaches.

A. Watch What You Say! Defamation Online Is on the Rise

At the risk of sounding like a broken record, social network users might want to watch what they say about other people when online. If a comment is considered defamatory in nature, a user may be liable in both criminal and civil proceedings.

On one hand, social network providers have, thus far, been able to insulate themselves from criminal or tortious liability as a result of a user's defamatory comments by implicating statutory immunities available under applicable law.[247] In fairly uniform fashion, courts have held that any claims premised on a website's role as the publisher of third-party content are barred by Section 230 of the CDA.[248]

For instance, in *Zeran v. American Online, Inc.*, the victim of an online prank sued America Online ("AOL") for its failure to remove the prank ad and failure to promptly post a retraction.[249] The website ad posting "described the [purported] sale of shirts featuring offensive and tasteless slogans related to the April 19, 1995, bombing of" an Oklahoma City federal building and instructed interested buyers to call "Ken" at the plaintiff's home telephone number.[250] Shortly thereafter, the plaintiff received a flood of calls, "comprised primarily of angry and derogatory messages, but also including death threats."[251]

In filing suit, the plaintiff argued that even if AOL was immune from liability with respect to the initial posting, it was negligent in failing to remove the messages after he notified the company of their falsity.[252]

The Fourth Circuit disagreed and upheld the lower court's decision that the CDA barred the plaintiff's claims by largely relying on the preemptive effect inherent in the CDA.[253] The court explained that even if notice had been given, the CDA immunizes interactive computer

---

[247] *See supra* text and accompanying notes 228–243.

[248] *See, e.g.,* Zeran v. America Online, Inc., 129 F.3d 327, 330–35 (4th Cir. 1997); Dimeo v. Max, 433 F. Supp. 2d 523, 527–31 (E.D. Pa. 2006).

[249] *Zeran*, 129 F.3d at 328.

[250] *Id.* at 329.

[251] *Id.*

[252] *See id.* at 330.

[253] *Id.* at 334–35.

service providers from liability stemming from defamatory or threatening posts.[254] Likewise, in cases following *Zeran*, courts have held that websites and other interactive computer services cannot be held liable for publishing defamatory statements created by a third-party.[255]

Conversely, because social networking users are not lucky enough to enjoy any of the immunities afforded to social networking sites, they should always be careful to act appropriately when posting messages to a particular site. The few cases on this issue so far have dealt with students suffering some type of legal action or adverse consequences at their schools after posting purportedly defamatory, threatening or indecent messages on social networking sites. Consider for example, the case *J.S. v. Blue Mountain School District*,[256] in which one student learned the potential ramifications of posting defamatory content the hard way. Here, the student created a personal profile on MySpace describing the principal of Blue Mountain Middle School, albeit not by name, as "a pedophile and a sex addict."[257] The school determined that the plaintiff student had violated several provisions of the school's disciplinary code and, as a result, levied a ten-day, out-of-school suspension against the student.[258] The parents of the student brought suit and argued that the punishment violated the United States Constitution because the conduct was outside the school and did not disrupt the classes and infringed upon their rights as parents to direct the upbringing of their child.[259] The court disagreed and held that because the vulgar, lewd, and potentially illegal speech had an effect on the school campus, the school did not violate the plaintiff's Constitutional rights by punishing the student for an imposter profile of the principal.[260]

In the context of defamation cause of actions, the current law appears to be: post a defamatory comment and you, the person posting the comment—not the social network provider—will bear the burden of defending against lawsuits brought by an allegedly injured party. The decision to post inappropriate comments is likely tied to the false sense

---

[254] *Id.* at 333–34. The court premised its decision on its belief that by imposing potential tort liability for an allegedly defamatory or threatening post would severely undermine the CDA's goal of promoting speech using these Internet services. *Id.*

[255] Marin & Popov, *supra* note 207, at 3.

[256] J.S. v. Blue Mountain Sch. Dist., No. 3:07CV585, 2008 WL 4279517 (M.D. Pa. Sept. 11, 2008).

[257] *Id.* at *1. The posted profile, which included the principal's photograph, described the principal's interests as "detention, being a tight ass, riding the fraintrain, spending time with my child (who looks like a gorilla), baseball, my golden pen, f---ing in my office, hitting on students and their parents." *Id.*

[258] *Id.* at *2.

[259] *Id.* at *3.

[260] *Id.* at *6, *9.

of privacy a user believes to be attached to social networking, whether from perceived anonymity or the fact that the individual is communicating with a machine rather than a person. Thus, as a rule of thumb, think through each posting and its possible legal implications before posting.

B. To Be or Not to Be a Journalist

More and more frequently, Internet users are turning to blogs as their primary source of major news stories or reading a blogger's posts as an alternative and independent source of the news.[261] As traditional journalists have been afforded both First Amendment and state statutory privileges, the question of whether bloggers should enjoy the same immunities has been pushed to the legal vanguard but remains undecided.[262] This question has sparked numerous debates and has been a catching point in federal legislation.[263] And while courts have yet to definitively fall on one side or another of this issue, a May 2006 ruling by a California appeals court seems to suggest that perhaps online bloggers have the same rights as their more traditional offline counterparts.[264]

In *O'Grady v. Superior Court*, Apple Computer, Inc. ("Apple") issued subpoenas to the publishers of websites seeking the identities of individuals who leaked information regarding new Apple products.[265] The publishers moved for a protective order to prevent the discovery of these sources citing confidentiality; however, the trial court denied this motion and granted Apple the authority to request such information.[266] The California Court of Appeals subsequently reversed this decision, holding that online journalists have the same right to protect the confidentiality of their sources as offline reporters do.[267]

Proponents advocating bloggers' rights have hailed this decision as the inception of bloggers being afforded the same rights as journalists.[268] Others have been less optimistic and have argued that the issue really boils down to whether a blogger acts like a traditional journalist or

---

[261] *See* Cydney Tune & Marley Degnar, *Blogging and Social Networking: Current Legal Issues*, *in* 929 INFO. TECH. LAW INST. 2008, NEW DIRECTIONS: SOCIAL NETWORKS, BLOGS, PRIVACY, MASH-UPS, VIRTUAL WORLDS AND OPEN SOURCE 73, 87 (2008).

[262] *See id.* at 87–88.

[263] *See id.* at 88.

[264] *See* O'Grady v. Superior Court, 44 Cal. Rptr. 3d 72 (Cal. Ct. App. 2006).

[265] *Id.* at 76.

[266] *Id.* at 81–82.

[267] *Id.* at 105–16.

[268] *E.g.*, Press Release, Electronic Frontier Foundation, Huge Win for Online Journalists' Source Protection, (May 26, 2006), http://www.eff.org/press/archives/2006/05/26.

not.[269] As the debate rages on, courts will likely make the final call on this hot new issue, building on the precedent of this particular case or departing from this decision and establishing a new line of reasoning.

C. Stolen: Your IDENTITY

All too often, a story will surface about how data thieves, through a social networking site, were able to steal proprietary or sensitive information.[270] The ease and frequency with which these virtual crooks have been able to gain access to private information is a serious cause for concern.

There is a virtual mountain of stories concerning the theft of personal information. Rather than exhaustively listing each and every one, a few of the most interesting and unique stories deserve reference.

Hackers have now turned their attention to the "hundreds of independent applications" created specifically for social networking.[271] In support for this, security blogger Chris Soghoian maintains that a recent article in *2600: The Hacker Quarterly* explained that many popular Facebook applications are vulnerable to simple attacks which allow the thief to view personal information sent to the application itself.[272]

Twitter has also been in the news frequently with respect to information theft. In one such attack, hackers made off with over 300 personal and confidential documents.[273] And these documents didn't just provide an individual's birthday or personal interests. No, "[s]ome of these documents include[d] credit card numbers, PayPal accounts," confidentiality agreements, and even security codes.[274]

This sort of identity theft is now big business—and, as always, the thieves are running way ahead of security experts and law enforcement.

D. Law Firm Social Networking Policies

So what are law firms to do? Finally realizing that there are problems with social networking, firms have been scrambling to enact special policies to deal with them. Approximately forty-five percent of law firms have gone so far as to block access to some of the most popular

---

[269] *See, e.g.*, Citizen Media Law Project, California Protections for Sources and Source Material, http://www.citmedialaw.org/legal-guide/california-protections-sources-and-source-material (last visited Nov. 19, 2009).

[270] *See infra* notes 271–274.

[271] Chris Soghoian, *Hackers Target Facebook Apps*, CNET NEWS, Mar. 27, 2008, http://news.cnet.com/8301-13739_3-9904331-46.html.

[272] *Id.* (citing Siderr, *Facebook Applications Revealed*, 2600: HACKER Q., Winter 2007–2008, at 32, 32–33).

[273] Andrew Lyle, *Twitter Hacked, Personal Documents Leak*, NEOWIN.NET, Jul. 17, 2009, http://www.neowin.net/news/main/09/07/17/twitter-hacked-personal-documents-leak.

[274] *Id.*

sites.[275] Some may have placed special restrictions on certain sites, while still others have done nothing thus far. And, if you have not completely barred access, you might want to consider this list of eight guidelines highlighting some of the policies every law firm should employ:

1. Remind attorneys that they should avoid the appearance of establishing an attorney-client relationship. Rule of thumb: Don't give legal advice—speak about the issues of law generally and factually instead.

2. Confidential information must at all times remain confidential. Firms must have a rule that explicitly forbids any posting of confidential information. Attorneys should be required to request permission to post any information that may even remotely seem private.

3. Strict privacy settings should be employed when joining a new social network. Do not rely on the default settings for the social network, which are generally very open and public.

4. Require attorneys to use disclaimers when publishing any content that is related to work performed by the law firm. Consider requiring the following generic example: "The postings on this site are my own and don't necessarily represent my law firm's positions, strategies, or opinions."

5. Request good judgment. Ask attorneys to be polite and avoid sensitive subjects.

6. Any use of a firm's insignia or logo should be run through the law firm's marketing department first.

7. Remind attorneys that copyright and financial disclosure laws apply equally to online conduct and offline conduct.

8. Firms should take steps to educate their attorneys on these guidelines. Whether through a video presentation or a quick, informal seminar, attorneys should be given an opportunity to learn of these guidelines and ask questions about the guidelines if necessary.

---

[275] Doug Cornelius, *Online Social Networking: Is It a Productivity Bust or Boon for Law Firms?*, LAW PRAC., Mar. 2009, at 28, 28, *available at* http://www.abanet.org/lpm/magazine/articles/v35/is2/pg28.shtml.

Do you see the common theme in the suggested guidelines? For the most part, these guidelines simply ask an attorney to follow the basic rules they learned in their legal ethics classes. The remaining rules are basic, common sense.

And, for heaven's sake, check with your insurance provider. Not all insurance providers cover blogs or social networking activity—and, of those who do, some require special insurance riders to do so.

CONCLUSION

The electronic world has certainly given us many challenges, with more undoubtedly to come. This new era seems to offer us both benefits and dangers simultaneously. Social networking appears to be here to stay, in one form or another. Thus, risk management in the context of social networking has become a major concern.

Instead of free-falling into this potential "hot-zone" with reckless abandon, deploy your "common sense parachute" which, in reality, would prevent most of the hiccups (or total disasters) that occur. Deploying this "parachute" is simple. Common sense requires neither that a person purchase special technology nor that states adopt new legislation. Rather, common sense simply requires a user to think through his or her actions and realize that there is no special shield protecting a person's online actions. Instead, online actions are analogous to offline actions. The ethical rules forbidding *ex parte* communications, talking to represented clients, and engaging in conduct detrimental to the implementation of justice apply equally in the paper and the online world.

The external forces that make social networking more dangerous than the paper world must be weighed against the benefits of using social networking—and we'll be struggling with that balancing act for some time to come. There is much, however, that you can do to protect yourself from the pitfalls of social networking, but the ultimate responsibility rests on you.

As Air Force cadets are wont to say, "Never jump with a parachute packed by someone else." Good advice for our times.