The Legal Implications of Social Networking

By Sharon Nelson, John Simek and Jason Foltin
© 2009 Sensei Enterprises, Inc.

The world has embraced social networking with a fervor rarely seen. Lawyers, though always slower 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 recent statistics.

In April of 2009, Facebook announced that it had over 200 million active users worldwide[1]. In the same month, Twitter, the new hotshot kid on the social networking block, reached 14 million users in the U.S.[2] Linked In claims 44 million members worldwide and Plaxo over 40 million.[3] MySpace, once the 800 pound gorilla of this new world, is now widely disparaged as a destination for teens and the Joe Six Pack crowd. Still, according to TechCrunch, it has an impressive 125 million users globally.[4]

We thought about defining all these networks, but it is increasingly rare to find anyone who isn't familiar with them. If any of the sites above are unfamiliar to you, just take a look at their Wikipedia entries.[5]

As part of the social networking phenomenon, texting and blogging are often included and we will include them here from time to time, as there is such interconnection between all these technologies.

This alluring new world has demonstrated many pitfalls. At first, very few people used the privacy settings that were available to them. They simply left them at the default settings – meaning that everything they posted was wide open to anyone. And let's face

---

[1] *See* Facebook Statistics, http://www.facebook.com/facebook?ref=pf#/press/info.php?statistics (last visited Aug. 15, 2009).

[2] Posting of Nick O'Neill to Social Times blog, http://www.socialtimes.com/2009/04/twitter-14-million/ (April 7th, 2009, 9:00 EST)

[3] *See* LinkIn, About Us, http://press.linkedin.com/about (last visited Aug, 15, 2009).

[4] Posting of Michael Arrington to TechCrunch blog, http://www.techcrunch.com/2009/01/22/facebook-now-nearly-twice-the-size-of-myspace-worldwide/ (Jan. 22, 2009).

[5] *See generally* Facebook, http://en.wikipedia.org/wiki/Facebook (last visited Aug. 21, 2009); LinkedIn, http://en.wikipedia.org/wiki/LinkedIn (last visited August 21, 2009); Plaxo, http://en.wikipedia.org/wiki/Plaxo (last visited August 21, 2009); MySpace, http://en.wikipedia.org/wiki/MySpace (last visited Aug. 21, 2009).

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. Then there are the terms of use, which even most lawyers do not read, and which give the sites enormous power over how your postings may be used. It's 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 folks 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.[6] The advertiser had merely lifted her attractive photo from a Facebook page.

Hackers have shown increasing interest in these sites as well, never a good omen for sites that once seemed fairly innocent. By using the powerful features that allow the downloading of content from third-party sites, the networks have left huge security holes for hackers to exploit.[7]

Because social networking is so new, the barrage of tales involving missteps have 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.

COURTS WRESTLE WITH SOCIAL NETWORKING

The new 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.[8] One wants to ask in exasperation, "What in the world was she thinking?" But this is the world we live in and we take our jurors as we find them.

---

[6] Posting of Cheryl Smith of CultureSmith consulting blog, http://www.culturesmithconsulting.com/husband-speaks-out-on-seeing-wife-in-facebook-dating-ad/ (Jul. 29, 2009).

[7] *See generally* Brian Krebs, Hackers' Latest Target: Social Networking Sites, The Washington Post, ¶ (Aug. 9, 2009), http://www.washingtonpost.com/wp-dyn/content/article/2008/08/08/AR2008080803671.html, (last visited Aug. 21, 2009).

[8] DailyMail.co.uk, Juror Dismissed after Asking Facebook Friends how to Vote on Trial, http://www.dailymail.co.uk/sciencetech/article-1089228/Juror-dismissed-asking-Facebook-friends-vote-trial.html (last visited Aug,16, 2009).

For example, one complaint in the post-verdict appeal of convicted Pennsylvania state senator Vincent Fumo was that a juror used Twitter, Facebook and blogs to post information about the trial during deliberations. The complaint was rejected in the court's ruling[9] on Fumo's post-trial motion.

> "The Twitter message at issue simply stated, "This is it . . . no looking back now!" (Govt.'s Resp. 141.) 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."[10]

With respect to his Facebook postings, the court found that they were in the nature of oblique 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.[11]

And though he had posted on his almost moribund blog that he was on jury duty, he offered no further information, nor did he receive any comments to the blog post.[12]

In conclusion, the Court found, "As the Court stated during the *in camera* hearing, despite violating the Court'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 Defendants."[13]

It is noteworthy in this case that the Court clearly finds that this juror violated the Court's orders. He "skates" and the decision holds only because his misconduct had no prejudicial impact. It is all too easy to imagine a case where there might be considerable prejudicial impact from this sort of misconduct.

---

[9] U.S. v. Fumo. No. CRIM.A. 06-319 (Jun. 17, 2009), *available at* http://www.paed.uscourts.gov/documents/opinions/09d0710p.pdf

[10] Id. at 117.

[11] Id. at 117-22.

[12] Id. at 123-27.

[13] Id. at 128-29.

Consider: 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 (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. Stoam Holdings and its owner Russell Wright were accused of running a Ponzi scheme.[14] During the trial, the juror's tweets (he tweeted during breaks) included one that said, "oh and nobody buy Stoam.[15] Its [sic] bad mojo and they'll probably cease to Exist, now that their wallet is 12m lighter."[16]

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, but not improper.[17] It is questionable whether other courts might have treated that offense so lightly.

Witness a recent case in which Miami-Dade Circuit Judge Scott Silverman dismissed a civil fraud lawsuit after he had declared a mistrial when a boss sent text messages to his employee on the witness stand during a bench conference.[18] After being alerted by a spectator, Silverman questioned both parties, who admitted the texting.[19] The judge had the offending text messages read aloud and made part of the record.[20]

Judge Silverman wrote, in his August 11th, 2009 order dismissing the case, 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 court's quiver of sanctions, drawn the bowstring taut and aimed the arrow at the heart of its own case. The court has justifiably released the string."[21] The judge also awarded attorney fees and costs to the defense.[22]

---

[14] Tresa Baldas, For Jurors in Michigan, No Tweeting (or Texting, or Googling) Allowed, LAW.com ¶ 9 (Jul. 1, 2009), http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202431952628&slreturn=1&hbxlogin=1 (last visited Aug, 16, 2009).

[15] Id.

[16] Id.

[17] Id.

[18] Deborah C. Espana, Judge Tosses Fraud Suit after Witness Is Texted by Boss during Trial, LAW.com ¶ 1 (Aug. 17, 2009), http://www.law.com/jsp/law/LawArticleFriendly.jsp?id=1202433074669 (last visited Aug. 17, 2009).

[19] Id. at ¶ 5.

[20] Id.

[21] Id. at ¶ 3.

[22] Id. at ¶ 4.

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 cellphones entirely. This is, to put it very mildly, not 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 hearing and trial dates rather then use their smartphones. It seems quite deliciously antiquated for an otherwise very modern court.

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 must check their devices in the lobby.[23]

Some states are bringing down the hammer, notably Michigan, which acted decisively in making a Supreme Court rule (effective September 1, 2009) banning the use of any handheld devices, such as iPhones and BlackBerrys, while in the jury box or during deliberations.[24]

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. Prosecutors have argued that, where 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, and 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?

There is a veritable smorgasbord of policies: New Jersey allows jurors to bring cell phones to court, but they must be turned off during trial.[25] In Malheur County, Oregon, and federal court in the Western District of Louisiana, jurors are not allowed to bring cell phones to court at all.[26] In Alaska's first judicial district, a court bailiff confiscates cell phones during jury deliberations.[27]

Some courts, like Ramsey County, Minnesota have issued a new policy prohibiting jurors from bringing any wireless communication device to court – in the case of Ramsey County, two mistrials were declared after jurors used cell phones during deliberation in violation of the court's order.[28]

---

[23] Katherine Helm, Courtrooms All Atwitter, National Law Journal, Aug. 2009, at 24.

[24] Id.

[25] Anita Ramasastry, Why Courts Need to Ban Jurors' Electronic Communications Devices, FindLaw.com ¶ 15 (Aug. 11, 2009), http://writ.news.findlaw.com/ramasastry/20090811.html (last visited Aug.16, 2009).

[26] Id.

[27] Id.

[28] Id.

In Multnomah County, Oregon, the court provides a jury instruction that makes explicit reference to certain electronic devices and activities.[29] The court tells jurors: "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."[30]

The instruction also cautions jurors about conducting Internet searches and does so in a very clear and commonsense manner: "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."[31]

Another instruction was issued on April 21, 2009 by an Arkansas judge, who said, "... during 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."[32] Similar instructions have reportedly been given to jurors by judges frustrated by the misuses of these new technologies.

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![33] We have clearly identified the problem, but we certainly have not standardized on a solution.

Reporters are also caught up in the fray. In March of 2009, U.S. District Judge Thomas J. Marten allowed a reporter to use Twitter to “tweet” about court proceedings in a trial of

---

[29] Id. at ¶ 16.

[30] Id.

[31] Id. at ¶ 17.

[32] Posting of Sharon Nelson on Ride the Lightning blog, http://ridethelightning.senseient.com/2009/05/web-20-jury-instructions-in-arkansas.html (May 8, 2009).

[33] Gregory S. Hurley, National Center for State Courts, Cell Phone Policies/Instructions for Jurors (May 1, 2009), http://www.ncsconline.org/WC/Publications/KIS_JurInnJurE05-01-09.pdf (last accessed Aug.16, 2009).

six Crips gang defendants in Kansas.[34] He felt it was opening the legal process to the public.

In July of 2009, a court order in Florida went in the opposite direction. The reporters were given a temporary press room while covering a criminal trial. They were permitted to bring in their "cellular phones, BlackBerries, iPhones, Palm Pilots, and other similar electronic devices as long as they agree in writing to not email, text message, twitter, type or otherwise use those devices inside any courtroom within this District."[35]

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."

LAWYERS AND JUDGES WHO HAVE FALLEN INTO THE TAR PIT

You might read the preceding section and think, "Gosh, what dumb people." However, it appears that lawyers and judges are no brighter. Consider some of the following examples.

Texas Judge Susan Criss recalled a lawyer who asked for a continuance because of the death of her father. The lawyer had earlier posted a string of status updates on Facebook, detailing her week of drinking, going out and partying.[36] Strangely, her story in court didn't match her Facebook posts. You might have guessed the result – no continuance.

Then there was the lawyer who complained about having to handle a motion in Criss's court. Criss good-naturedly threw her a barb, also on Facebook.

Judge Criss has seen lawyers on the verge of crossing, if not entirely crossing, ethical lines when they complain about clients and opposing counsel. She had to admonish one family member who jeopardized her own tort case by bragging online about how much money she would get from a lawsuit.[37]

Here's 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 the Gap) on a clothing rack and a lawsuit was filed in federal court based on diversity jurisdiction.[38]

---

[34] Posting of Larry Magid on LarrysWorld.com blog, http://www.pcanswer.com/2009/03/09/twitter-in-the-court-federal-judge-gets-it/ (Mar. 9, 2009).

[35] United States v. UBS AG, 2009 U.S. Dist. LEXIS 67270, at 3-4 (S.D. Fla. Jul. 9, 2009).

[36] Molly McDonough, Facebooking Judge Catches Lawyer in Lie, Sees Ethical Breaches, ABAJournal ¶ 5 (Jul. 31, 2009), http://www.abajournal.com/news/facebooking_judge_catches_lawyers_in_lies_crossing_ethical_lines_abachicago (last visited Aug. 20, 2009).

[37] Id. at ¶ 7.

[38] *See generally* Wei Ngai v. Old Navy, 2009 U.S. Dist. LEXIS 67117 (D.N.J. Jul. 31, 2009).

The Plaintiffs deposed the Gap's General Liability Claims Manager via video deposition on the chain of custody of the clothing rack.[39] The witness was in Sacramento, California, Defense attorneys were in Fort Lee, New Jersey and the Pro Hac Vice attorney was in Southfield, Michigan. The deponent and the Pro Hac Vice attorney were only visible from the chest up and their hands were not visible.

Can you see where this is going? Before the deposition, the two sent 11 text messages between themselves.[40] During the one hour and twelve minute deposition, the attorney and client exchanged 5 more text messages.[41]

Then came one of those moments that make the virtuous smile. The Pro Hac Vice attorney inexplicably sent a text to the PLAINTIFF's attorney saying, "[you] [are] doing fine," thus hoisting himself on his own petard.[42]

Suspecting (do you think?) that something fishy was afoot, the Plaintiff's attorney requested that the defending attorney preserve his text messages from the deposition. 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.[43] The court did indeed find that the text messages made before the deposition were privileged as they were typical of the words of encouragement that any lawyer might give in person.[44] However, the text messages found to be sent during the course of the deposition were not privileged.[45]

The Court stated that the Pro Hac Vice attorney violated Federal Rule of Civil Procedure Rule 30 by texting during the deposition.[46] 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."[47]

If it had not been for the Pro Hac Vice attorney sending a text to the Plaintiff's attorney, no one would have known of this impermissible (and ethically questionable for arguably

---

[39] Id. at 1.

[40] Id. at 3-4.

[41] Id. at 3.

[42] Id.

[43] Id. at 7.

[44] Id. at 10-11.

[45] Id. at 11-12.

[46] Id. at 14-15.

[47] Id. at 15.

witness coaching) conduct. It will be a sad day for our system if deposing attorneys need to include a "no texting" provision to deposition admonitions.

A California lawyer (non-practicing) was suspended for blogging about a trial while serving as a juror.[48] Though warned by a judge not to discuss the case, orally or in writing, he apparently knew better, as egotistical individuals always seem to. "Nowhere do I recall the jury instructions mandating I can't post comments in my blog about the trial."[49] He then proceeded to describe the judge and the defendant in a highly unflattering way. Because of his misconduct, the appellate court reversed the felony burglary conviction.[50] The disciplinary authorities in the California Bar were not amused and his law license was suspended for 45 days.[51]

Let us not assume the judiciary is immune to the temptations of the technological world. Following a formal investigation by the North Carolina Judicial Standards Commission, District Court Judge B. Carlton Terry Jr. was issued a public reprimand for using Facebook to discuss a case being tried before him.[52]

According to the public reprimand, which was issued April 1, 2009, Terry presided over a child custody and child support hearing from Sept. 9 to Sept. 12, 2008, in Iredell County.[53] During this time, Terry and the attorney for the defendant became "friends" on Facebook and began posting messages discussing the case, such as when it would be settled and whether or not one of the parties had engaged in an affair.[54]

Terry also used Google to conduct independent research on the plaintiff's business Web site even though it had never been offered or entered into evidence during the hearing.[55] Terry never disclosed to the counsel or the parties that he had visited a Web site

---

[48] Martha Neil, Calif. Lawyer Suspended Over Trial Blogging While Serving as Juror, ABAJournal.com, ¶ 1 (Aug. 4, 2009) http://www.abajournal.com/news/calif._lawyer_suspended_over_trial_blog_while_serving_as_juror (last visited Aug. 20, 20090).

[49] Id. at ¶ 3

[50] Id at ¶ 2.

[51] Id. at ¶ 1.

[52] Ryan Jones, Judge Reprimanded for Discussing Case on Facebook, The-Dispatch.com ¶ 1 (Jun. 1, 2009), http://www.the-dispatch.com/article/20090601/ARTICLES/905319995/1005?Title=Judge-reprimanded-for-discussing-case-on-Facebook (last visited Aug. 20, 2009).

[53] Id. at ¶ 2.

[54] Id.

[55] Id. at ¶ 3.

belonging to the plaintiff. Terry disqualified himself from the case Oct. 14, 2008, and his order was vacated.[56]

The Judicial Standards Commission found that "Judge Terry's actions constitute conduct prejudicial to the administration of justice that brings the judicial office into disrepute."[57] Terry agreed that he would refrain from repeating such actions in the future, familiarize himself with the Code of Judicial Conduct and refrain from retaliating against any person who cooperated with the commission in the matter.[58]

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. What can they accomplish on these social networks that has such appeal?

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

2. They will gather followers if they provide consistently valuable content.

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

4. They may attract reporters, who are known to use and quote blogs on a regular basis these days.

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

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

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

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

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 god nuggets of evidence.

SOCIAL NETWORKING AS EVIDENCE

---

[56] Id. at ¶ 6.

[57] Id. at ¶ 7.

[58] Id. at ¶ 8.

The legal world took notice when, on February 20, 2009, the Ontario Superior Court of Justice issued an order permitting a defendant to cross-examine a plaintiff in a motor vehicle accident suit regarding the content on his private Facebook profile.[59] The Court noted, "It is reasonable to infer that his social networking site contains some content relevant to the issue of how Mr. Leduc has been able to lead his life since the accident."[60]

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.[61] Whoops.

In another case, an attorney helped secure shared custody for a father after discovering that his wife had posted sexually explicit comments on her boyfriend's MySpace page.[62] And in yet another instance, a husband's credibility came into question when it was revealed that his MySpace page said he was "single and looking."[63]

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 got into a crash resulting in the death of her passenger.[64] 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 with plastic shot glasses on it.[65] Other photos showed her holding a beer bottle and wearing a shirt advertising tequila. 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.[66]

In 2008, two weeks after Joshua Lipton had been charged with drunk driving in an accident that seriously injured a woman, he made the foolish decision to show up at a Halloween party in a prisoner costume with the label "Jail Bird" on his orange jumpsuit.

---

[59] Tariq Remtulla, Canada: Facebook Not So Private? Ontario Court Finds Facebook Profile Discoverable, Mondaq.com ¶ 1 (Mar. 2009), http://www.mondaq.com/article.asp?articleid=76332 (last visited Aug. 20, 2009).

[60] Id.

[61] *See* Shannon Kari, Facebook Postings Not Serious: Defence, FinanciaPost.com, (Feb. 12, 2008), http://www.financialpost.com/news-sectors/technology/story.html?id=302023 (last accessed Aug. 20, 2009).

[62] Vensa Jaksic, Finding Treasures for Cases on Facebook, LAW.com ¶ 3 (Oct.15, 2007), http://www.law.com/jsp/legaltechnology/pubArticleLT.jsp?id=1192179809126 (last accessed Aug. 20, 2009).

[63] Id,

[64] Id at ¶ 23-6.

[65] CBSNews.com, Drinking, Driving and Facebook Don't Mix ¶ 14 (Jul. 18, 2008), http://www.cbsnews.com/stories/2008/07/18/tech/main4272846.shtml (last visited Aug. 20, 2009).

[66] Id. at ¶ 15-17.

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.[67] The judge called the photos "depraved" and sentenced him to two years in prison.[68]

In a sentencing hearing, Matthew Cordova found himself with a five year prison sentence in Arizona.[69] He had pled guilty to aggravated assault with a gun – at the hearing, his attorney tried to portray him as a peaceful man who had found religion, but the prosecution had a MySpace picture of Cordova holding a gun and posting comments about it.[70]

In 2009, Raul Cortez was found guilty of murder, but his attorney thinks he might not have been sent to death row without the gang signs and colors displayed on his MySpace page being introduced in court.[71]

The police routinely monitor the social networking sites of gang members who regularly discuss their activities on their social networking sites. Happily, they are often dumb enough to provide great fodder for criminal investigations.

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 the social networking sites of all the parties. In one such case in which the authors were involved, a well groomed woman who portrayed herself as a "soccer man" was undone by explicit photos of herself that she had posted online looking to "hook up" with men. Dad got custody.

In another case the authors handled, a wife learned of her husband's infidelity because he talked to his lover on his Facebook page – the wife had no access to the page, but one of her friends did.

It is now 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.

HOW DO LAWYERS MANAGE TO GET THEMSELVES TAKEN TO THE WOODSHED?

---

[67] Id. at ¶ 1.

[68] Id at ¶ 3.

[69] Erica Perez, Getting Booked by Facebook, redOrbit.com ¶ 15-16 (Oct. 3, 2007), http://www.redorbit.com/news/technology/1087625/getting_booked_by_facebook/index.html (last accessed Aug. 20, 2009)

[70] Id.

[71] Jay Gormley, MySpace and Facebook Becoming Evidence in Court, CBS11tv.com ¶ 3 (Feb. 3, 2009), http://cbs11tv.com/local/MySpace.Facebook.Evidence.2.926231.html (last accessed Aug. 20, 2009)

Apart from some of the courtroom and litigation antics referenced earlier:

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

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

3. They drink a glass or 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.

5. They fail to realize that they may be divulging client confidences – even though only your "friends" may have access to your Facebook page, they may shoot off your 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 50 year old lawyer who has a child who is her friend on Facebook and chooses to post 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 don't proofread and they look like idiots, 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 cannot inveigle a third party into "friending" someone on Facebook in order to gain access to an opposing party's Facebook page.

SOCIAL NETWORKING: AN E-DISCOVERY AND RECORDS MANAGEMENT NIGHTMARE

Even if you haven't caught the Twitter bug yourself, you can be assured that some within your law firm have indeed gotten the bug. And what are they saying, when sending their "tweets" via Twitter? Stupid stuff like "walking the dog" and "when did I get so darn fat?" But they are also saying "the Smith, Smith and Smith law firm is EVIL" and

naming names. And "we're working on a case that's going to put Acme Corporation in a stock market tailspin."

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

Is a tweet done on firm resources a "record" for purposes of retention requirements and, ESI preservation/production? It probably depends. If it is a company tweet, probably yes. A personal tweet, probably no. Probably. Much of this remains unsettled ground.
If you find that scary, you're not alone. For a while, record managers thought they had the universe pretty well covered with e-mail and company approved programs. After a while, some of them caught up with instant messages. But Twitter, blogs and social networks have given almost everyone a Goliath-size headache. Whether you are thinking in terms of your own law firm or your clients, you must now consider these new technologies.

They bedevil records management (RM) in particular. The minute RM catches up to technology, technology leapfrogs ahead with something else to cause consternation. Douglas Winter, who heads the electronic discovery unit at Bryan Cave, stresses that tweets are no different from letters, e-mail or text messages – they can be damaging and discoverable, which is especially problematic for companies that are required to preserve electronic records, such as the securities industry and federal contractors.[72] Yet another compliance headache is born.

Tom Mighell of the electronic discovery company Fios suggests that we may find a post from a proud employee that says "Our brakes are fine. I'm an engineer on that product. We went to 5X tolerance, so you can be rougher on them than you think. Don't worry." As Tom points out, after that post, "you've got potential product liability in 140 characters."[73]

Twitter is by no means alone. There is also Yammer, and present.ly (no that's not a typo) – and surely many more to come. Enterprise versions are just beginning to emerge, but there is currently precious little policy to govern them. For the most part, microblogs like Twitter are being treated as blogs from a corporate policy perspective.

Blogs

---

[72] Tresa Baldas, Beware: Your 'tweet' on Twitter could be Trouble, The National Law Journal ¶ 7 (Dec.22, 2008), http://www.law.com/jsp/nlj/PubArticleNLJ.jsp?id=1202426916023 (last accessed Aug.18, 2009)

[73]Posting of Carolyn Elefant on LAW.com Legal Blog Watch blog, http://legalblogwatch.typepad.com/legal_blog_watch/2008/11/organizations-u.html (Nov. 6, 2008 14:35 EST).

As blogs have exploded in popularity over the last few years, so have cases in which employees have disclosed trade secrets and insider trading information on their blogs. Blogs have also led to wrongful termination and harassment suits.

There should, of course, be a company policy about blogging at work or about work. Many companies sanction blogs – Microsoft has hundreds of them. 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.[74]

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

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

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

One wag has suggested a very simple corporate blog policy: "Don't be stupid."[75]

Social Networks

The lifeblood of many employees is their social networks, including MySpace, Facebook, LinkedIn and Plaxo. Besides being a gigantic timewaster, these sites abound with risks for business as most businesses do not monitor their employees' sites and therefore all the risks associated with blogs apply here. Many experts believe that companies are well advised to use filters to block access to all social networking sites at work. At the very least, this action will keep the posts from being company records. In fact, a survey released in August of 2009 shows that 76% of companies are indeed blocking access to social networking sites, an astonishingly high percentage.[76] They report seeing them as both a security risk and a productivity drain. On the other hand, genuine business usage of these sites has grown tremendously and it may be very difficult to allow business

---

[74]*See generally* Nickolas v. Fletcher, 2007 U.S. Dist. LEXIS 23843 (E.D. Ky. Mar. 30, 2007).

[75]*See* posting of Jeremy Zawodny on Jeremy Zawodny blog, http://jeremy.zawodny.com/blog/archives/004725.html (May 31, 2005 22:35 EST).

[76] Chuck Miller, Survey: Social Networks Increasingly Blocked, SC Magazine ¶ 2 (Aug. 19, 2009), http://www.scmagazineus.com/Survey-Social-networks-increasingly-blocked/article/146833/ (last visited on Aug. 20, 2009).

usage and forbid personal usage, no matter what a company's policy may say.

A 2008 independent survey commissioned by FaceTime Communications[77] (based in the U.K. but we have no reason to suspect the answers would be much different here) found that roughly 80 percent of employees use social networks at work – and for BOTH personal and business reasons. The work-related purposes were for professional networking, researching and learning about colleagues.

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

Is employer monitoring of social networking sites really happening in the wild? The authors did an ad hoc online survey – though everyone said an employer had a right to monitor, no one actually knew of an employer who WAS monitoring personal sites.

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. You'll save a fortune if you become embroiled in litigation. Shrinking the data to search will shrink the volume of potentially responsive data that must be reviewed.

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

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, gulp, legal liability. Management of Web 2.0 records is limited at best, often chaotic and duplicative. 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 offense, denigrating these grumbling competitors in off-site blog posts and wiki entries, tagging negative stories on the Web, posting slated 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

[77] FaceTime, Executive Summary 2008, (Oct. 2008), http://www.facetime.com/survey08/summary/ (last visited on Aug. 19, 2009).

innocence and tries to limit the scope of discovery, but is compelled by law to agree to hand over all relevant ESI."

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

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 fully filled-out Facebook profile can contain a virtual treasure trove of personal information including an individual's name, birthday, political and religious views, online and offline contact information, gender, sexual preference, and relationship status, favorite books, movies, and so on, educational and employment history, and, of course, pictures.[78] As the list of features and applications available to those frequenting social networking sites has grown, so too has the depth of information about both who you are and who you know.[79]

Consider for example the all too familiar case of a job applicant losing his or her employment offer after the employer finds out that one of their listed interests on Facebook includes "bonging beers" or "smoking blunts."[80]

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 racy photographs obtained from a private photo album to blackmail Miss New Jersey 2007.[81] The thought that anyone can dig up personal photographs and disclose them to the world at large is enough to send shivers down anyone's back.

Making matters worse, unbeknownst to the average citizen, courts have been unwilling to recognize a reasonable expectation of privacy in materials people willingly post on the

---

[78] James Grimmelmann, *Saving Facebook*, 94 Iowa L. Rev. 1137, 1149 (2009).

[79] 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).

[80] See Id. at 1665 (citing Alan Finder, When a Risque Online Persona Undermines a Change for a Job, N.Y. Times, June 11, 2006, §1, at 1).

[81] Id. (citing Austin Fenner, N.J. Miss in a Fix over Her Pics, N.Y. Post, July 5, 2007, at 5, http://www.nypost.com/seven/07062007/news/regionalnews/n_j_miss_in_a_fix_over_her_pics_regional_austin_fenner_with_post_wire_services.htm.

Internet without taking any measures to restrict access to them, or otherwise protect them.[82]

One such cautionary tale is the case of Cynthia Moreno.[83] 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.[84] Ms. Moreno then brought suit alleging, among other things, that the newspaper violated her privacy by publishing her online remarks.[85] 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 anyone with a computer and thus, opened it to the public eye.[86] As such, the court stated it had no choice but to 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.[87]

Similarly, in *Commonwealth v. Protetto*,[88] the court held that no expectation of privacy existed with regard to sexually explicit e-mails messages sent by a man to a fifteen-year-old girl or an electronic chat room conversation between them.[89] 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.[90]

Finally, in perhaps the best illustration of the risks associated with posting information about one's self on a social network, the court in *Cedrick D. v. Stacy W.* terminated a

---

[82] *See supra* text and accompanying notes 64-75.

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

[84] Id. at 861. Local reaction to the publication was alleged to include numerous death threats and a gunshot 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.

[85] Id.

[86] Id. at 862.

[87] 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.

[88] 771 A.2d 823 (Pa. Super. 2001).

[89] Id. at 830.

[90] Id. The court analogized sending an e-mail or chat-room communication to leaving a message on an answering machine. Id. 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. Id. So too, 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.

father's parental rights after viewing his MySpace profile.[91] 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 the best interests of a child.[92] As cases like this illustrate, content on an individual's social networking profile may now play a pivotal role in establishing criminal or civil liability in court proceedings.[93] More importantly, this case stands for the proposition that a user can and will be held accountable for their statements on social networking sites, sometimes with life-altering consequences.[94]

Several different policy interventions have been proposed to "fix" the social networks' privacy problem.[95] Some individuals say that perhaps the best policy is to do nothing and allow market forces to establish the optimal level of privacy protection.[96] Others have argued for better technical controls or establishing user restrictions.[97] Still others have suggested a strengthened public-disclosure tort and a right to opt out.[98]

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). 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, but rather, be mindful that the information they provide will be subject to strict scrutiny by potential employers, the legal system, and their peers. As of August, 2009, 45% of employers are reported to use social networking sites to research their job candidates.[99] 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.

---

[91] Hillel I. Parness, Toward "Social Networking Law"?, 1 No. 4 Landslide 13, 16 (2009).

[92] Id.

[93]Id.

[94]Id.

[95] *See generally* James Grimmelmann, *Saving Facebook*, 94 Iowa L. Rev. 1137, 1178-1206 (2009).

[96] Id. at 1178-79.

[97] Id. at 1179.

[98] Id. at 1196-1201.

[99] *See* Yahoo!, Forty-five Percent of Employers Use Social Networking Sites to Research Job Candidates, CareerBuilder Survey Finds, (Aug. 19, 2009), http://finance.yahoo.com/news/Fortyfive-Percent-of-prnews-3546498479.html?x=0&.v=1 (last visited Aug, 20, 2009).

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 too have begun to tap into social networks and turn these sites into their own twisted little playgrounds.[100] In fact, investigators have found that activities such as posting pornographic images or videos and soliciting minors are ubiquitous on both MySpace and Facebook despite terms of service for both that explicitly prohibit such conduct.[101]

And while Facebook and MySpace have set minimum age restrictions for users at thirteen, an overwhelming number of social network users are, and will continue to be, minors.[102] 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 to prevent sexual predators from turning these sites into hunting grounds; however, these attempts have largely been unsuccessful and have instead given rise to many well-established legal defenses.[103] Most notably, social networks have put up legal roadblocks by arguing 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.[104] These roadblocks have largely been successful in shielding Web sites from liability for the criminal and tortious acts of their users, thereby preventing injured parties from seeking recourse from anyone save the offending party.

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, brought in June of 2006, MySpace was sued by a mother and her fourteen-year-old daughter, Julie, because the girl had been sexually assaulted by a man whom she first met on MySpace.[105] The complaint alleged that the social network

---

[100] Note, Sander J.C. van der Heide, Social Networking and Sexual Predators: The Case for Self-Regulation, 31 Hastings Comm. & Ent. L.J. 173, 177 (Fall 2008).

[101] Joesph Spector, Cuomo Launches Sex Predator Probe of Facebook, The Journal News (Westchester County, New York), Sept. 25, 2007, at 1B.

[102] MySpace Terms & Conditions, supra note 1; Facebook Terms of Use, supra note 4.

[103] Michael D. Marin, & Chirstopher V. Popov, Doe v. MySpace: Liability for Third Party Content on Social Networking Sites, 25 Comm. Law. 3, 3 (Spring 2007).

[104] *See supra* text and accompanying notes 110-124.

[105] Doe v. Myspace, Inc., 528 F.3d 413, 416 (C.A.5, 2008).

provider had been grossly negligent, or at the very least negligent, in failing to prevent sexual predators from communicating with minors on its website.[106]

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.[107] The court rejected Plaintiffs' disingenuous attempts to circumvent the CDA immunity by arguing that their claims were not against MySpace as a publisher, but rather for failing to implement any safety measures.[108] 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.[109]

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.[110] And while exceptions to the general rule exist, none of the special relationship exceptions have been found to apply in the case of online social networking.[111] 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.[112]

Notwithstanding this attenuated relationship, Plaintiffs attempted to apply a novel theory of premises liability to argue that MySpace had a duty to protect its users from sexual predators.[113] The court rejected the argument stating that not only was there no legal basis for Plaintiffs' theory, but also that "to 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."[114]

---

[106] Id.

[107] Id. at 416-17. In its pertinent part, the act 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." 42 U.S.C. § 230 (c)(1). 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." 42 U.S.C. § 230 (e)(3).

[108] Id. at 419.

[109] Id. at 420.

[110] Doe v. MySpace, Inc., 474 F. Supp. 2d 843 (W.D. Tex. 2007).

[111] Michael D. Marin, & Chirstopher V. Popov, Doe v. MySpace: Liability for Third Party Content on Social Networking Sites, 25 Comm. Law. 3, 3 (Spring 2007).

[112] Id. at 5.

[113] Doe, 474 F. Supp. at 851.

[114] Id.

Likewise, in another recent case, *Doe v. Sexsearch.com*,[115] Plaintiff sued the website provider after he was introduced and had sex with an underage partner, Jane Roe, resulting in criminal proceedings against him.[116] Plaintiff employed a "double barreled shotgun approach" in this case, alleging a plethora of claims, all of which essentially boiled down to either (1) Defendant failed to discover that Jane Roe lied about her age, or (2) the contract terms were unconscionable.[117] 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 Defendants were immune from liability pursuant to section 230 of the CDA.[118] The remaining claims were either barred by the Ohio state law or because the contract itself was generally not unconscionable.[119]

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. However, increasingly negative media scrutiny has caught the nation's attention and appears to be forcing social networking sites into action. This negative national attention pulls at the heart of these social network providers – money. If parents prevent their minor children from using the Web sites in fear that they may become prey, it means less traffic going through them, which in turn drives down financial profits.

And if that doesn't work, Louisiana has recently issued a warning about how far states may be willing to go to prevent online predators from using social networking.[120] The legislation bans all registered sex offenders from using social networking sites as part of their parole.[121] You can see how this has caught the attention of social networks – if banning sex offenders doesn't work, perhaps the next step is to force these sites to increase and enforce their respective minimum age requirements.

---

[115] 502 F. Supp. 2d 719 (N.D. Ohio 2007)

[116] Id. at 721.

[117] Id. at 724. In total, Plaintiff brought forth fourteen claims against Defendant which were as followed: (1) breach of contract; (2) fraud; (3) negligent infliction of emotional distress; (4) negligent misrepresentation; (5) breach of warranty; (6) deceptive trade practices; (7) unfair and deceptive trade practices; (8), (9), (10), (11), (12), (13) unconscionability of contract; and (14) failure to warn. Id.

[118] Id. at 727-28.

[119] Id. at 728.

[120] 720 Ill. Comp. Stat. 5 (2009), *available at* http://www.ilga.gov/legislation/96/HB/09600HB1314enr.htm.

[121] Id.

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 "blow up" in the faces of both users and potentially social network providers.

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 Millenium Copyright Act (DMCA) so long as the provider complied with the "notice and take-down" provisions of the statute.[122] However, recent lawsuits brought by copyright owners against YouTube and Google for allegedly infringing on their copyrights may force changes in the legal landscape of copyright law as it pertains to Internet providers and specifically, social networking sites.[123]

First, a brief history lesson. In 1998, Congress attempted to bring U.S. copyright law into the twenty-first century by ratifying the Digital Millennium Copyright Act (DMCA), which created a series of "safe harbors" for certain activities of qualifying Internet service providers.[124] Section 512 of this Act sets forth the criteria an Internet service provider must meet in order to be afforded the protection under the DMCA's safe harbor.[125] The Act requires that the Internet providers have no knowledge that infringing material exists on its sites or be aware of any factual evidence tending to make infringing content apparent and, once aware, the site must promptly remove the infringing content.[126] Additionally, an Internet Service Provider can receive no pecuniary gains "attributable to the infringing activity."[127] Finally, upon notice by the copyright owner of purportedly infringing content, the Internet Service Provider must remove the material.[128] As a threshold matter, section 512(i) of the DMCA requires an Internet service provider to have adopted a policy informing subscribers of the provider's right to terminate the access of repeat offenders in appropriate circumstances.[129]

Several cases have highlighted a straightforward application of section 512(c) and the safe harbor provisions as applied to Internet service providers. Many of these cases have

---

[122] *See* 17 U.S.C. § 512 (2000).

[123] *See supra* text accompanying notes (INSERT)

[124] Note, Lauren Brittain Patten, From Safe Harbor to Choppy Waters: YouTube, The Digital Milennium Copyright Act, and a Much Needed Change of Course, 10, Van. J. Ent. & Tech. L. 179, 188 (Fall 2007).

[125] *See* 17 U.S.C. § 512(c)(1)).

[126] Id.

[127] Id.

[128] Id. § 512 (c)(1)(B).

[129] Id. § 512(i).

focused on the burden of the plaintiffs to notify the defendants of the infringing content. In one such case, brought in 2001, a California district court 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 alleged misconduct.[130] Finding that the Web site was afforded protection under the auspices of the safe harbor provisions of DMCA, the court granted eBay's request for summary judgment.[131]

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.[132] In its complaint, Viacom alleges that YouTube's popularity is built on the website's vast availability of infringing works. Further, Viacom contends that YouTube uses this library of works to increase the amount of traffic drawn to its Web site.[133] Likewise, a second complaint, filed in May of 2007 by the Football Association Premier League, Ltd., accused YouTube of engaging in copyright infringement for pecuniary gain.[134] Plaintiffs argue that YouTube's feeble notice and take down mechanism is nothing more than a meaningless attempt to satisfy the requirements of the DMCA.[135] In fact, Plaintiffs complain that not only is it nearly impossible to find all infringing material, but it is also an exercise of futility; YouTube users simply repost the content under a different file or user name.[136]

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.[137] Under this scenario, YouTube would lose any protection provided through the DMCA's safe harbor provisions and effectively open the company up to legal liability for copyright infringement. Others have argued that these lawsuits against YouTube illustrate the fundamental problems with the DMCA and urge concrete changes through the judicial or

---

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

[131] Id. at 1094.

[132] *See* Viacom International, Inc., v. YouTube, Inc., Complaint for Declaratory and Injunctive Relief and Damages, Mar. 13, 2007 (filed S.D.N.Y. 2007).

[133] Id.

[134] *See* The Football Ass'n Premier League Ltd. v. YouTube, Inc., Complaint, May 4, 2007 (filed S.D.N.Y. 2007).

[135] Id.

[136] Id.

[137] Kevin Fayle, Understanding the Legal Issues for Social Networking Sites and Their Users, FindLaw.com, (2007), http://technology.findlaw.com/articles/00006/010966.html (last visited Aug. 20, 2009).

legislative systems.[138] In either case, the outcomes of these cases could reshape the legal obligations of social networking sites, the services they provide, and the business models used.

More certain though is the fact 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.

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. 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.[139] 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.[140]

For instance, in *Zeran v. American Online, Inc.*,[141] the victim of an online prank sued AOL for its failure to remove the ad and post a retraction.[142] The messages described the purported sale of shirts featuring offensive and tasteless slogans related to the 1995 bombing of an Oklahoma City federal building and instructed interested buyers to call "Ken" at Plaintiff's home phone number.[143] Shortly thereafter, Plaintiff received a flood of calls, comprised mainly of angry and derogatory messages, but also including several death threats.[144]

---

[138] Note, Lauren Brittain Patten, From Safe Harbor to Choppy Waters: YouTube, The Digital Milennium Copyright Act, and a Much Needed Change of Course, 10, Van. J. Ent. & Tech. L. 179, 209 (Fall 2007).

[139] *See supra* text and accompanying notes 122-130.

[140] *See generally* Zeran v. American Online, Inc., 129 F.3d 327 (4th Cir. 1997); Dimeo, III, v. Max, 929 F.Supp. 824 (E.D. Pa. 1996).

[141] 129 F.3d 327(E.D. Pa. 1996).

[142] Id. at 329.

[143] Id.

[144] Id.

In filing suit, 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.[145]

The Fourth circuit disagreed and upheld the lower court's decision that the CDA barred Plaintiff's claims.[146] The court explained that even if notice was given, the CDA immunizes interactive computer service providers from liability stemming from defamatory or threatening posts.[147] Likewise, in cases following *Zeran,* courts have held that Web sites and other interactive computer services cannot be held liable for publishing defamatory statements created by a third party.[148]

Conversely, because social networking users aren't 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. Even if the website has been immunized under section 230 of the CDA, a user will likely be liable if found to have posted defamatory content unless he or she can effectively invoke either First Amendment or state-constitutional free speech rights.[149]

Many of the most prominent cases on this issue 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*,[150] in which one student learned the potential ramifications of posting defamatory content the hard way. Here, the student had created a personal profile on the website MySpace.com depicting the principal of Blue Mountain Middle School as a pedophile and a sex addict.[151] The school determined that the Plaintiff student had violated several provisions of its disciplinary code and as a result, levied a ten-day out-of-school suspension against her.[152] The parents of the student brought suit and argued that the punishment violated the Constitution of the

---

[145] Id.

[146] Id. at 334.

[147] Id. at 334. 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.* at 333.

[148] Michael D. Marin, & Chirstopher V. Popov, *Doe v. MySpace: Liability for Third Party Content on Social Networking Sites*, 25 Comm. Law. 3, 3 (Spring 2007).

[149] Id.

[150] 2008 U.S. Dist. LEXIS 72685 (M.D. Pa. Sept. 11, 2008).

[151] Id. at 1. The profile described its subject'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, fucking in my office, hitting on students and their parents." Id.

[152] Id. at 2.

United States and their rights as parents.[153] The court disagreed and held that because the vulgar, lewd, and potentially illegal speech had an effect on the campus, the school did not violate the Plaintiff's Constitutional rights by punishing her for an imposter profile.[154]

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

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.[155] As traditional journalists have been afforded both First Amendment and a state statutory privilege, the question of whether bloggers should enjoy the same immunities has been pushed to the legal vanguard.[156] This question has sparked numerous debates and has been a catching point in federal legislation. And while courts have yet to definitively fall on one side or another of this issue, a May 2006 ruling by a California state appeals court seems to suggest that perhaps online bloggers have the same rights as their more traditional offline counterparts.

In *O'Grady v. Superior Court*,[157] Apple issued subpoenas to the publishers of three websites seeking the identities of individuals who leaked information regarding new Apple products. 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.[158] The California state appeals court subsequently reversed this decision, holding that online journalists have the same right to protect the confidentiality of their sources as offline reporters do.[159]

---

[153] Id. at 3.

[154] Id.

[155] Cydney Tune and Marley Degnar, Blogging and Social Networking: Current Legal Issues, 929 PLI/Pat 73, 87 (March-April 2008).

[156] Id. at 88.

[157] 139 Cal. App. 4th 1423 (Cal. App. 6th Dist. 2006).

[158] Id. at 1431-32

[159] Id. at 1480.

Many proponents advocating bloggers' rights have hailed this decision as the inception of bloggers being afforded the same rights as journalists. Others have been less optimistic and have argued that the issue really boils down to whether a blogger acts like a traditional journalist or not. 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.

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. The ease and frequency which these virtual crooks have been able to gain access to private information is a serious cause for concern.

There is a literal 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.[160] For instance, a recent article in the *Hacker Quarterly* explained that many popular Facebook applications are vulnerable to simple attacks which allow the thief to view any personal information sent to the application itself.[161]

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.[162] And these documents didn't just provide an individual's birthday or personal interests. No, some of these documents included credit card numbers, Paypal accounts, and even security codes for the office buildings of companies such as AOL, Dell, Ericsson and Nokia.[163]

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

LAW FIRM SOCIAL NETWORKING POLICIES

---

[160] Chris Soghoian, Hackers Target Facebook Apps, CNET ¶ 1, (Mar. 1, 2008), http://news.cnet.com/8301-13739_3-9904331-46.html (last visited Aug. 20, 2009).

[161] Id. at ¶ 5.

[162] Andrew Lyle, Twitter Hacked, Personal Documents Leaked, Neowin.net ¶ 1 (Jul. 17, 2009), http://www.neowin.net/news/main/09/07/17/twitter-hacked-personal-documents-leak (last visited Aug. 20, 2009).

[163] Id.

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 45% of law firms have gone so far as to block access to some of the most popular sites.[164] Some have placed special restrictions on certain sites, while still others have done nothing thus far. And, if you haven't 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.

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

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

4. Disclaimer. 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. Use of firm insignia or logo should be run through the marketing department first.

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

8. Education. 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 if necessary.

Do you see the common theme? 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 basically common sense.

---

[164]Doug Cornelius, Legal Web 2.0 - Online Social Networking: Is It a Productivity Bust or Boon for Law Firms?, ABA ¶ 4 (Mar. 2009), http://www.abanet.org/lpm/magazine/articles/v35/is2/pg28.shtml, (last visited Aug. 20, 2009).

And for heaven's sake, check with your insurance provider. Not all of them cover blogs or social networking activity – and some require special 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 would appear to be here to stay, in one form or another, and so risk management has become a major concern.

Instead of free-falling into this "hot-zone" with reckless abandon, deploy your common sense parachute which, in reality, would prevent about 95% of the hiccups (or total disasters) that occur. And it's simple. Common sense doesn't require a person to purchase special technology or states to adopt new legislation; it simply requires a user to think through his or her actions and realize that there is not 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 weighing process for some time to come. There is much 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.

Authors Sharon Nelson and John Simek are the President and Vice President of Sensei Enterprises, a computer forensics and information technology company in Fairfax, Virginia. Author Jason Foltin is a paralegal with Sensei Enterprises.