ALFA INTERNATIONAL
2015 INSURANCE LAW SEMINAR
June 10-12, 2015 – The Ritz-Carlton Battery Park –
New York, New York

LOOSE LIPS SINK SHIPS – EFFECTIVE USE OF
SOCIAL MEDIA

Kelly A. Hedberg
Moderator
RENAUD COOK DRURY MESAROS
Phoenix, Arizona
khedberg@rcdmlaw.com

Nicole Nowlin
Partner
COSGRAVE VERGEER KESTER LLP
Portland, Oregon
nnowlin@cosgravelaw.com
Using Social Media in Your Claims Investigations

You’ve Got A “Friend”

By Wayne Partenheimer
February 02, 2011

A photo posted on a Facebook page of a young man named “Tom” on skis is nothing out of the ordinary. Hundreds of thousands of photos just like it are splattered all over the Internet. The exception in this case is that this man claimed to be a robust, healthy, active young man before a car accident caused by your insured a year before this particular photo was taken supposedly caused neck and back injuries that severely hampered his active lifestyle.

Wouldn’t you have loved to be armed with the picture of “Tom” on his skis when you entered settlement negotiations? How much less would you be willing to pay if you knew that the injured person was zooming down the slopes, running races, playing golf, or lifting weights following the accident? This might be a good time to re-examine your reserve.

The explosion of online “social media” can make this type of valuable information readily available from your desk—that is, if you know where and how to look for it.

In Tom’s case, his lawyer has sent you a demand letter in which he details how before the accident his client skied, played tennis, went dancing, did all the heavy work around the house, and coached his kids’ soccer teams in his spare time. But now, because of your insured’s negligence, the lawyer asserts that his client has been restricted to a sedentary lifestyle. Even worse, his income has taken a dive, because he can’t do the physical work his thriving landscape business requires.

Incriminating Posts

The Internet has been around long enough that most claims handlers now use it routinely to check everything from court dockets to statistical information about the venue of a lawsuit, but “social media” can often provide a much more detailed and candid look at a claimant than can be found in those dry statistics. At the very least, these sites can tell you a little bit more about the type of person with whom you are dealing. In the best case, you might find the incriminating photo or other information that completely contradicts the claims being presented before a settlement is reached.

Information available on these types of websites can include not only photos such as “Tom” doing the double black diamond trails, but also comments from his friends (for example, “can’t wait for skiing this weekend!”), current status reports from the claimant
himself ("having a great time on the slopes!")], and even videos (maybe showing the claimant and friend après ski).

The most popular of the “social media” or “social networking” sites is Facebook, which was founded by Harvard undergraduate students in 2004. In July 2010, Facebook boasted 500 million users. Facebook, Inc., now based in Palo Alto, Calif., employs some 1,700 people and reports projected revenues of more than $1 billion for 2010.

Facebook allows users to post photographs and personal information, write messages on other users’ “walls,” and announce their status, or what they are doing at that moment. Depending on the user’s privacy settings, this information may be restricted to “friends” whom he or she approves, or made more widely available to friends of friends or even the general public.

Other similar, but less popular sites include Myspace and Friendster, while Linked-In is more of a business networking site. Twitter provides short (140-character or less) bursts of instant news called “tweets” sent to a member’s “followers.” YouTube, founded in California in 2005 and now owned by Google, is a video exchange site that includes everything from TV commercials, professional music videos and movie segments, to grainy personal home videos. Craig’s List, which has been on the Web since the mid-1990s, is the online version of a newspaper’s classified ads, which allows users to list personal ads, jobs, and sales among other things.

Other Online Clues

Although not technically “social media,” other online resources helpful for investigating a claimant are their own personal web pages and blogs and the websites of any organizations to which they might belong. (For the uninitiated, a “blog,” short for “web log” is an online diary.) These may provide documentation of a person’s regular activities, which could be helpful in evaluating the effects, if any, of his injuries.

These online resources can provide a veritable treasure trove of information about claimants and witnesses. You might find that a claimant who says he can’t walk is boasting via Twitter about having just completed a 10-mile training run. A Facebook photo could be useful if you need to conduct surveillance. (If you are fortunate enough to catch a claimant in a blatant misrepresentation of his injuries, then you probably won’t need surveillance.) A video on YouTube of a supposedly injured person doing any physical activity could mean the difference between a win or a loss, and a person’s business activities on Linked-In may suggest he has exaggerated his economic claims.

In addition to learning more about your claimant, you may be able to locate others who can be helpful to your investigation. One way you might do this is by uncovering the identity of the claimant’s friends or business acquaintances who might be frank about his
condition. Sometimes plaintiffs exchange information on their blogs or pages about their accidents, or even their lawsuits.

Imagine this exchange on the Facebook “wall” of a claimant: “How’s your lawsuit going?” asks a friend. “Pretty good,” replies the plaintiff. “My lawyer says I’m going to get a lot of money.” Although this may sound farfetched, it does happen.

You can usually locate a person’s blog, Facebook, and other relevant pages with a simple run of their name through a search engine such as Bing or Google. It’s even possible to do a search for the person at a specific website to see if he or she is a member.

More on Tom’s Travails

Let’s return to our mythical claimant named Tom. When his lawyer describes the activities he allegedly can no longer do, check those as well. If the attorney says Tom has been forced to give up his passion for skiing because of the accident, then Google “ski clubs.” With a simple query, you might navigate to a database providing a list of ski clubs around the world. Then look for one near Tom’s hometown to check whether he is a member. If Tom claims to have given up coaching his kids’ soccer teams, then check the soccer club’s website, or online soccer bulletin boards.

If you are able to access Tom’s Facebook page or his blog and you find an entry such as: “In car accident yesterday. Not hurt. Off on ski trip,” then just imagine how helpful that information would be a year later when he testifies in the deposition that his skiing has been severely limited since the accident. Or, perhaps his Linked-In profile boasts of record earnings for his landscape business last year, all while he tells you he has a wage loss claim, access to the network to prove otherwise could be helpful. Conversely, sometimes these pages could validate a claim, as when Tom writes on his ski blog that he’s missing the season because of an accident.

Not everything online is public. Certain websites or website pages might be available only to those approved by the creator or owner of the page. On Facebook, for example, these are known as “friends,” or on Linked-In they are “connections.” Many users grant access to their pages to anyone who asks, but before you go asking a claimant to be your Facebook friend or posting a comment on his blog, make sure you are familiar with the insurance laws in the claimant’s state which might prohibit contact with a claimant who is represented by counsel.

If such contact is prohibited, then don’t even have someone else try to “friend” the person for you. Often, however, some of a Facebook page is available to anyone who looks, and sites such as blogs are usually open to anyone who finds them. Investigation becomes easier when a claim is in suit because it is then possible to have discovery, which can be enforced by court order. In that case, you might have defense counsel obtain in written discovery details of all activities in which the plaintiff participates, and of his work if
there is a claim for wage loss or loss of earning capacity. Ask counsel to follow up in depositions. If you are taking a proactive role in the investigation during litigation, then you can follow up on these, but the advantage of the attorney doing it is that it is more likely to be protected as work product.

If information about Tom and his ski trip or the like can be obtained from public sources, then it may not have to be revealed by defense counsel in discovery and may be used as rebuttal in trial, or if settlement strategy dictates, in mediation or settlement conferences.

Whether a defendant may compel a plaintiff through discovery to provide information needed to access his Facebook or MySpace pages—such as a log-in and password—remains to be seen, but as courts become more conversant with these sources of information, it seems likely that they will be made available subject to the same rules of relevance and privilege as older media outlets.

While the Internet and jet travel may have “shrunk” the world, the former has greatly expanded it in terms of opportunities for a more thorough and timely investigation of a claim.

**Know the Law Before You Snoop**

There are ways of obtaining non-public information as well, although the element of surprise will be lost. Ethical rules will most likely prohibit your counsel or anyone on their behalf from “friending” a represented claimant on Facebook or otherwise communicating with a plaintiff through a social networking site. At least one federal court in California, citing the 1986 Stored Communications Act, 18 U.S.C. §2701, et seq., has recognized the standing of social networking sites to move to quash subpoenas for members’ pages. However, Facebook’s policies advise members that the company may disclose information in response to a subpoena if it has a good faith belief that the law requires it.

http://www.propertycasualty360.com/2011/02/02/using-social-media-in-your-claims-investigations?t=investigativeforensics&page_all=1
Using Social Media in Claims Investigations
By Denise Johnson | November 5, 2012

The fact that there are currently 850 million Facebook users should prompt claims adjusters to look at the use of social media as a tool to further claims investigations.

The expectation that the number of Facebook users will grow to 1 billion by the end of this year is even more of reason, according to Richard Harer, vice president of Calif. – based Specialized Investigations.

“Social networking research and investigation is a required tool,” Harer said in remarks as one of the speakers at the Combined Claims Conference held earlier this year in Long Beach.

According to Harer, there are various investigative uses for social media including:

• Surveillance cases (photos, habits, activities)
• Locating witnesses, insured, claimant
• Background information like character, habits, activities, financial information
• Identifying relationships and/or accomplices

Harer said he investigated a claim involving a policyholder’s GPS alleged to have been stolen out of his car. Through investigation, Harer determined the policyholder had actually listed the GPS for sale on Craigslist.

While there is nothing unethical with accessing publicly available information, according to Harer, the now easily-accessible information may be dwindling as privacy concerns grow.

“Two thirds of Americans currently have a profile and six out of 10 set their main profile to private,” he said.

Though checking on a claimant via an Internet search is easily done in minutes, Harer warned that adjusters need to watch out for fictitious profiles.

As invaluable as social media is to a claims investigation, adjusters should not use impersonation to trick someone into releasing personal information, the investigator said. According to California insurance code section 791.03, one cannot pretend to be someone
he or she is not. There are exceptions where fraud or criminal activity or material misrepresentation is suspected.

Consider this scenario – an adjuster sets up a fake profile but has no friends. Harer said that is a red flag to those familiar with social media. In addition, doing this could create legal issues for the adjuster under current laws and many sites would consider it a violation of their terms.

There are ethical issues to consider, according to Jonathan H. Colman, an attorney with McDowell Shaw Colman & Garcia, a law firm with offices throughout the state. Most adjusters know better than to speak with a represented claimant; yet social media provides just that opportunity with the option of friending. He said there shouldn’t be any communication with a represented claimant via social media sites.

He advised against attorneys or adjusters instructing investigators to do something relating to social media because they may be liable for an investigator’s improper actions, citing the 1973 California case of Noble v. Sears, Roebuck & Co.

Harer said that while a user might enable privacy settings, the information may still be available for discovery in a legal proceeding. According to the New York case of Romano v. Steelcase, Inc. a social media site user has no reasonable expectation of privacy.

While someone’s Facebook postings may be discoverable, adjusters should not expect site owners to willingly cooperate with information requests, the investigator said, citing the 2010 California copyright infringement case of Crispin v. Christian Audigier. Subpoenas rarely get results because social networking providers usually don’t comply, he said.

“[Site owners are] very reticent to give up that information,” Colman said.

Defendants may be able to circumvent subpoenas altogether because the threshold for admissibility is low. According to Harer, courts have held that website printouts need not be authenticated by the website’s owner as per the 2007 California trademark claims case Jarritos Inc. v. Los Jarritos.

Colman recommended that interrogatories should seek to identify an opponent’s screen names and relevant information regarding social media usage. Requests for production should seek blog entries and social media postings and request for admissions should be designed to authenticate such information.

Depositions are also a good time for defense counsel to inquire about a claimant’s social media usage.
Adjusters should be aware that plaintiffs firms are now warning claimants to keep off of social media sites and to post fake information and comments such as, “Wow, my back is killing me. I’ve never been in this much pain.”

He said claimants are posting faked claims on Facebook, knowing that insurance company personnel, defense attorneys and investigators will look for it.

“Others post false information about subjects as form of retribution or retaliation,” Harer said. A jilted lover, ex-spouse or ex-business partner are commonly to blame.

Harer said adjusters should consider creating a social media release, similar to a medical records release, in order to obtain the information early on in a claims investigation. Adjusters can also create a list of questions directed at social media usage that can be asked during a recorded statement.

http://www.claimsjournal.com/news/national/2012/11/05/216789.htm
Social Media—Another Item for the Claims Toolbox

by John Butler, William Baumann and William Lenz, Gen Re, New York

Technology has done much for claims professionals over the years—the mobile office, searchable databases, interactions viewable online, GPS and "the paperless file," to name just a few. While investigative techniques have gained a high-tech edge, methods have always remained grounded in the fundamentals, such as personal interaction, witness statements, supporting documentation and photographs. However, information that once was only available through surveillance, anonymous tips, or a deep background check, may now be obtained via another source—namely social media websites.

As a result of the growing amount of information that is posted to social networking sites, claim professionals, and/or the experts they engage, have discovered that social media can be a useful investigative tool for conducting research and uncovering relevant information on claimants. Information obtained in this manner may contradict statements made by a claimant. Similarly, information derived from social media sites can also serve to provide further confirmation of the damages or injuries being claimed, thereby assisting a claim professional to establish a proper reserve and move a claim towards resolution. The impact and influence of social media on claim handling and litigation cannot be ignored.

In this article, we highlight some key factors about the social media platform and how its wealth of information can assist underwriters and claim professionals in evaluating risks and analyzing claim exposures.

Why is social media important to claim professionals? We are all in the risk-taking business, and information is our lifeline. When an additional tool becomes available that is likely to enhance the risk management or claim investigation process, it should be prudently embraced.
Understanding Social Media

Simply put, social media is an online platform that enables people, and other entities, to share information and/or content with many others in an interactive manner. Another online resource, which may not technically be "social media," includes "blogs." A blog is a type of interactive website maintained by an individual featuring regular entries that could include comments on events, current news, or personal editorials. Blog editors often encourage outside comment or feedback.

Over the past several years, the popularity of social networking sites on the Internet has increased dramatically. Millions of Internet users worldwide have embraced this relatively new form of communication. Participants willingly contribute and share their social and personal data, including photographs, through electronic storage systems where nothing is absolutely confidential. The sites are well-suited for obtaining information about individuals.

Wikipedia lists over 200 well-known, active social media sites, and its list is not exhaustive. The list includes the popular sites Facebook, Twitter, MySpace, YouTube and LinkedIn. Leading the way by far is Facebook which was launched in 2004. It has more than 800 million active users worldwide with more than 350 million of these users accessing Facebook through a mobile device. Like its competitor MySpace, which was launched the previous year, Facebook allows participants to set up a profile to which comments and photos can be posted. These profiles can also be connected to the profiles of other users. If a user does not take steps to limit access to his or her profile via privacy settings, this information is in the public domain.

Using social media in this way can serve to eliminate the time and money spent searching for claimants.

In a recent California workers' compensation matter, surveillance of the claimant's home proved fruitless. A perusal of his Facebook page revealed his scheduled participation in a bowling tournament, complete with the date, time and place. With this information, surveillance proved to be much more successful.

In another matter, a social media search provided proof of a claimant's side business that was not previously disclosed.

Not all benefits of social media investigations relate to contradicting a claimant's allegations. For example, a New Jersey auto loss resulted in serious injuries to a college student. The claimant's attorney was unresponsive to the adjuster's requests for information as to the extent of the claimant's injuries and his present condition. A social media search by the claim adjuster found a blog that was started by a friend of the claimant, which provided updated comments as to his condition and ongoing treatment. This information allowed the adjuster to keep his file current, assess the exposure and establish a proper reserve. While this blog was meant for the claimant's friends and family members, its public domain status provided useful information to the auto liability carrier.

It is standard practice for adjusters to obtain newspaper articles dealing with large property losses (e.g., fires, floods, etc.) or serious accidents. These days, it is possible that a video clip may have been taken by an observer from a cell phone or other electronic/digital device and posted to YouTube. In addition to the actual video that may provide insight into the loss, the videographer typically provides his or her own commentary. Further comments are typically posted by viewers, some of whom may also have been witnesses to the loss. These additional sources of information could aid in expediting adjustment of a claim.

Social Media and Discovery

Social media is fast becoming an integral part of the disclosure process. If a claimant's social media page is not available to the general public, related content should be requested through discovery requests. Once a claim is in litigation, the discovery process should be utilized to confirm the claimant's usage of social media and to obtain screen names, log-on information, and a release of relevant data from social networking sites. Obtaining information via subpoena from social media hosts without having user consent can be difficult. A better way to obtain this data is directly from the user as the social hosts have made it easy for social media users to download their entire account. Social media should also be considered as a topic for deposition questioning.

There are a few court rulings that address the permissible scope of discovery requests involving Facebook and other social networks. In one widely reviewed case, EEOC v. Simply Storage Management, LLC, an Indiana District Court's May 11, 2010 ruling provided guidance regarding the scope of discovery claimants would have to produce from their Internet social networking site ("SNS") profiles. The court
interpreted “profile” to mean “any content—including postings, pictures, blogs, messages, personal information, lists of ‘friends’ or causes joined—that the user has placed or created online by using her user account.”

In the case, the EEOC filed a complaint on behalf of two named claimants and similarly situated individuals who alleged sexual harassment by a supervisor. It was alleged that the employees had suffered from depression and stress disorders because of the harassment. Due to the parties’ disagreement about the proper scope of discovery regarding SNS profiles, the EEOC requested a discovery conference. The court saw that its challenge was to define “appropriately broad limits” on the discoverability of social communications in light of the “emotional and mental health” allegations while providing “meaningful direction” to the parties.

The court outlined three principles it would apply:

1. SNS content is not shielded from discovery simply because it is “locked” or “private.”
2. SNS content must be produced when it is relevant to a claim or defense in the case.
3. Allegations of depression, stress disorders, and like injuries do not automatically render all SNS communications relevant, but the scope of relevant communications is broader than that urged by the EEOC.

The court recognized discovery of the claimants’ SNS could reveal private and/or embarrassing information; however, the concern was “outweighed by the fact that the production here would be of information that the claimants have already shared with at least one other person through private messages or a larger number of people through postings.”

Other Uses of Social Media

The information that is available on social media sites will likely be used by all parties in litigation. Therefore don’t overlook posted content.

Double-Check Your Own Insured’s Background

Keep in mind that the claimant’s attorney will likely be conducting a similar search on your insured. The information available through social media may be utilized to research the insured and witnesses in order to determine whether there are any previously undisclosed facts that may be potentially damaging. The credibility of an insured or witness can be severely impacted by an ill-advised posting to a social network.

Underwriting Verification of Application

Such a search in regard to both personal and commercial insureds can be utilized to determine whether all material information was provided on the policy application. This type of search can be done during the underwriting process, as well as after the receipt of a claim.

Jury Selection

Lawyers on both sides have also taken to social media as an additional method by which to vet potential jurors during the jury selection process. Prior to selection, attorneys have been known to review the online personalities of prospective jurors in an attempt to ascertain how they may side on the particular issues of a claim. This information is then on hand during the voir dire to assist with decision making.

Product Liability Cases

Similarly, product liability lawyers are starting to search social media sites in an effort to identify information about product defects that may be posted by consumers via blogs or other websites. Attorneys have begun to cite consumer Internet postings in filed complaints and legal briefs as evidence in product liability matters.

Caveats and Concerns

As with all investigations, claim professionals should always proceed with caution and take measures to ensure that all actions are in compliance with the rules of professional and ethical responsibility in claim handling.

The investigator should not attempt to “friend” the claimant or set up a fake profile in an effort to get around privacy settings. Nor should there be any engagement in online discussion with the claimant in an attempt to elicit certain comments. Such activity could be seen as violating good faith claims handling guidelines and may open up exposure to privacy violations if seen as gaining information inappropriately.

In regard to information obtained from social networking sites, the applicable rules of evidence govern the admissibility of social media as evidence. The evidence must be proven to be relevant. Social media data must also be properly authenticated as webpages may be created under someone else’s name. Authentication could include the testimony of the investigator who procured the information or obtained the material directly from the website.

Conclusion

If at all possible, the investigation of social media should commence early in the claim handling process and be ongoing in light of the fact that additional content often continues to be posted to these sites. Information obtained from social media investigations may not provide evidence for outright rejection or denial of a claim but could possibly provide areas for further probing.
Claim professionals and attorneys are increasingly turning to social media as an additional resource by which to gather information during the course of claims investigation. While it is not a substitute for standard investigative methods, social media is a valuable tool and one that should be embraced and utilized appropriately.

About the Authors

**John Butler**, CPCU, ARe, is a Vice President and Claims Executive in Gen Re’s Claims department in New York. John has multi-line, Treaty and Facultative claim management responsibilities. He may be reached at 212 341 8038 or jbutler@genre.com.

**William Baumann** is a Vice President and Claims Executive in New York. Bill has claim management responsibilities for D&O, EPLI, financial institution E&O and general liability accounts. In this capacity, Bill is responsible for claim reviews, establishing and maintaining appropriate loss reserves, providing clients with claim trends, EPLI claims training and counseling on the high exposure cases to achieve optimal case outcomes. He may be reached at 212 341 8036 or wbaumann@genre.com.

**William Lentz**, CPCU, ARe, is a Second Vice President and Claims Executive in New York. Bill has multi-line claim management responsibilities for Treaty and Facultative claims, providing technical and administrative advice and support through client claim reviews, exposure analysis and large loss oversight. He may be reached at 212 341 8087 or wlentz@genre.com.

Here are some recent Gen Re Research publications:

- Changing the Rules—State High Courts Redefine Exposures for Commercial and Personal Lines Insurers—*Casually Matters*, November 2011
- EPLI Jurisdictional Survey—November 2011
- No Exit Strategy—November 2011
- Nanotechnology—The Smallest and Biggest Emerging Issue Facing Casualty Insurers?—*Insurance Issues*, November 2011
- Navigating the Claims Made Legal Maze—*Insurance Issues*, October 2011
- Logistics and 3PL—Property Matters, October 2011
- UM/UIM Updated Law Survey for Third Quarter 2011—*E-News Auto*, October 2011
- Dog Bite Liability—Insurers’ Best Friend?—*Insurance Issues*, September 2011
- The Regulatory Challenges Ahead—The Bulletin, September 2011
- Wind and Solar Energy Time Element—More Than Meets the Eye—*Facultative Matters*, August 2011
- Emerging Exposures and New Wordings—Are Your Forms Keeping Up?—*Policy Wordings Matters*, June 2011

**Endnotes**

1. www.wikipedia.com
2. www.facebook.com/press/info.com

The difference is... the quality of the promise.

www.genre.com

© 2011 General Re Corporation, Stamford, CT

This information was compiled by Gen Re and is intended to provide background information to our clients, as well as to our professional staff. The information is time sensitive and may need to be revised and updated periodically. It is not intended to be legal advice. You should consult with your own legal counsel before relying on it.
A Florida Bar member has asked the committee regarding the ethical obligations on advising clients to “clean up” their social media pages before litigation is filed to remove embarrassing information that the lawyer believes is not material to the litigation matter. The inquirer asks the following 4 questions:

1) Pre-litigation, may a lawyer advise a client to remove posts, photos, videos, and information from social media pages/accounts that are related directly to the incident for which the lawyer is retained?

2) Pre-litigation, may a lawyer advise a client to remove posts, photos, videos, and information from social media pages/accounts that are not related directly to the incident for which the lawyer is retained?

3) Pre-litigation, may a lawyer advise a client to change social media pages/accounts privacy settings to remove the pages/accounts from public view?

4) Pre-litigation, must a lawyer advise a client not to remove posts, photos, videos and information whether or not directly related to the litigation if the lawyer has advised the client to set privacy settings to not allow public access?

Rule 4-3.4(a) is applicable and states as follows:

A lawyer must not:

(a) unlawfully obstruct another party's access to evidence or otherwise unlawfully alter, destroy, or conceal a document or other material that the lawyer knows or reasonably should know is relevant to a pending or a reasonably foreseeable proceeding; nor counsel or assist another person to do any such act;

The comment to the rule provides further guidance:

The procedure of the adversary system contemplates that the evidence in a case is to be marshalled competitively by the contending parties. Fair competition in the adversary system is secured by prohibitions against destruction or concealment of evidence, improperly influencing witnesses, obstructive tactics in discovery procedure, and the like.

Documents and other items of evidence are often essential to establish a claim or defense. Subject to evidentiary privileges, the right of an opposing party, including the government, to obtain evidence through discovery or subpoena is an important procedural right. The exercise of that right can be frustrated if relevant material is altered, concealed, or destroyed. Applicable law in many jurisdictions makes it an offense to destroy material for the purpose of impairing its availability in a pending proceeding or one whose commencement can be foreseen. Falsifying
evidence is also generally a criminal offense. Subdivision (a) applies to evidentiary material generally, including computerized information.

The committee is of the opinion that the representation in this inquiry involves a “reasonably foreseeable proceeding” as the client has hired the lawyer, presumably to determine whether the client has a viable claim and pursue the claim if viable. However, under the rule, the proper inquiry is whether information on a client’s social media page is relevant to that reasonably foreseeable proceeding, rather than whether information is “related directly” or “not related directly” to the client’s matter. Information that is not “related directly” to the incident giving rise to the need for legal representation may still be relevant. However, what is relevant requires a factual, case-by-case determination. In Florida, the second District Court of Appeal has determined that normal discovery principles apply to social media, and that information sought to be discovered from social media must be “(1) relevant to the case's subject matter, and (2) admissible in court or reasonably calculated to lead to evidence that is admissible in court.” Root v. Balfour Beatty Construction, Inc., 132 So.3d 867, 869-70 (Fla. 2nd DCA 2014).

What constitutes an “unlawful” obstruction, alteration, destruction, or concealment of evidence is a legal question, outside the scope of an ethics opinion. The committee is aware of cases addressing the issue of discovery or spoliation relating to social media, but in these cases, the issue arose in the course of discovery after litigation commenced. See, Allied Concrete Co. v. Lester, 736 S.E.2d 699 (Va. 2013) (Sanctions of $542,000 imposed against lawyer and $180,000 against the client for spoliation when client, at lawyer's direction, deleted photographs from client's social media page, the client deleted the accounts, and the lawyer signed discovery requests that the client did not have the accounts); Gatto v. United Airlines, 2013 WL 1285285, Case No. 10-cv-1090-ES-SCM (U.S. Dist. Ct. NJ March 25, 2013) (Adverse inference instruction, but no monetary sanctions, against plaintiff who deactivated his social media accounts, which then became unavailable, after the defendants requested access); Romano v. Steelcase, Inc. 907 N.Y.S.2d 650 (NY 2010) (Court granted request for access to plaintiff's MySpace and Facebook pages, including private and deleted pages, when plaintiff's physical condition was at issue and information on the pages is inconsistent with her purported injuries based on information about plaintiff's activities available on the public pages of her MySpace and Facebook pages). In the disciplinary context, at least one lawyer has been suspended for 5 years for advising a client to clean up Facebook page, causing the removal of photographs and other material after a request for production had been made. In the Matter of Matthew B. Murray, 2013 WL 5630414, VSB Docket Nos. 11-070-088405 and 11-070-088422 (Virginia State Bar Disciplinary Board July 17, 2013).

The New York County Lawyers Association has issued NYCLA Ethics Opinion 745 (2013) addressing the issue. The opinion concludes that lawyers may advise their clients to use the highest level of privacy settings on their social media pages and may advise clients to remove information from social media pages unless the lawyer has a duty to preserve information under law and there is no violation of law relating to spoliation of evidence. Other states have since come to similar conclusions. See, e.g., North Carolina Formal Ethics Opinion 5 (attorney must advise client about information on social media if information is relevant and material to the client’s representation and attorney may advise client to remove information on social media if not spoliation or otherwise illegal); Pennsylvania Bar Association Opinion 2014-300 (attorney may advise client to delete information from client’s social media provided that this does not
constitute spoliation or is otherwise illegal, but must take appropriate action to preserve the
information); and Philadelphia Bar Association Professional Guidance Committee Opinion
2014-5 (attorney may advise a client to change the privacy settings on the client’s social media
page but may not instruct client to destroy any relevant content on the page). Subsequent to the
publication of the opinion, the New York State Bar Association’s Commercial and Federal
Litigation Section adopted Social Media Ethics Guidelines. Guideline No. 4.A, citing to the
opinion, states as follows:

A lawyer may advise a client as to what content may be maintained or made
private on her social media account, as well as to what content may be “taken
down” or removed, whether posted by the client or someone else, as long as there
is no violation of common law or any statute, rule, or regulation relating to the
preservation of information. Unless an appropriate record of the social media
information or data is preserved, a party or nonparty may not delete information
from a social media profile that is subject to a duty to preserve. [Footnote
omitted.]

The committee agrees with the NYCLA that a lawyer may advise a client to use the
highest level of privacy setting on the client’s social media pages.

The committee also agrees that a lawyer may advise the client pre-litigation to remove
information from a social media page, regardless of its relevance to a reasonably foreseeable
proceeding, as long as the removal does not violate any substantive law regarding preservation
and/or spoliation of evidence. The committee is of the opinion that if the lawyer does so, an
appropriate record of the social media information or data must be preserved if the information
or data is known by the lawyer or reasonably should be known by the lawyer to be relevant to the
reasonably foreseeable proceeding.

The committee is of the opinion that the general obligation of competence may require
the inquirer to advise the client regarding removal of relevant information from the client’s social
media pages, including whether removal would violate any legal duties regarding preservation of
evidence, regardless of the privacy settings. If a client specifically asks the inquirer regarding
removal of information, the lawyer’s advice must comply with Rule 4-3.4(a). What information
on a social media page is relevant to reasonably foreseeable litigation is a factual question that
must be determined on a case-by-case basis.

In summary, a lawyer may advise that a client change privacy settings on the client’s
social media pages so that they are not publicly accessible. Provided that there is no violation of
the rules or substantive law pertaining to the preservation and/or spoliation of evidence, a lawyer
also may advise that a client remove information relevant to the foreseeable proceeding from
social media pages as long as an appropriate record of the social media information or data is
preserved.
Fitbit Data Now Being Used In The Courtroom
Parmy Olson – November 16, 2014

Personal injury cases are prime targets for manipulation and conjecture. How do you show that someone who’s been in a car accident can’t do their job properly, and deserves thousands of dollars in compensation? Till now lawyers have relied on doctors to observe someone for half an hour or so and give their, sometimes-biased opinion. Soon, they might also tap the wealth of quantifiable data provided by fitness trackers. A law firm in Calgary is working on the first known personal injury case that will use activity data from a Fitbit to help show the effects of an accident on their client.

The young woman in question was injured in an accident four years ago. Back then, Fitbits weren’t even on the market, but given that she was a personal trainer, her lawyers at McLeod Law believe they can say with confidence that she led an active lifestyle. A week from now, they will start processing data from her Fitbit to show that her activity levels are now under a baseline for someone of her age and profession.

It will “back up what she’s been saying,” says her lawyer, Simon Muller of McLeod Law.

The lawyers aren’t using Fitbit’s data directly, but pumping it through analytics platform Vivametrica, which uses public research to compare a person’s activity data with that of the general population.

Muller says the case is “unique,” and does appear to be the first known case where data from a wearable is used in court. (If other earlier cases come to light I will update this post.)

“Till now we’ve always had to rely on clinical interpretation,” Muller says from his office in Calgary. “Now we’re looking at longer periods of time though the course of a day, and we have hard data.” His plaintiff will share her Fitbit data with Vivametrica for several months as part of an assessment period.

“We’re expecting the results to show that her activity level is less and compromised as a result of her injury.”

What’s intriguing (and a little creepy) is that cases like Muller’s could open the door to wearable device data being used not just in personal injury claims but in prosecutions. “Insurers will want it as much as plaintiffs will,” says Muller, for assessing sketchy claims.

Insurers wouldn’t be able to force claimants to wear Fitbits as part of an “assessment period,” like Muller’s client, but they could request a formal court order from whoever holds the data to release it to them, says Dr. Rick Hu, co-founder and CEO of
Vivametrica. “We would not release the information,” he adds. Insurers could instead request it from a law firm or even from Fitbit directly.

“It’s always evolving with technology,” says Muller. “A number of years ago we saw courts requisition Facebook [for] information. If you’ve been wearing the Fitbit monitors it’s likely you’ll see court applications to compel disclosure of that data.”

Data from wearables is poised to become even more insightful for courts as their sensors become ever more sophisticated: tracking not only steps, but continuous heart beat and temperature data.

Legal experts have already speculated about the idea of forcing the disclosure of wearable data on various law blogs. Says Neda Shakoori at McManis and Faulkner (emphasis mine):

“Wearables are yet another example of how technology may be a gold mine of potentially relevant [electronically stored information] for use in litigation. Take, for example, a personal injury case where a plaintiff is claiming the injuries he sustained in an automobile accident prevent him from participating in physical activities, such as running. Suppose further that the plaintiff has worn a fitness tracking device which has been recording every one of his five-mile runs during the past three months. The data generated by the plaintiff’s wearable device may be discovered in litigation and, as a result, completely discredit plaintiff’s case for damages resulting from the accident.

Wearable devices could become a “black box” for the human body, adds Matthew Pearn on Claims Canada, who says several previous court cases have already paved the way for more invasive disclosure of digital information in the court room.

At Muller’s law firm, using Fitbit data for his personal injury claim isn’t a one off.

“I’m already lining up more clients with a variety of circumstances to use this data,” he says. “You can’t rely on just one piece of data. You have to get all the pieces lined up.”

In a personal injury case, Maria Nucci petitions for certiorari relief to quash a December 12, 2013 order compelling discovery of photographs from her Facebook account. The photographs sought were reasonably calculated to lead to the discovery of admissible evidence and Nucci’s privacy interest in them was minimal, if any. Because the discovery order did not amount to a departure from the essential requirements of law, we deny the petition.

In her personal injury lawsuit, Nucci claimed that on February 4, 2010, she slipped and fell on a foreign substance on the floor of a Target store. In the complaint, she alleged the following:

- Suffered bodily injury
- Experienced pain from the injury
- Incurred medical, hospital, and nursing expenses, suffered physical handicap
- Suffered emotional pain and suffering
- Lost earnings
- Lost the ability to earn money
- Lost or suffered a diminution of ability to enjoy her life
- Suffered aggravation of preexisting injuries
- Suffered permanent or continuing injuries
- Will continue to suffer the losses and impairment in the future

Target took Nucci’s deposition on September 4, 2013. Before the deposition, Target’s lawyer viewed Nucci’s Facebook profile and saw that it contained 1,285 photographs. At the deposition, Nucci objected to disclosing her Facebook photographs. Target’s lawyer examined Nucci’s Facebook profile two days after the deposition and saw that it listed only 1,249 photographs. On September 9, 2013, Target moved to compel inspection of Nucci’s Facebook profile. Target wrote to Nucci and asked that she not destroy further information posted on her social media websites. Target argued that it was entitled to view the profile because Nucci’s lawsuit put her physical and mental condition at issue.

Nucci’s response to the motion explained that, since its creation, her Facebook page had been on a privacy setting that prevented the general public from having access to her account. She claimed that she had a reasonable expectation of privacy regarding her Facebook information and that Target’s access would invade that privacy right. In addition, Nucci argued that Target’s motion was an overbroad fishing expedition.

On October 17, 2013, the trial court conducted a hearing on Target’s motion to compel. At the hearing, Target showed the court photographs from a surveillance video in which Nucci could be seen walking with two purses on her shoulders or carrying two jugs of water. Again, Target argued that because Nucci had put her physical condition at question, the relevancy of the Facebook photographs outweighed Nucci’s right to privacy. It also argued that there was no constitutional right to privacy in photographs posted on Facebook. The circuit court denied Target’s motion to compel, in part because the request was “vague, overly broad and unduly burdensome.”

Target responded to the court’s ruling by filing narrower, more focused discovery requests. Target served Nucci with a set of Electronic Media Interrogatories, with four questions. It also served a Request for Production of Electronic Media, requesting nine items. In response to the interrogatories, Nucci objected on the grounds of (1) privacy; (2) items not readily accessible; and (3) relevance.
As to the Request for Production, Nucci raised the same three objections and additionally argued that the request was (4) overbroad; (5) brought solely to harass; (6) “over[ly] burdensome;” (7) “unduly burdensome”; and (9) unduly vague. Nucci raised only these general claims and no objections specifically directed at any particular photograph.

Target moved that the trial court disallow Nucci’s objections. At a hearing on the motion, Target conceded that its request for production should be limited to photographs depicting Nucci. After a hearing on the motion, the trial court granted Target’s motion in part and denied it in part. On December 12, 2013, the trial court compelled answers to the following interrogatories:

1. Identify all social/professional networking websites that Plaintiff is registered with currently (such as Facebook, MySpace, LinkedIn, Meetup.com, MyLife, etc.)

2. Please list the number and service carrier associated with each cellular telephone used by the Plaintiff and/or registered in the Plaintiff’s name (this includes all numbers registered to and/or used by the Plaintiff under a “family plan” or similar service) at the time of loss and currently.

The order also compelled production of the following items:

1. For each social networking account listed in response to the interrogatories, please provide **copies or screenshots of all photographs associated with that account during the two (2) years prior to the date of loss.**

2. For each social networking account listed in the interrogatories, provide **copies or screenshots of all photographs associated with that account from the date of loss to present.**

3. For each cell phone listed in the interrogatories, please provide **copies or screenshots of all photographs associated with that account during the two years prior to the date of loss.**

4. For each cellular phone listed in response to the interrogatories, please provide **copies or screenshots of all photographs associated with that account from the date of loss to present.**
5. For each cellular phone listed in the interrogatories, please provide **copies of any documentation outlining what calls were made or received on the date of loss**.

Nucci argues that the December 12 order departs from the essential requirements of the law because it constitutes an invasion of privacy.\(^1\) Citing to *Salvato v. Miley*, No. 5:12-CV-635-Oc-10PRI, 2013 WL 2712206 (M.D. Fla. June 11, 2013), which involved a request for e-mails and text messages, she contends that “the mere hope” that the discovery yields relevant evidence is not enough to warrant production. She also argues that the traditional rules of relevancy still apply to a request for social media materials. Nucci additionally asserts that her activation of privacy settings demonstrates an invocation of federal law. *See Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 961 F. Supp. 2d 659, 665 (D.N.J. 2013). Relying upon *Ehling*, Nucci argues that her private Facebook posts were covered by the Federal Stored Communications Act (“SCA”), 18 U.S.C. §§ 2701-2712, and were not therefore discoverable. We note that Nucci objected below to all disclosure; she did not attempt to limit disclosure of the photographs by establishing discrete guidelines. *See Reid v. Ingerman Smith LLP*, No. CV 2012-0307(ILG)(MDG), 2012 WL 6720752, at *2 (E.D.N.Y. Dec. 27, 2012); *E.E.O.C. v. Simply Storage Mgmt., LLC*, 270 F.R.D. 430, 436 (S.D. Ind. 2010).

In its response, Target points out, as it did below, that surveillance videos show Nucci carrying heavy bags, jugs of water, and doing other physical acts, suggesting that her claim of serious personal injury is suspect.

Target suggests that the material ordered is relevant to Nucci’s claim of injury in that it allows a comparison of her current physical condition and limitations to her physical condition and quality of life before the date of the slip and fall. In its response to this Court, Target concedes that the order is limited to photographs depicting Nucci from the two years before the date of the incident to the present. It argues that the trial court did not grant unfettered access because it did not compel the production of passwords to her social networking accounts.

As to material injury or harm, Target points out that Nucci has not claimed that production of any particular photograph or other identifiable material will cause her damage or embarrassment. Citing to *Davenport v. State Farm Mutual Automobile Insurance Co.*, No. 3:11-cv-632-J-JBT, 2012

\(^1\)The petition challenges the order to produce content from social networking sites. The petition does not challenge that portion of the orders below pertaining to a cellular telephone.
WL 555759 (M.D. Fla. Feb. 21, 2012), Target contends that the content of social networking sites is not privileged or protected by the right to privacy. It notes that Facebook’s terms and conditions explain that, regardless of a user’s intentions, the material contained in a post could be disseminated by Facebook at its discretion or under court order.

Finally, Target argues that in the context of a civil lawsuit, Florida courts can compel a party to release relevant records from social networking sites without implicating or violating the SCA.

Discussion

This case stands at the intersection of a litigant’s privacy interests in social media postings and the broad discovery allowed in Florida in a civil case. Consideration of four factors leads to the conclusion that Nucci’s petition for certiorari should be denied. First, certiorari relief is available in only a narrow class of cases and this case does not meet the stringent requirements for certiorari relief. Second, the scope of discovery in civil cases is broad and discovery rulings by trial courts are reviewed under an abuse of discretion standard. Third, the information sought—photographs of Nucci posted on Nucci’s social media sites—is highly relevant. Fourth, Nucci has but a limited privacy interest, if any, in pictures posted on her social networking sites.

Nucci’s petition challenges only the discovery of photographs from social networking sites, such as Facebook. Thus, the order compelling the answers to interrogatories and production pertaining to a cellular phone are not at issue. Similarly, our ruling in this case covers neither communications other than photographs exchanged through electronic means nor access to other types of information contained on social networking sites.

Legal Standard for Certiorari

Certiorari is not available to review every erroneous discovery ruling. To be entitled to certiorari, the petitioner must establish three elements: “(1) a departure from the essential requirements of the law, (2) resulting in material injury for the remainder of the case (3) that cannot be corrected on postjudgment appeal.” Williams v. Oken, 62 So. 3d 1129, 1132 (Fla. 2011) (quoting Reeves v. Fleetwood Homes of Fla., Inc., 889 So. 2d 812, 822 (Fla. 2004)). The last two elements, often referred to as “irreparable harm,” are jurisdictional. If a petition fails to make a threshold showing of irreparable harm, this Court will dismiss the petition. Bared & Co., Inc. v. McGuire, 670 So. 2d 153, 157 (Fla. 4th DCA 1996).
Overbreadth of discovery alone is not a basis for certiorari jurisdiction. *Bd. of Trs. of Internal Improvement Trust Fund v. Am. Educ. Enters., LLC*, 99 So. 3d 450, 456 (Fla. 2012). Similarly, mere irrelevance is not enough to justify certiorari relief. Certiorari may be granted from a discovery order where a party “affirmatively establishes” that the private information at issue is not relevant to any issue in the litigation and is not reasonably calculated to lead to admissible evidence. *Id.* at 457 (quoting *Allstate Ins. Co. v. Langston*, 655 So. 2d 91, 95 (Fla. 1995)); see also *Berkeley v. Eisen*, 699 So. 2d 789 (Fla. 4th DCA 1997) (granting certiorari relief to protect privacy rights of non-parties to litigation). “The concept of relevancy has a much wider application in the discovery context than in the context of admissible evidence at trial.” *Bd. of Trs.*, 99 So. 3d at 458.

Certiorari relief is discretionary, but this Court should exercise this discretion only where the party has shown that “there has been a violation of clearly established principle of law resulting in a miscarriage of justice.” *Williams*, 62 So. 3d at 1133 (quoting *Haines City Cmty. Dev. v. Heggs*, 658 So. 2d 523, 527 (Fla. 1995)). The error must be serious to merit certiorari relief. Even where a departure from the essential requirements of law is shown, this Court may still deny the petition as certiorari relief is discretionary. *Id.*

*The Broad Scope of Discovery*

A “part[y] may obtain discovery regarding any matter, not privileged, that is relevant to the subject matter of the pending action, whether it relates to the claim or defense of the party seeking discovery or the claim or defense of any other party.” Fla. R. Civ. P. 1.280(b)(1). “It is not ground for objection that the information sought will be inadmissible at the trial if the information sought appears reasonably calculated to lead to the discovery of admissible evidence.” *Id.* (emphasis added). Florida Rule of Civil Procedure 1.350(a) includes electronically stored information within the scope of discovery. An outer limit of discovery is that "litigants are

2Rule 1.350(a) states:

Any party may request any other party (1) to produce and permit the party making the request, or someone acting in the requesting party’s behalf, to inspect and copy any designated documents, including *electronically stored information*, writings, drawings, graphs, charts, photographs, phono-records, and other data compilations from which information can be obtained, translated, if necessary, by the party to whom the request is directed through detection devices into reasonably usable form, that constitute or contain matters within the scope of rule 1.280(b) and that are in
not entitled to carte blanche discovery of irrelevant material.” Life Care Ctrs. of Am. v. Reese, 948 So. 2d 830, 832 (Fla. 5th DCA 2007) (quoting Tanchel v. Shoemaker, 928 So. 2d 440, 442 (Fla. 5th DCA 2006)). Because the permissible scope of discovery is so broad, a “trial court is given wide discretion in dealing with discovery matters, and unless there is a clear abuse of that discretion, the appellate court will not disturb the trial court’s order.” Alvarez v. Cooper Tire & Rubber Co., 75 So. 3d 789, 793 (Fla. 4th DCA 2011) (direct appeal of discovery issue). It is because of this wide discretion accorded to trial judges that it is difficult to establish certiorari jurisdiction of discovery orders.

In a personal injury case where the plaintiff is seeking intangible damages, the fact-finder is required to examine the quality of the plaintiff’s life before and after the accident to determine the extent of the loss. From testimony alone, it is often difficult for the fact-finder to grasp what a plaintiff’s life was like prior to an accident. It would take a great novelist, a Tolstoy, a Dickens, or a Hemingway, to use words to summarize the totality of a prior life. If a photograph is worth a thousand words, there is no better portrayal of what an individual’s life was like than those photographs the individual has chosen to share through social media before the occurrence of an accident causing injury. Such photographs are the equivalent of a “day in the life” slide show produced by the plaintiff before the existence of any motive to manipulate reality. The photographs sought here are thus powerfully relevant to the damage issues in the lawsuit. The relevance of the photographs is enhanced, because the post-accident surveillance videos of Nucci suggest that her injury claims are suspect and that she may not be an accurate reporter of her pre-accident life or of the quality of her life since then. The production order is not overly broad under the circumstances, as it is limited to the two years prior to the incident up to the present; the photographs sought are easily accessed and exist in electronic form, so compliance with the order is not onerous.

The Right of Privacy

To curtail the broad scope of discovery allowed in civil litigation, Nucci asserts a right of privacy. However, the relevance of the photographs overwhelms Nucci’s minimal privacy interest in them.

---

the possession, custody, or control of the party to whom the request is directed . . .

(Emphasis added).
The Florida Constitution expressly protects an individual’s right to privacy. See Art. I, § 23, Fla. Const. (“Every natural person has the right to be let alone and free from governmental intrusion into the person’s private life except as otherwise provided herein.”). This right is broader than the right to privacy implied in the Federal Constitution. Berkeley, 699 So. 2d at 790. The right to privacy in the Florida Constitution “ensures that individuals are able ‘to determine for themselves when, how and to what extent information about them is communicated to others.’” Shaktman v. State, 553 So. 2d 148, 150 (Fla. 1989) (quoting A. Westin, Privacy and Freedom 7 (1967)).

Before the right to privacy attaches, there must exist a legitimate expectation of privacy. Winfield v. Div. of Pari-Mutuel Wagering, Dep’t of Bus. Regulation, 477 So. 2d 544, 547 (Fla. 1985). Once a legitimate expectation of privacy is shown, the burden is on the party seeking disclosure to show the invasion is warranted by a compelling interest and that the least intrusive means are used. Id. In the civil discovery context, courts must engage in a balancing test, weighing the need for the discovery against the privacy interests. Rasmussen v. S. Fla. Blood Serv., Inc., 500 So. 2d 533, 535 (Fla. 1987). If the person raising the privacy bar establishes the existence of a legitimate expectation of privacy, the party seeking to obtain the private information has the burden of establishing need sufficient to outweigh the privacy interest. Berkeley, 699 So. 2d at 791-92.

In a thoughtful opinion, a Palm Beach County circuit judge has summarized the nature of social networking sites as follows:

Social networking sites, such as Facebook, are free websites where an individual creates a “profile” which functions as a personal web page and may include, at the user’s discretion, numerous photos and a vast array of personal information including age, employment, education, religious and political views and various recreational interests. Trail v. Lesko, [No. GD-10-017249,] 2012 WL 2864004 (Pa. Com. Pl. July 5, 2012). Once a user joins a social networking site, he or she can use the site to search for “friends” and create linkages to others based on similar interests. Kelly Ann Bub, Comment, Privacy’s Role in the Discovery of Social Networking Site Information, 64 SMU L. Rev. 1433, 1435 (2011).

Through the use of these sites, “users can share a variety of materials with friends or acquaintances of their choosing, including tasteless jokes, updates on their love lives, poignant
reminiscences, business successes, petty complaints, party photographs, news about their children, or anything else they choose to disclose.” Bruce E. Boyden, Comment, *Oversharing: Facebook Discovery and the Unbearable Sameness of Internet Law*, 65 Ark. L. Rev. 39, 42 (2012). As a result, social networking sites can provide a “treasure trove” of information in litigation. Christopher B. Hopkins, *Discovery of Facebook Contents in Florida Cases*, 31 No. 2 Trial Advoc. Q. 14 (2012).


We agree with those cases concluding that, generally, the photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings that the user may have established. *See Davenport v. State Farm Mut. Auto. Ins. Co.*, No. 3:11-cv-632-J-JBT, 2012 WL 555759, at *1 (M.D. Fla. Feb. 21, 2012); *see also Patterson v. Turner Constr. Co.*, 931 N.Y.S.2d 311, 312 (N.Y. App. 2011) (holding that the “postings on plaintiff’s online Facebook account, if relevant, are not shielded from discovery merely because plaintiff used the service’s privacy settings to restrict access”). Such posted photographs are unlike medical records or communications with one’s attorney, where disclosure is confined to narrow, confidential relationships. Facebook itself does not guarantee privacy. *Romano v. Steelcase, Inc.*, 907 N.Y.S.2d 650, 656 (N.Y. Sup. Ct. 2010). By creating a Facebook account, a user acknowledges that her personal information would be shared with others. *Id.* at 657. “Indeed, that is the very nature and purpose of these social networking sites else they would cease to exist.” *Id.*

Because “information that an individual shares through social networking web-sites like Facebook may be copied and disseminated by another,” the expectation that such information is private, in the traditional sense of the word, is not a reasonable one. *Beswick v. N.W. Med. Ctr., Inc.*, No. 07-020592 CACE(03), 2011 WL 7005038 (Fla. 17th Cir. Ct. Nov. 3, 2011). As one federal judge has observed,

Even had plaintiff used privacy settings that allowed only her “friends” on Facebook to see postings, she “had no justifiable expectation that h[er] ‘friends’ would keep h[er] profile private. . . .” *U.S. v. Meregildo*, 2012 WL 3264501, at *2 (S.D.N.Y. 2012). In fact, “the wider h[er] circle of ‘friends,’ the more likely [her] posts would be viewed by someone [s]he never expected to see them.” *Id.* Thus, as the Second Circuit has recognized, legitimate expectations of privacy may be lower in
e-mails or other Internet transmissions. *U.S. v. Lifshitz*, 369 F.3d 173, 190 (2d Cir. 2004) (contrasting privacy expectation of e-mail with greater expectation of privacy of materials located on a person’s computer).

*Reid v. Ingerman Smith LLP*, No. CV2012-0307(ILG)(MDG), 2012 WL 6720752, at *2 (E.D.N.Y. Dec. 27, 2012); see also *Tompkins v. Detroit Metro. Airport*, 278 F.R.D. 387, 388 (E.D. Mich. 2012) (holding that “material posted on a ‘private’ Facebook page, that is accessible to a selected group of recipients but not available for viewing by the general public, is generally not privileged, nor is it protected by common law or civil law notions of privacy”); *Mailhoit v. Home Depot U.S.A., Inc.*, 285 F.R.D. 566, 570 (C.D. Cal. 2012) (indicating that social networking site content is neither privileged nor protected, but recognizing that party requesting discovery must make a threshold showing that such discovery is reasonably calculated to lead to admissible evidence).

We distinguish this case from *Root v. Balfour Beatty Construction, LLC*, 132 So. 3d 867 (Fla. 2d DCA 2014). That case involved a claim filed by a mother on behalf of her three-year-old son who was struck by a vehicle. Unlike this case, where the trial court ordered the production of photographs from the plaintiff’s Facebook account, the court in *Balfour* ordered the production of a much broader swath of Facebook material without any temporal limitation—postings, statuses, photos, “likes,” or videos—that relate to the mother’s relationships with all of her children, not just the three year old, and with “other family members, boyfriends, husbands, and/or significant others, both prior to, and following the accident.” *Id.* at 869. The second district determined that “social media evidence is discoverable,” but held that the ordered discovery was “overbroad” and compelled “the production of personal information . . . not relevant to” the mother’s claims. *Id.* at 868, 870. The court found that this was the type of “carte blanche” irrelevant discovery the Florida Supreme Court has sought to guard against. *Id.* at 870; *Langston*, 655 So. 2d at 95 (“[W]e do not believe that a litigant is entitled carte blanche to irrelevant discovery.”) The discovery ordered in this case is narrower in scope and, as set forth above, is calculated to lead to evidence that is admissible in court.

Finally, we reject the claim that the Stored Communications Act, 18 U.S.C. §§ 2701-2712, has any application to this case. Generally, the “SCA prevents ‘providers’ of communication services from divulging private communications to certain entities and/or individuals.” *Quon v. Arch Wireless Operating Co., Inc.*, 529 F.3d 892, 900 (9th Cir. 2008), rev’d on other grounds by *City of Ontario, Cal. v. Quon*, 560 U.S. 746 (2010) (citation
omitted). The act does not apply to individuals who use the communications services provided. See, e.g., Flagg v. City of Detroit, 252 F.R.D. 346, 349 (E.D. Mich. 2008) (ruling that the SCA does not preclude civil discovery of a party’s electronically stored communications which remain within the party’s control even if they are maintained by a non-party service provider).

Finding no departure from the essential requirements of law, we deny the petition for certiorari.

STEVENSON and GERBER, JJ., concur.

*    *    *

Not final until disposition of timely filed motion for rehearing.
Presently before the Court is the Defendant’s (hereinafter “Weis Markets”) Motion to Compel Disclosure and Preservation of Plaintiff’s (“Zimmerman”) Facebook and MySpace Information. At issue is access, by court order, to the non-public portions of these websites established by Zimmerman through his disclosure of passwords, user names and log in names to counsel for Weis Markets.

The case at bar involves an accident that occurred on April 21, 2008 while Zimmerman was operating a forklift at Weis Markets’ warehouse located in Milton, Pennsylvania.¹ Zimmerman seeks damages for the injuries caused to his left leg as a result of the accident, including lost wages, lost future earning capacity, pain and suffering, scarring and “embarrassment.” He avers that “his health in general has been seriously and permanently impaired and compromised” and, that “he has sustained a

¹ Zimmerman was an employee of a subcontractor of Weis Markets.
permanent diminution in the ability to enjoy life and life’s pleasures.” See Complaint, paragraph 25 (b),(e) and (f).

Weis Markets, upon review of the public portion of Zimmerman’s Facebook page, discovered that his interests included “ridin” and “bike stunts” and his MySpace page contains more recent photographs depicting Zimmerman with a black eye and his motorcycle before and after an accident. Additionally, there are photographs of Zimmerman wearing shorts, and his scar from this accident is clearly visible. Weis Markets argues that this is relevant because at his deposition, Zimmerman claimed he never wears shorts because he is embarrassed by his scar. Based on what was observed on the publicly available portions of Zimmerman’s Facebook and MySpace pages, Weis Markets believes there may be other relevant information as to Zimmerman’s damage claims on the non-public portions of his Facebook and MySpace pages.

Zimmerman argues that his privacy interests outweigh the need to obtain the discovery material.\(^2\) Weis Markets urges this Court to adopt the holding in *McMillen v. Hummingbird Speedway Inc.*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Jefferson Co. Com.Pl. 2010), which granted a request for access to plaintiff’s Facebook and MySpace pages. *McMillen* appears to be the only published opinion in Pennsylvania which relates to access to social networking information through discovery.\(^3\) For the reasons that follow, this Court will grant the Motion to Compel.

\(^2\) In the alternative, Zimmerman also argued that the Court should conduct an in-camera review and decide what materials should be provided to Weis Markets. This argument is flatly rejected as an unfair burden to place on the Court, which would not only require the time and resources necessary to complete a thorough search of these sites, but also would require the Court to guess as to what is germane to defenses which may be raised at trial.

\(^3\) Most recently, on May 5, 2011, in the Bucks County Court of Common Pleas, in the case of *Piccolo v. Paterson*, the Honorable Albert J. Cepparulo denied a motion to compel filed by defendant seeking access to photographs the plaintiff had posted on her Facebook page. As discussed in the article “Facebook Postings Barred from Discovery in Accident Case,” published in *The Legal Intelligencer* on May 17, 2011,
This Court agrees with the rationale of the opinion in McMillen, authorizing access for the reasons that no privilege exists in Pennsylvania for information posted in the non-public sections of social websites, liberal discovery is generally allowable, and the pursuit of truth as to alleged claims is a paramount ideal. Upon review of this area of the law, this Court further finds the analysis and rationale, with discussion of instructive cases from other jurisdictions, as set forth in Romano v. Steelcase, Inc., 907 N.Y.S.2d 650 (Suffolk Co. 2010), well reasoned and applicable to the present case. The defendant in Romano sought access to plaintiff’s current and historical Facebook and MySpace pages and accounts, including deleted pages, based on the fact that the plaintiff had posted information on those sites inconsistent with her claims in the personal injury action. As in the case at bar, the plaintiff in Romano alleged that she could no longer participate in certain activities and that her injuries affected her enjoyment of life. Contrary to those claims, pictures on her Facebook and MySpace pages demonstrated an active social life and travel to other states, despite assertions that her injuries prohibited travel.

Likewise, the defendant in Romano had gained access to its initial information from the public portions of plaintiff’s Facebook and MySpace accounts, but sought

the motion to compel followed the plaintiff’s deposition, where she indicated that she had a Facebook page, and the information was publicly available. Despite this claim, when defense counsel attempted to view the plaintiff’s Facebook page, it was discovered that only “friends” of the plaintiff could view her postings and photographs. Defense counsel sought to have the plaintiff accept a “friend request” so that her photographs could be viewed, and cited McMillen, supra in support of her position. Counsel for plaintiff argued that she was only questioned about photographs at her deposition, and an extensive number of photographs both before and after the accident had already been provided, and there was no assertion that the textual postings on her Facebook page would likely lead to the discovery of material evidence. Following a review of briefs, Judge Cepparulo denied the motion, without amplification.

As set forth in McMillen: “Where there is an indication that a person’s social network sites contain information relevant to the prosecution or defense of a lawsuit, therefore, and given Koken’s [Koken v. One Beacon Ins. Co., 911 A.2d 1021 (Pa.Cmwlth. 2006)] admonition that the courts should allow litigants to utilize “all rational means for ascertaining the truth,” 911 A.2d at 1027, and the law’s general dispreference for the allowance of privileges, access to those sites should be freely granted.” McMillen at page 12.
access to the non-public portions of these sites, arguing there was a reasonable likelihood therein that additional evidence relating to plaintiff’s claims of loss of enjoyment of life’s activities would be found. The court in Romano agreed, finding that the information sought by the defendant was both material and necessary. Id. at 654.

The Romano court, faced with a dearth of any New York case law directly on point, actually reviewed a Canadian case which had previously addressed this issue. In the case of Leduc v. Roman, 2009 CarswellOnt 843 (February 20, 2009), the Superior Court of Justice of Ontario, Canada permitted access to plaintiff’s private Facebook profile, stating:

To permit a party claiming very substantial damages for loss of enjoyment of life to hide behind self-set privacy controls on a website, the primary purpose of which is to enable people to share information about how they lead their social lives, risks depriving the opposite party of access to material that may be relevant to ensuring a fair trial. Romano at 655.

The same conclusion was noted by the court in Romano to have been reached by a Colorado court in Ledbetter v. Wal-Mart Stores, Inc., 2009 WL 1067018 (D.Colo. 2009)(the content of social networking sites in the public areas contradicted the allegations as to the effect of the injuries on their daily lives). Persuaded by these authorities, the Romano court specifically found:

Thus, it is reasonable to infer from the limited postings on Plaintiff’s public Facebook and MySpace profile pages, that her private pages may contain materials and information that are relevant to her claims or that may lead to the disclosure of admissible evidence. To deny Defendant an opportunity [to] access to these sites not only would go against the liberal discovery policies of New York favoring pre-trial disclosure, but would condone Plaintiff’s attempt to hide relevant information behind self-regulated privacy settings. Id.
The plaintiff in Romano contended that production of her entries on Facebook and MySpace would violate her right to privacy, which outweighed the defendant’s need for the information.\textsuperscript{5} However, as Romano aptly noted, “[t]he Fourth Amendment’s right to privacy, protects people, not places” citing Katz v. United States, 389 U.S. 347 (1967) and the reasonableness standard imposed thereunder (i.e. a reasonable expectation of privacy). As noted by Romano, it was stated by the United States District Court of New Jersey in Beye v. Horizon Blue Cross Blue Shield of New Jersey, 06-5337 (D.N.J. December 14, 2007): “[t]he privacy concerns are far less where the beneficiary herself chose to disclose the information.” Further, Romano found both California and Ohio courts that rejected the notion of a reasonable expectation of privacy as to MySpace postings. See Moreno v. Hanford Sentinel Inc., 172 Cal.App.4th 1125 (Cal.App. 5 Dist. 2009) and Dexter v. Dexter, 2007 WL 1532084 (Ohio App. 11 Dist. 2007). All the authorities recognize that Facebook and MySpace do not guarantee complete privacy. Facebook’s privacy policy explains that users post any content on the site at their own risk and informs users that this information may become publicly available.\textsuperscript{6} The Romano court therefore concluded:

Thus, when Plaintiff created her Facebook and MySpace accounts, she consented to the fact that her personal information would be shared with others, notwithstanding her privacy settings...Since Plaintiff knew that her information may become publicly available, she cannot now claim that she had a reasonable expectation of privacy. Romano at 657.

\textsuperscript{5} This contention was not addressed in McMillen, supra, which focused on the issue of whether a privilege for such non-disclosure existed.

\textsuperscript{6} It is well publicized that Facebook’s privacy policy and its revisions have been the subject of criticism and controversy that may be never ending. One need only “Google” search the terms “Facebook privacy” for an exhaustive list of access to articles on the topic.
In view of the sound, logical approach of the court in *Romano*, this Court is likewise persuaded that the argument of Zimmerman that his privacy interests outweigh the discovery requests is unavailing.

It is well recognized that the Pennsylvania Rules of Civil Procedure, like New York, provide for liberal discovery: “Generally, discovery is liberally allowed with respect to any matter, not privileged, which is relevant to the cause being tried. Pa.R.C.P. 4003.1.” *Rohm and Haas Co. v. Lin*, 992 A.2d 132, 143 (Pa.Super. 2010). Zimmerman placed his physical condition in issue, and Weis Markets is entitled to discovery thereon. Based on a review of the publicly accessible portions of his Facebook and MySpace accounts, there is a reasonable likelihood of additional relevant and material information on the non-public portions of these sites. Zimmerman voluntarily posted all of the pictures and information on his Facebook and MySpace sites to share with other users of these social network sites, and he cannot now claim he possesses any reasonable expectation of privacy to prevent Weis Markets from access to such information. By definition, a social networking site is the interactive sharing of your personal life with others; the recipients are not limited in what they do with such knowledge. With the initiation of litigation to seek a monetary award based upon limitations or harm to one’s person, any relevant, non-privileged information about one’s life that is shared with others and can be gleaned by defendants from the internet is fair game in today’s society.

Accordingly, Weis Markets’ Motion to Compel is granted.8

---

7 The proposed amendments to Pa.R.C.P. 4009.1, 4009.11, 4009.12, 4009.21, 4009.23 and 4011, which relate to e-discovery and electronically stored information, do not address the issue of access to information contained on social networking sites. However, the proposed amendments indicate that the discovery of electronically stored information will be governed by the same considerations governing other discovery. *See* 41 Pa.Bull. No. 3, 334-336 (January 15, 2011).

8 However, this should not be construed as an entitlement to this type of information in every personal injury case where damages are claimed, i.e. a carte blanche entitlement to Facebook and MySpace
Based on the foregoing, the following Order is entered:

ORDER

AND NOW, this 19th day of May, 2011, it is hereby ORDERED that Plaintiff shall provide all passwords, user names and log-in names for any and all MySpace and Facebook accounts to Defendant within twenty (20) days from the date hereof. It is FURTHER ORDERED that Plaintiff shall not take steps to delete or alter existing information and posts of his MySpace or Facebook accounts.9

BY THE COURT:

__________________________
Charles H. Saylor, Judge

pc: Douglas N. Engleman, Esquire, and Jonathan F. Bach, Esquire, 140 East Third Street, Williamsport, PA 17701
Stephen E. Geduldig, Esquire, and Stephanie L. Hersperger, Esquire, 305 North Front Street, P.O. Box 999, Harrisburg, PA 17108
Jessica Lynn Harlow, Esquire, Law Clerk
Legal Journal
Court

passwords, user names and log in names as part of a discovery request by way of interrogatories or request for production of documents, as that issue is not before the Court at this time. Generally, this Court is of the view that a motion for this special type of discovery must be made with allegations of some threshold showing that the publicly accessible portions of any social networking site contain information that would suggest that further relevant postings are likely to be found by access to the non-public portions. See generally McCann v. Harleysville Insurance Company, 78 A.D.3d 1524 (N.Y.S.2d 2010). As noted herein and in Romano, a review of the publicly accessible portions of the Facebook and MySpace sites revealed relevant information, and thus, it was reasonable to expect that further evidence pertinent to the case would be found in the non-public portions of these sites. There must be some factual predicate for the examination of the non-public portions of social networking sites. So called “fishing expeditions” will not be authorized. 9 The present motion did not request access to deleted pages.
§ 9:9 Authenticating email, social media, web pages, text messages, instant messaging, electronic signatures

Laird C. Kirkpatrick


This paper can be downloaded free of charge from the Social Science Research Network:
http://ssrn.com/abstract=2540102
§ 9:9 Authenticating email, social media, web pages, text messages, instant messaging, electronic signatures

In the electronic communication era, email and web pages and social media, not to mention twitter and texting and Instant Messaging, have become increasingly important types of evidence.¹ Yet electronic evidence, because of the ease with which it can be created, altered, and manipulated, presents challenging issues of authentication.²

Email, text messages, instant messaging. Material of this sort is

¹D.C. Circuit: U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (referring to our “age of technology and computer use” in which email is a “normal and frequent” mechanism for the majority of us, including “the professional world”).

²See Jerry E. Smith, Email Evidence in the Age of Instant Communication: A View from the Bench, Address at ALI-ABA CLE Seminar on Evidence Issues
often proved by computer printout or electronic images. The evidentiary hurdles are minimal with respect to authenticating printouts as accurate copies. A witness who has seen the email or text message or instant message need only testify that a printout offered is an accurate reproduction.³ With printouts, and also with electronic images, the proponent can show the manner in which a computer makes the image or gathers the data and sends those data to a printer: Rule 901(b)(9) allows this form of authentication, authorizing a showing that a process “produces an accurate result.”⁴ A court may even take judicial notice of these processes. There is no Best Evidence problem with respect to printouts or electronic images, because Rule 1001(d) defines “original” to include “any printout—or other output readable by sight—if it accurately reflects the information.”⁵

Authenticating the email itself, or a text message or instant message, can also be simple, depending on the purpose for which it is offered. A witness can authenticate such material as having

³See discussion of Rule 901(b)(9) in § 9:20, infra.

⁴See discussion of Rule 901(b)(9) in § 9:20, infra.

⁵See discussion of Rule 1001(3) in § 10:9, infra.
been sent by the witness himself by identifying it as such.\footnote{Seventh Circuit: \textit{Fenje v. Feld}, 301 F. Supp. 2d 781, 809 (N.D. Ill. 2003), aff’d, 398 F.3d 620 (7th Cir. 2005) (can authenticate emails by “statements or other communications” from purported author “acknowledging” them).\textit{Mississippi:} \textit{Kearley v. State}, 843 So. 2d 66, 70 (Miss. App. 2002) (defendant admitted to sending emails).}

Similarly, one who receives an email, text message, or instant message, can authenticate it as having been received simply by so testifying, but of course it is another matter to prove the identity of the author of such an email, text or instant message.\footnote{Seventh Circuit: \textit{B.S. ex rel. Schneider v. Board of School Trustees}, 255 F. Supp. 2d 891, 893–894 (N.D. Ind. 2003) (affidavit of recipient is “acceptable method” of authentication).\textit{Mississippi:} \textit{Kearley v. State}, 843 So. 2d 66 (Miss. App. 2002) (in sexual battery trial, minor victim could authenticate emails from defendant).\textit{Texas:} \textit{Shea v. State}, 167 S.W.3d 98, 105 (Tex. App. 2005) (testimony of complainant that she received the emails).} Testimony by the recipient indicating receipt of such material satisfies Rule 901(b)(1) because it is testimony by a witness with knowledge “that an item is what it is claimed to be,” namely an email (or text or instant message) that the witness received.\footnote{Fifth Circuit: \textit{Middlebrook v. Anderson}, 2005 WL 350578 (N.D. Tex. 2005) (statements in defendant’s affidavit that he “did not intend” email messages to be viewed in a particular state was a concession that he sent them).\textit{Seventh Circuit:} \textit{Superhighway Consulting, Inc. v. Techwave, Inc.}, 1999 WL 1044870 (N.D. Ill. 1999) (production of email during discovery from party files justifies finding of authenticity).}

As indicated below, often the recipient can provide additional testimony that proves not only receipt of a particular email or text or instant message, but the source as well.

Particularly in civil litigation, the authenticity of such material can be established in pretrial discovery, including identification at a deposition, in an answer to an interrogatory, or in response to a request for admission. These mechanisms can often establish not only receipt of such material, but authorship, and these matters are sometimes accomplished in pretrial settings by informal means, even inadvertently, paving the way to admit the material at trial (or sometimes simply making the task of authentication easier by paving the way for a witness to testify that the matter was conceded)\footnote{See discussion of Rule 901(b) in § 9:3, supra. See generally Note, “God Mail”: Authentication and Admissibility of Electronic Mail in Federal Courts, 34 Am. Crim. L. Rev. 1387 (1997).}

The more difficult challenge is to establish authorship of emails, and of text messages and instant messages, where the purported author is unavailable or unable or unwilling to acknowledge the
point. Here the proponent must rely on other methods. Certainly testimony by a person who saw the purported author write and send such material would suffice. If the computer, or for that matter the cellphone or “android” from which such material was sent is owned by a particular person, was seized from that person’s possession, or there are other compelling circumstances linking the computer to that person, such facts may be enough to authenticate the material as having come from that person.

If it is a shared computer, or one to which others had access, additional evidence linking the purported author to the email seems essential. For example, proof that the person in question was the one using the computer when the message was sent should suffice to connect the message to that person. Particularly in criminal cases where establishing authorship, and where a jury may have to be persuaded beyond a reasonable doubt that the defendant was the author in order to convict him, prosecutors sometimes call technical witnesses who do a trace. For emails, an expert may rely on the coded Internet Protocol Address appearing in the email header and trace it back to the service provider who relayed the message and sometimes back to a particular computer, and electronic data can sometimes be authenticated by reference to metadata stored in documents and by “hashtags” used to encrypt data, and specifically by SHA (“secure hash algorithm”) or the MD5 algorithm.

If the email message was encrypted by means of a digital signature and was therefore only available to a receiver who had a private key or access to a public key, a technical expert should be called to explain the encryption process and establish the necessary linkages to authenticate the email.

The most common method of authenticating emails, text mes-
sages, and instant messages involves showing “appearance, contents, substance, internal patterns, or other distinctive characteristics . . . , taken together with all the circumstances,” which can suffice Rule 901(b)(4).  

*North Dakota*: State v. Thompson, 777 N.W.2d 617, 626 (N.D. 2010) (in trial of wife for assaulting husband, admitting her text messages to him with “profane and threatening language,” on circumstantial evidence that she wrote them, including proof of her phone number and fact that her “distinctive signature” showed on message; complainant testified that messages from her appeared on his phone labeled “Fr: Jen,” which appears on messages) (citing this Treatise).

*Pennsylvania*: In re F.P., 878 A.2d 91, 94–95 (Pa. Super. 2005) (distinguishing features in emails contributed to finding that they were authentic).


*D.C. Circuit*: U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (emails authenticated by distinctive characteristics, including actual email address containing the “@” symbol, name of the person connected to that address, name of senders and receiver in headers and bodies of email).

*Seventh Circuit*: Fenje v. Feld, 301 F. Supp. 2d 781, 810 (N.D. Ill. 2003), aff’d, 398 F.3d 620 (7th Cir. 2005) (emails authenticated by testimony that purported sender sent emails, source email address, matching that on purported sender’s letterhead, and content, which was consistent with other evidence).

*Eleventh Circuit*: U.S. v. Siddiqui, 235 F.3d 1318, 1322–1323 (11th Cir. 2000) (fact that alleged sender’s name and address appeared on email counts).


*Tenth Circuit*: U.S. v. Simpson, 152 F.3d 1241, 1250 (10th Cir. 1998) (admitting instant messaging chat on basis that person using name “Stavron” told officer his name was Simpson and gave street address; later exchanges indicated email address belonging to Simpson; pages near computer in home noted name, address, email address and phone number that officer gave in chat room).


*North Carolina*: State v. Wilkerson, 733 S.E.2d 181, 183–184 (N.C. App. 2012) (in robbery trial, admitting message sent from defendant’s cellphone and stored there referencing some of the stolen property found in his trunk).
toward the two as being sender and recipient, a course of conduct or dealing between two people that regularly employs emails, texts, or instant messages and showing that the material in question fits into that course of dealing, and connections between the person in question and the phone in question, coupled with other information about behavior as it relates to content.

The fact that a person's name appears in the header as the “sender” should not be enough to authenticate the email as being from that person, just as self-identification by a telephone caller is insufficient to authenticate the call as being from that person. However, self-identification can complement other authenticating factors such as circumstances, content, internal patterns and extrinsic evidence.

Stronger circumstantial evidence would be a showing that the actual email address, e.g., mailto:johndoe@aol.com, matches an account in that person’s name with the indicated internet service provider, although this is not necessarily sufficient by itself because it is not technically difficult to send an email message using another’s email address.

In most modern cases, courts have relied primarily on the content of the message as a basis for authenticating emails. If an email contains particularized information that only the purported sender is likely to know, this will authenticate the

---

17 *New York*: People v. Green, 2013 WL 3029447 (N.Y. App. Div. 2013) (in trial for rape and related offenses, admitting text messages from defendant to complainant, since content made no sense unless they were sent by him).

18 *Ohio*: State v. Huge, 2013 WL 2325637 (Ohio App. 2013) (in trial of father for killing his infant daughter, admitting text messages to victim’s mother on basis of her testimony that “texting was her normal means of communicating with” him, and that message had been sent by him and “saved to her phone”).

19 *Florida*: Symonette v. State, 100 So.3d 180 (Fla. App. 2012) (in robbery trial, admitting text messages apparently sent by defendant to driver of getaway car and by her to him; driver identified messages and context; they were also found on defendant’s phone, retrieved on his arrest).

20 See § 9:16, supra.

21 *Third Circuit*: Victaulic Co. v. Tieman, 499 F.3d 227, 236 (3d Cir. 2007) (error to take judicial notice of facts about plaintiff company based on website, which was not authenticated: anyone may purchase web address, so trade name in URL does not authenticate website: can only notice matters not subject to reasonable dispute).

email to the same extent that such knowledge would authenticate a written message.\textsuperscript{23} Obviously the more specialized or unique the information, the more such content tends to authenticate the message as being from a particular sender who has such knowledge.

Particularized content may include information about serial numbers, credit card numbers, ordering information, personal transactions, private communications, particular relationships, coded communications, and other types of private information, or at least information that is not known to the general public.\textsuperscript{24}

A common type of content used to authenticate is content given in reply to an earlier email message.\textsuperscript{25} An email purporting to be a reply to an earlier message sent to a particular person is likely to be authored by that person. Often an email message will include the message to which it is responding as an attachment or even in the body of the message. Even though it is possible that a reply is sent by a person other than the recipient of the original message, the danger is no greater here than for written messages.

Other circumstances that can be used to help authenticate an email include the fact that the purported sender promised to send an email to the recipient and one was later received, the fact that previous messages sent to a particular email address

---


\textsuperscript{24} See also Note, When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception to the Federal Rules of Evidence, 64 Fordham L. Rev. 2285 (1996).

\textsuperscript{25} See §§ 9:6 to 9:9, supra.

\textsuperscript{24} Eleventh Circuit: U.S. v. Siddiqui, 235 F.3d 1318, 1322 (11th Cir. 2000) (in trial for submitting fraudulent recommendations for National Science Foundation award, admitting emails from defendant; they showed knowledge of actions only he would have, apologized for things he had done, came from his email address, were signed with his nickname, and he made similar points in conversations thereafter).

\textsuperscript{25} Fifth Circuit: U.S. v. Barlow, 568 F.3d 215, 220 (5th Cir. 2009) (in trial for seeking sex with underage female, admitting chatroom log on testimony by freelance undercover agent posing as girl, indicating that transcripts “fairly and fully reproduced” chats between her, posing as Rebecca, and defendant; agent was the other participant in year-long “relationship” and had direct knowledge of chats and could authenticate chat log).


See discussion of the “reply doctrine” in § 9:7, supra.
reached the purported sender of the email in question, or the fact that actions were taken by the purported sender in response to emails sent to the purported sender's address, such as the shipping of merchandise. Many other circumstances count as well.

Emails can also be authenticated under Rule 901(b)(3), which authorizes “comparison with an authenticated specimen by an expert witness or the trier of fact.” Thus emails that are not clearly identifiable on their own can be authenticated by allowing the jury to compare them with specimens that have been previously authenticated. Even if an email is successfully authenticated, it is not admissible to prove the truth of its content unless an additional foundation is laid showing that it fits an exception to the hearsay rule. If the email is shown to be from a party opponent, this will ordinarily suffice to allow its introduction into evidence as an admission. An email forwarding another email may sometimes constitute an adoptive admission of the original email by the person forwarding it. In unusual circumstances, an email statement may qualify as a present sense impression or an excited utterance.

Emails, even if made in the course of business, do not necessar-

---

26Eleventh Circuit: U.S. v. Siddiqui, 235 F.3d 1318, 1322–1323 (11th Cir. 2000) (alleged sender had previously received email at that address).


28Tenth Circuit: U.S. v. Simpson, 152 F.3d 1241, 1249–1250 (10th Cir. 1998) (admitting printout of chat room discussion between defendant and undercover officer on proof that person calling himself “Stavron” gave officer his name as Simpson and his street address; later exchanges indicated email address belonging to him; pages found near computer in his home contained notation of name, street address, email address and phone number that officer gave in chat room).

29D.C. Circuit: U.S. v. Safavian, 435 F. Supp. 2d 36 (D.D.C. 2006) (can authenticate emails by comparing them with other emails that had been authenticated by content and distinctive characteristics).


31Ninth Circuit: Sea-Land Service, Inc. v. Lozen Intern., LLC., 285 F.3d 808, 821 (9th Cir. 2002) (employee of plaintiff “incorporated and adopted the contents” of an email message from another of plaintiff’s employees when she forwarded it to defendant with a cover note that “manifested an adoption or belief in the truth” of information contained in original email).

ily qualify for admission as business records. While emailed billing statements and similar records may qualify, routine personal and professional email communications, like routine written correspondence, often fail to satisfy the exception because they lack the regularity and systematic checking of information that justifies making business records an exception to the hearsay rule.

The procedures for authenticating printouts of online conversations in internet “chat rooms” are essentially the same as those for authenticating emails.

---


33 For a discussion of the application of the business records exception to email, see Note, When the Postman Beeps Twice: The Admissibility of Electronic Mail Under the Business Records Exception of the Federal Rules of Evidence, 64 Fordham L. Rev. 2285 (1996).

34 First Circuit: U.S. v. Ferber, 966 F. Supp. 90, 98 (D. Mass. 1997) (it may have been employee’s routine practice to make email records; there was not enough evidence that employer required such records; business records exception requires business duty to make and maintain records).

Ninth Circuit: Monotype Corp. PLC v. International Typeface Corp., 43 F.3d 443, 450 (9th Cir. 1994) (electronic documents may fit business records exception, but email is “far less of a systematic business activity than a monthly inventory printout” and is instead “an ongoing electronic message and retrieval system”).

35 Fifth Circuit: U.S. v. Barlow, 568 F.3d 215 (5th Cir. 2009) (transcripts of “chat log” of conversations between agent and defendant authenticated by agent’s testimony that they were accurate).

Ninth Circuit: U.S. v. Tank, 200 F.3d 627, 629–631 (9th Cir. 2000) (in T’s trial for sexual exploitation, from transactions in Internet chat room called the Orchid Club, where members trade digital child porn, admitting logs kept on R’s computer; R was a club member and he deleted “nonsexual conversations and extraneous material, such as date and time stamps,” but remainder of logs implicated T; reviewing court rejects claim that changes might have introduced “undetectable material alterations,” since R explained how he created logs, and they “appeared to be an accurate representation” of conversations; government connected logs with T by showing he used screen name “Cessna” which appeared in printouts of logs).


Eleventh Circuit: U.S. v. Lanzon, 639 F.3d 1293, 1301 (11th Cir. 2011) (in sex offense trial, admitting instant message transcripts where detective testified that he participated in online chats and transcripts were accurate).
Web pages. It was only a matter of time before courts were asked to consider the matter of authenticating internet web pages (or websites) and web postings. Clearly such material is subject to the authentication requirement, and authenticating such material can be a matter of some difficulty. Particularly in the case of private websites, authenticating proof is necessary, although government websites appear to be self-authenticating under Rule 902(5) as a publication “purporting to be issued by a public authority.”

Just as a phone call can sometimes be authenticated by proof that the calling party “dialed” the number assigned by the phone company to another, coupled usually with proof that the ensuing conversation was the sort of conversation that would go forward if the caller got the intended number, it is usually sufficient to show that a web surfer looked up a particular person or company in a directory or found it by using a search engine, and went to that site and was able to place an order or conduct business that would be expected at such a site. Although these questions are just now beginning to appear, it is clear that authentication should be required in this setting.

Some of the early judicial opinions indicated extreme skepticism toward this form of evidence. One court described the Internet as “one large catalyst for rumor, innuendo, and misinformation” and suggested that there is a presumption that information discovered on the Internet is “inherently untrustworthy.” Other decisions have been more receptive and approving. There is no reason why evidence from websites should

---


Eighth Circuit: Fraserside IP LLC v. Netvertising Ltd., 902 F.Supp.2d 1165, 1179 n2 (N.D. Iowa 2012) (private websites are not self-authenticating; must produce some statement or affidavit by person with knowledge).

37Hawaii: Child Enفورcement Agency v. MSH, 2013 WL 1829647 (the “.gov” internet domain generally denotes a website administered by a government entity, and as such it is self-authenticating under Rule 902(5)).


39Fifth Circuit: St. Clair v. Johnn’s Oyster & Shrimp, Inc., 76 F.Supp. 2d 773, 774–775 (S.D. Tex. 1999) (some look to Internet as innovative vehicle for communication, but court “warily and wearily” views it as “catalyst for rumor, innuendo, and misinformation,” which provides “no way of verifying the authenticity” of contentions plaintiff wishes to use in response to defense mo-
not be admissible for certain purposes, provided it has been adequately authenticated.

Website postings may have particular value when offered against the owner of the website, for example, as an admission by that party or for a nonhearsay purpose such as establishing the price of a product, representations to induce a sale, the terms of a contract, or a warranty.

To authenticate a printout of a web page, the proponent must offer evidence that: (1) the printout accurately reflects the computer image of the web page as of a specified date; (2) the website where the posting appears is owned or controlled by a particular person or entity; and (3) the authorship of the web posting is reasonably attributable to that person or entity. Evidence that may corroborate these points could include testimony of others who saw the posting on the website, continuation of the posting on the website so that it is available to be seen by the court, or evidence that the party to whom the posting is attributed made similar postings or published the same information elsewhere. Some services take “snapshots” of websites as they appeared on particular dates and store that information in an archive. The testimony of an expert familiar with how those services work may be sufficient to authenticate an image purporting to depict the appearance of a website on a date in question.

---

40 Ninth Circuit: Perfect 10, Inc. v. Cybernet Ventures, Inc., 213 F. Supp. 2d 1146, 1154 (C.D. Cal. 2002) (in copyright case, declarations that printouts were “true and correct” copies of internet pages, “in combination with circumstantial indicia of authenticity (such as the dates and web addresses)” would support reasonable juror belief that documents are what proponent claims).

Ohio: See Johnson-Wooldridge v. Wooldridge, 2001 WL 838986, *4 (Ohio App. 2001) (party who printed documents from a website “could have authenticated the documents himself via an affidavit or through his own testimony”).


Third Court: U.S. v. Bansal, 663 F.3d 634, 667 (3d Cir. 2011) (in drug conspiracy case, admitting screenshots of defendant’s online pharmacy operation where government obtained images from company that maintained “Wayback Machine,” a historical database of all internet websites, and witness testified about operation and reliability of company’s operations, and stated that
If authorship or responsibility for the web posting cannot be sufficiently established, exclusion will normally be required. If the web posting is offered for the truth of what it asserts, it is necessary to lay an additional foundation to admit it under an exception to the hearsay rule. A distinction must of course be drawn between authenticating a web posting as being from a particular person and offering it to prove the truth of any assertions it contains. In the case of admissions, these issues conflate. If the web posting is adequately authenticated as being from a party opponent, it normally will be admissible as an admission. If the web posting is by a third party and is offered for its truth, an additional foundation is necessary to admit it as an exception to the hearsay rule.

In the case of government-maintained websites, courts are divided on whether information posted thereon is admissible to

screenshots were authentic based on comparison with previously authenticated and admitted images from defendant’s website).

Seventh Circuit: Telewizja Polska USA, Inc. v. Echostar Satellite Corp., 65 Fed. R. Evid. Serv. 673 (N.D. Ill. 2004) (noting that while such archiving technology does not fall within any of the examples listed in Rule 901, there was no evidence that it was unreliable or biased; and holding that the affidavit of an expert affiliated with an archiving company was sufficient to authenticate an exhibit purporting to depict a website as of a particular date).

Eighth Circuit: Jones v. National American University, 608 F.3d 1039, 1045–46, 257 Ed. Law Rep. 866, 82 Rule Serv. 1236 (8th Cir. 2010) (online employment advertisements authenticated by testimony from (a) university president that he was familiar with employment section of university’s website, and that advertisements offered by plaintiff were in same format of web postings, and (b) university employees that they had seen advertisement for director of admissions position) (authentication was sufficient even though posting differed in format from other advertisements and author was not identified).

Seventh Circuit: U.S. v. Jackson, 208 F.3d 633, 638 (7th Cir. 2000) (in trial for defrauding UPS by suggesting that African-American artwork had been damaged by white supremacist group when defendant did it, purported web pages of white supremacist group taking credit were not authenticated; defendant was savvy computer user and made no showing that pages were posted by supremacist group rather than defendant herself).


Wady v. Provident Life and Accident Ins. Co. of America, 216 F. Supp. 2d 1060, 1064–65 (C.D. Cal. 2002) (postings from defendant’s website not authenticated; proponent could not establish who maintained website or authorship or accuracy of contents).

prove the matter asserted, with some allowing\textsuperscript{44} and some rejecting such evidence.\textsuperscript{45} The resolution of this issue should depend on the reasons for the existence of the government website. If its purpose is to function as the equivalent of an official government publication, properly authenticated web postings should be admissible under Rule 902(5).\textsuperscript{46}

Electronic signatures. Because so much commerce is now in electronic form, Congress passed the Electronic Signatures in Global and National Commerce Act (E-Sign) in 2000.\textsuperscript{47} The Act provides that in transactions affecting interstate or foreign commerce “a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form” and the contract itself may not be denied legal effect “solely because an electronic signature or electronic record was used in its formation.”\textsuperscript{48}

The Act has broad effect in affirming the legal status of a wide variety of records in electronic format, including business records, public records, and insurance documents.\textsuperscript{49} It authorizes the retention of records in electronic form under a variety of existing statutes that require record retention.\textsuperscript{50}

The Act defines an electronic signature as “an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person


Washington: State v. Davis, 10 P.3d 977, 1009–1010 (Wash. 2000) (printout from state website on population statistics was not self-authenticating official publication; did not satisfy public records exception).

\textsuperscript{46}Sannes v. Jeff Wyler Chevrolet, Inc., 1999 WL 33313134, n3 (S.D. Ohio 1999) (press release on FTCs website was self-authenticating official publication).


\textsuperscript{49}15 U.S.C.A. § 7001(i) (noting intent that statute apply to insurance).

\textsuperscript{50}15 U.S.C.A. § 7001(d).
with the intent to sign the record.” However, there is no specified procedure for authenticating such signatures in a court proceeding, and other provisions of the Act give little guidance on this point. The Act provides that where law requires a signature under oath to be notarized, acknowledged, or otherwise made under oath, that requirement is satisfied “if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.” However, the electronic signature of the notary or person administering the oath will also need to be authenticated.

Because there are so many potential forms of electronic signature, the authentication methods must necessarily vary with the type of signature used. Certainly a party can authenticate that party's own signature under Rule 901(b)(1), as can a knowledgeable witness who observed the signing or has another basis for recognizing the signature. Sometimes a signature can be authenticated by the out-of-court admissions of the purported signer and admitted under Rule 801(d)(2). It may be possible to authenticate an electronic signature under Rule 901(b)(3) by having an expert witness or even the trier of fact compare it to a specimen which has been authenticated.

In some cases, the signature can be authenticated by its “appearance, contents, substance, internal patterns, or other distinctive characteristics . . . , taken together with all the circumstances” under Rule 901(b)(4). Electronic signature systems sometimes use verification technologies that might fall within this section. Much as with email authentication, electronic signatures might be authenticated by particularized information that only the purported signer is likely to know, in the form of a verification password (e.g., a deceased pet's name or mother's maiden name) that must be entered before the signature is accepted. Similarly, some technologies may require that a user provide personal information that can then be checked indepen-

52 The Secretary of Commerce is instructed to promote the use and acceptance of electronic signatures on an international basis in accordance with principles that “[p]ermit parties to a transaction to determine the appropriate authentication technologies and implementation models for their transactions, with assurance that those technologies and implementation models will be recognized and enforced” and to “[t]ake a nondiscriminatory approach to electronic signatures and authentication methods from other jurisdictions.” 15 U.S.C.A. § 7031.
dently to confirm the signer's identity, such as credit card information. Other technologies might employ an email to the signer's email address that requires a response before the signature is accepted; a reply from an email address known to be used by the purported signer may be used to authenticate a signature.

In some cases, the electronic signature may be a sound rather than an image, and a tape of the sound may be used to demonstrate the digitally produced sound. A witness would then need to identify the sound as one establishing the signature on the document offered.

In many cases writings at issue in litigation that rely on electronic signatures will be signed and sent using encryption technology. In such cases a technical witness is necessary who should be able to authenticate the signature by explaining the process of cryptography and the specific procedures that were used with respect to the electronic communication at issue.54

*Social media.* Modern cases have increasingly faced the question whether evidence from social media (Facebook, MySpace, Twitter, and others) should be admitted. Authentication issues resemble those found with other forms of electronic communication, but one distinguishing factor is that social media often involve postings that are accessible to large numbers of people, and sometimes to the entire world. It is uncertain whether social media accounts are more easily hacked than email accounts, but obvious concerns about security of social media arise, and it may well be that more people have both motive and access to social media, which heightens concerns over security and possibly malicious and fraudulent postings. The Maryland Supreme Court observed that “authentication concerns attendant to emails, instant messaging, and text messages differ significantly from those involving a MySpace profile and posting printout, because such correspondence is sent directly from one party to an

---

54 The process requires a public key and a private key. Each is a unique mathematical algorithm maintained by a “certification authority,” who is a neutral third party. The signer encrypts the message with a private key, sends it to the recipient, who uses a public key to decode the message. If the document is forged or altered, the keys will not function. Use of digital signature technology is specifically provided for by the Uniform Electronic Transactions Act, which has been adopted by a number of states. See, e.g., Kan. Stat. Ann. § 16-1602.

intended recipient or recipients, rather than published for all to see.”

As with other forms of electronic communication, the challenge is usually not in proving that a particular communication was received or posted, and the concern is rather in learning the identity of the sender or maker. A mere showing that the message was sent from a particular account or posted on a particular web page is not necessarily sufficient to authenticate the message as being from the owner of that account or web page, and more should be shown to establish the identity of the person posting the message, such as evidence that the originating site has security features that tend to assure the identity of the source.

The authentication method most commonly used by proponents of social media evidence is to demonstrate its distinctive characteristics. Under Rule 902(4) the proponent must show that the circumstantial evidence of the case combined with the “appearance, contents, substance, internal patterns, or other distinctive characteristics” of the exhibit are sufficient to prove that the proffered evidence is what it is purported to be. A distinctive characteristic particularly likely to persuade a court that the

---

55Maryland: Griffin v. Maryland, 19 A.3d 415, 426 n.13 (Md. 2011).
56First Circuit: Massachusetts v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010) (while foundational testimony showed that the messages “were sent by someone with access to [defendant's] MySpace Web page, it did not identify the person who actually sent the communication”).
Second Circuit: Connecticut v. Eleck, 23 A.3d 818, 824–25 (Conn. App. Ct. 2011) (witness claimed her Facebook account had been hacked, highlighting “the general lack of security of the medium” and raising the question “whether a third party may have sent the messages via [the witness's] account”),
Maryland: Griffin v. State, 19 A.3d 415, 421–422 (Md. 2011) (in homicide trial, error to admit posting on MySpace site: it said “snitches get stitches,” and was attributed to defendant’s girlfriend: anyone can establish such a site; people can set up fake accounts in the name of another, and possibility of fabrication or tampering “poses significant challenge”) (reversing).
57First Circuit: Massachusetts v. Williams, 926 N.E.2d 1162, 1172 (Mass. 2010) (excluding MySpace messages allegedly from defendant: there was no testimony on the security of such a Web Page, or “who can access a MySpace Web page, whether codes are needed for such access,” and no expert testimony indicated that only defendant could communicate from that page).
authentication requirement is satisfied is the use of code words known only to the parties.\textsuperscript{58}

Circumstantial evidence varies significantly from case to case, and courts apply different levels of scrutiny when determining whether the authentication threshold has been satisfied. Some courts have applied a strict standard\textsuperscript{59} and others a more lenient one.\textsuperscript{60}

If the proponent calls an authenticating witness to testify how a particular electronic communication is made, such as an expert from the company sponsoring the social media site, that person must be able to “provide factual specificity about the process by which the electronically stored information is created, acquired, maintained, and preserved without alteration or change, or the process by which it is produced if the result of a system or process that does so.”\textsuperscript{61} Courts have held, however, that it is not es-

\textsuperscript{58} \textit{Sixth Circuit}: Ohio v. Bell, 882 N.E. 2d 502, 512 (Ohio Ct. Com. Pl. 2008) (MySpace messages contained code words known only to defendant and his alleged victims).

\textsuperscript{59} \textit{Second Circuit}: Connecticut v. Eleck, 23 A.3d 818, 824–25 (Conn. App. Ct. 2011) (witness claimed her Facebook account had been hacked, which highlights “the general lack of security of the medium and raises an issue as to whether a third party may have sent the messages via [the witness’s] account”), \textit{New York}: State v. Lenihan, 911 N.Y.S.2d 588, 591–592 (N.Y. App. Div. 2010) (MySpace photographs downloaded by defendant’s mother and offered to impeach witnesses were not authenticated, given ease of editing photos on a computer).

\textsuperscript{60} \textit{Third Circuit}: In re F.P., 878 A.2d 91, 95 (Pa. Super. Ct. 2005) (admitting text messages; no need for heightened scrutiny for electronic evidence; “same uncertainties” exist with traditional written documents as they do with electronic evidence; “a signature can be forged; a letter can by typed on another’s typewriter; distinct letterhead stationery can be copied or stolen”)

\textit{Sixth Circuit}: Ohio v. Bell, 882 N.E.2d 502, 512 (Ohio Ct. Com. Pl. 2008) (there is a possibility that evidence from a social media site could be incomplete, altered or posted by a third party who hacked into the user’s account, but those issues “touch upon concerns regarding the weight of given evidence and not its authenticity”).

\textit{Texas}: Tienda v. State, 358 S.W.3d 633 (Tex. App. 2012) (in homicide trial arising out of shootout, admitting MySpace pages in which defendant presented violent self-image, on basis of testimony describing the creation of MySpace accounts, linking them to defendant through nicknames and photographs and zipcodes and references to events).

Sixth Circuit: Dockery v. Dockery, 2009 WL 3486662 (Tenn. Ct. App. 2009) (calling “representative from MySpace was not a prerequisite” to admitting printouts of exchanged messages).
Trial lawyers who use social media such as Facebook, Twitter, LinkedIn, and Instagram to pick out jurors now have the American Bar Association’s stamp of approval.

The ABA released formal opinion 466, which allows lawyers to review jurors’ Internet presence. It’s not anything new for most attorneys, but the recently released opinion ethically allows attorneys to do this in the courtroom.

Social media is just another tool in the shed for Columbus attorney Steve Chappelear.

“We learn something when we are in the courtroom, and we can look at them and hear them and we can ask them questions, but now we can get some background information and learn more about what bias or prejudices they may bring to a case,” Chappelear said.

Chappelear said the ABA opinion makes sense. It allows lawyers to use social media if the information is already public, but it doesn’t let attorneys “friend” a potential juror.

“It’s a good common sense approach, which protects the privacy of individuals. It eliminates the ability of lawyers to go in and use fraud or artifice to pretend to be someone else,” Chappelear said.

Chappelear said most jurors don’t even know attorneys look at their social media profiles.

“Frankly we don’t want to leave footprints because prospective jurors are – I suspect – not excited about the idea that lawyers are looking them up before a trial,” Chappelear said.

Case in point – potential jurors Brandi Jennings and Jonathan Samuel. The two were not selected for a jury trial during their week-long stint in Columbus, but just found out that their Facebook and Twitter accounts could’ve been used during their selection process.

“It didn’t cross my mind that they would look at Facebook or anything like that,” Jennings said. “It would make me feel some type of way – like why did they pick me from looking at my social media pages? What did I put out there to make them want me to be on the jury?”

Samuel said people should be mindful of their posts.
“You should be aware that there are a lot of different entities that can look at your Facebook, your Twitter, your Instagram,” Samuel said. “That’s personal responsibility. You’ve got to know ‘hey, what I’m posting right now can be seen by other people,’ so that’s your personal fault if you put something on there and you don’t want other people to see it … you’ve got to be careful.”

Chappelear said people can avoid all this just by adjusting their privacy settings.

“If you want to restrict it to just your true friends – fine, that’s easy enough to do – otherwise it’s all fair game for lawyers during the jury selection process,” Chappelear said.

http://www.courtnewsohio.gov/happening/2014/ABASocialMedia_100114.asp#.VR7YpWd0wuQ
Unless limited by law or court order, a lawyer may review a juror’s or potential juror’s Internet presence, which may include postings by the juror or potential juror in advance of and during a trial, but a lawyer may not communicate directly or through another with a juror or potential juror.

A lawyer may not, either personally or through another, send an access request to a juror’s electronic social media. An access request is a communication to a juror asking the juror for information that the juror has not made public and that would be the type of ex parte communication prohibited by Model Rule 3.5(b).

The fact that a juror or a potential juror may become aware that a lawyer is reviewing his Internet presence when a network setting notifies the juror of such does not constitute a communication from the lawyer in violation of Rule 3.5(b).

In the course of reviewing a juror’s or potential juror’s Internet presence, if a lawyer discovers evidence of juror or potential juror misconduct that is criminal or fraudulent, the lawyer must take reasonable remedial measures including, if necessary, disclosure to the tribunal.

The Committee has been asked whether a lawyer who represents a client in a matter that will be tried to a jury may review the jurors’ or potential jurors’ presence on the Internet leading up to and during trial, and, if so, what ethical obligations the lawyer might have regarding information discovered during the review.

Juror Internet Presence

Jurors may and often will have an Internet presence through electronic social media or websites. General public access to such will vary. For example, many blogs, websites, and other electronic media are readily accessible by anyone who chooses to access them through the Internet. We will refer to these publicly accessible Internet media as “websites.”

For the purposes of this opinion, Internet-based social media sites that readily allow account-owner restrictions on access will be referred to as “electronic social media” or “ESM.” Examples of commonly used ESM at the time of this opinion include Facebook, MySpace, LinkedIn, and Twitter. Reference to a request to obtain access to

1. Unless there is reason to make a distinction, we will refer throughout this opinion to jurors as including both potential and prospective jurors and jurors who have been empaneled as members of a jury.
another’s ESM will be denoted as an “access request,” and a person who creates and maintains ESM will be denoted as a “subscriber.”

Depending on the privacy settings chosen by the ESM subscriber, some information posted on ESM sites might be available to the general public, making it similar to a website, while other information is available only to a fellow subscriber of a shared ESM service, or in some cases only to those whom the subscriber has granted access. Privacy settings allow the ESM subscriber to establish different degrees of protection for different categories of information, each of which can require specific permission to access. In general, a person who wishes to obtain access to these protected pages must send a request to the ESM subscriber asking for permission to do so. Access depends on the willingness of the subscriber to grant permission.

This opinion addresses three levels of lawyer review of juror Internet presence:

1. passive lawyer review of a juror’s website or ESM that is available without making an access request where the juror is unaware that a website or ESM has been reviewed;

2. active lawyer review where the lawyer requests access to the juror’s ESM; and

3. passive lawyer review where the juror becomes aware through a website or ESM feature of the identity of the viewer;

Trial Management and Jury Instructions

There is a strong public interest in identifying jurors who might be tainted by improper bias or prejudice. There is a related and equally strong public policy in preventing jurors from being approached ex parte by the parties to the case or their agents. Lawyers need to know where the line should be drawn between properly investigating jurors and improperly communicating with them. In today’s Internet-saturated world, the line is increasingly blurred.

2. The capabilities of ESM change frequently. The committee notes that this opinion does not address particular ESM capabilities that exist now or will exist in the future. For purposes of this opinion, key elements like the ability of a subscriber to control access to ESM or to identify third parties who review a subscriber’s ESM are considered generically.

3. While this Committee does not take a position on whether the standard of care for competent lawyer performance requires using Internet research to locate information about jurors that is relevant to the jury selection process, we are also mindful of the recent addition of Comment [8] to Model Rule 1.1. This comment explains that a lawyer “should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.” See also Johnson v. McCullough, 306 S.W.3d 551 (Mo. 2010) (lawyer must use “reasonable efforts” to find potential juror’s litigation history in Case.net, Missouri’s automated case management system); N. H. Bar Ass’n, Op. 2012-13/05 (lawyers “have a general duty to be aware of social media as a source of potentially useful information in litigation, to be competent to obtain that information directly or through an agent, and to know how to make effective use of that information in litigation”); Ass’n of the Bar of the City of N. Y. Comm. on Prof’l Ethics, Formal Op. 2012-2 (“Indeed, the standards of competence and diligence may require doing everything reasonably possible to learn about jurors who will sit in judgment on a case.”).
For this reason, we strongly encourage judges and lawyers to discuss the court’s expectations concerning lawyers reviewing juror presence on the Internet. A court order, whether in the form of a local rule, a standing order, or a case management order in a particular matter, will, in addition to the applicable Rules of Professional Conduct, govern the conduct of counsel.

Equally important, judges should consider advising jurors during the orientation process that their backgrounds will be of interest to the litigants and that the lawyers in the case may investigate their backgrounds, including review of their ESM and websites.4 If a judge believes it to be necessary, under the circumstances of a particular matter, to limit lawyers’ review of juror websites and ESM, including on ESM networks where it is possible or likely that the jurors will be notified that their ESM is being viewed, the judge should formally instruct the lawyers in the case concerning the court’s expectations.

Reviewing Juror Internet Presence

If there is no court order governing lawyers reviewing juror Internet presence, we look to the ABA Model Rules of Professional Conduct for relevant strictures and prohibitions. Model Rule 3.5 addresses communications with jurors before, during, and after trial, stating:

A lawyer shall not:

(a) seek to influence a judge, juror, prospective juror or other official by means prohibited by law;

(b) communicate ex parte with such a person during the proceeding unless authorized to do so by law or court order;

(c) communicate with a juror or prospective juror after discharge of the jury if:

(1) the communication is prohibited by law or court order;

(2) the juror has made known to the lawyer a desire not to communicate; or

(3) the communication involves misrepresentation, coercion, duress or harassment . . .

Under Model Rule 3.5(b), a lawyer may not communicate with a potential juror leading up to trial or any juror during trial unless authorized by law or court order. See, e.g., In re Holman, 286 S.E.2d 148 (S.C. 1982) (communicating with member of jury selected for trial of lawyer’s client was “serious crime” warranting disbarment).

4. Judges also may choose to work with local jury commissioners to ensure that jurors are advised during jury orientation that they may properly be investigated by lawyers in the case to which they are assigned. This investigation may include review of the potential juror’s Internet presence.
A lawyer may not do through the acts of another what the lawyer is prohibited from doing directly. Model Rule 8.4(a). See also In re Myers, 584 S.E.2d 357 (S.C. 2003) (improper for prosecutor to have a lay member of his “jury selection team” phone venire member’s home); cf. S.C. Ethics Op. 93-27 (1993) (lawyer “cannot avoid the proscription of the rule by using agents to communicate improperly” with prospective jurors).

Passive review of a juror’s website or ESM, that is available without making an access request, and of which the juror is unaware, does not violate Rule 3.5(b). In the world outside of the Internet, a lawyer or another, acting on the lawyer’s behalf, would not be engaging in an improper ex parte contact with a prospective juror by driving down the street where the prospective juror lives to observe the environs in order to glean publicly available information that could inform the lawyer’s jury-selection decisions. The mere act of observing that which is open to the public would not constitute a communicative act that violates Rule 3.5(b).

It is the view of the Committee that a lawyer may not personally, or through another, send an access request to a juror. An access request is an active review of the juror’s electronic social media by the lawyer and is a communication to a juror asking the juror for information that the juror has not made public. This would be the type of ex parte communication prohibited by Model Rule 3.5(b). This would be akin to driving down the juror’s street, stopping the car, getting out, and asking the juror for permission to look inside the juror’s house because the lawyer cannot see enough when just driving past.

Some ESM networks have a feature that allows the juror to identify fellow members of the same ESM network who have passively viewed the juror’s ESM. The details of how this is accomplished will vary from network to network, but the key feature that is

5. Or. State Bar Ass’n, Formal Op. 2013-189 (“Lawyer may access publicly available information [about juror, witness, and opposing party] on social networking website”); N.Y. Cnty. Lawyers Ass’n, Formal Op. 743 (2011) (lawyer may search juror’s “publicly available” webpages and ESM); Ass’n of the Bar of the City of N.Y. Comm. on Prof’l Ethics, supra note 3 (lawyer may use social media websites to research jurors); Ky. Bar Ass’n, Op. E-434 (2012) (“If the site is ‘public,’ and accessible to all, then there does not appear to be any ethics issue.”). See also N.Y. State Bar Ass’n, Advisory Op. 843 (2010) (“A lawyer representing a client in pending litigation may access the public pages of another party’s social networking website (such as Facebook or MySpace) for the purpose of obtaining possible impeachment material for use in the litigation”); Or. State Bar Ass’n, Formal Op. 2005-164 (“Accessing an adversary’s public Web [sic] site is no different from reading a magazine or purchasing a book written by that adversary”); N.H. Bar Ass’n, supra note 3 (viewing a Facebook user’s page or following on Twitter is not communication if pages are open to all members of that social media site); San Diego Cnty. Bar Legal Ethics Op. 2011-2 (opposing party’s public Facebook page may be viewed by lawyer).

6. See Or. State Bar Ass’n, supra note 5, fn. 2, (a “lawyer may not send a request to a juror to access non-public personal information on a social networking website, nor may a lawyer ask an agent to do so”); N.Y. Cnty. Lawyers Ass’n, supra note 5 (“Significant ethical concerns would be raised by sending a ‘friend request,’ attempting to connect via LinkedIn.com, signing up for an RSS feed for a juror’s blog, or ‘following’ a juror’s Twitter account”); Ass’n of the Bar of the City of N.Y. Comm. on Prof’l Ethics, supra note 3 (lawyer may not chat, message or send a “friend request” to a juror); Conn. Bar Ass’n, Informal Op. 2011-4 (friend request is a communication); Mo. Bar Ass’n, Informal Op. 2009-0003 (friend request is a communication pursuant to Rule 4.2). But see N.H. Bar Ass’n, supra note 3 (lawyer may request access to witness’s private ESM, but request must “correctly identify the lawyer . . . [and] . . . inform the witness of the lawyer’s involvement” in the matter); Phila. Bar Ass’n, Advisory Op. 2009-02 (lawyer may not use deception to secure access to witness’s private ESM, but may ask the witness “forthrightly” for access).
relevant to this opinion is that the juror-subscriber is able to determine not only that his ESM is being viewed, but also the identity of the viewer. This capability may be beyond the control of the reviewer because the notice to the subscriber is generated by the ESM network and is based on the identity profile of the subscriber who is a fellow member of the same ESM network.

Two recent ethics opinions have addressed this issue. The Association of the Bar of the City of New York Committee on Professional Ethics, in Formal Opinion 2012-2, concluded that a network-generated notice to the juror that the lawyer has reviewed the juror’s social media was a communication from the lawyer to a juror, albeit an indirect one generated by the ESM network. Citing the definition of “communication” from Black’s Law Dictionary (9th ed.) and other authority, the opinion concluded that the message identifying the ESM viewer was a communication because it entailed “the process of bringing an idea, information or knowledge to another’s perception—including the fact that they have been researched.” While the ABCNY Committee found that the communication would “constitute a prohibited communication if the attorney was aware that her actions” would send such a notice, the Committee took “no position on whether an inadvertent communication would be a violation of the Rules.” The New York County Lawyers’ Association Committee on Professional Ethics in Formal Opinion 743 agreed with ABCNY’s opinion and went further explaining, “If a juror becomes aware of an attorney’s efforts to see the juror’s profiles on websites, the contact may well consist of an impermissible communication, as it might tend to influence the juror’s conduct with respect to the trial.”

This Committee concludes that a lawyer who uses a shared ESM platform to passively view juror ESM under these circumstances does not communicate with the juror. The lawyer is not communicating with the juror; the ESM service is communicating with the juror based on a technical feature of the ESM. This is akin to a neighbor’s recognizing a lawyer’s car driving down the juror’s street and telling the juror that the lawyer had been seen driving down the street.

Discussion by the trial judge of the likely practice of trial lawyers reviewing juror ESM during the jury orientation process will dispel any juror misperception that a lawyer is acting improperly merely by viewing what the juror has revealed to all others on the same network.

While this Committee concludes that ESM-generated notice to a juror that a lawyer has reviewed the juror’s information is not communication from the lawyer to the juror, the Committee does make two additional recommendations to lawyers who decide to review juror social media. First, the Committee suggests that lawyers be aware of these automatic, subscriber-notification features. By accepting the terms of use, the subscriber-notification feature is not secret. As indicated by Rule 1.1, Comment 8, it is important for a lawyer to be current with technology. While many people simply click their agreement to the terms and conditions for use of an ESM network, a lawyer who uses an ESM network in his practice should review the terms and conditions, including privacy

7. Ass’n of the Bar of the City of N.Y. Comm. on Prof’l Ethics, supra, note 3.
8. N.Y. Cnty. Lawyers’ Ass’n, supra note 5.
features – which change frequently – prior to using such a network. And, as noted above, jurisdictions differ on issues that arise when a lawyer uses social media in his practice.

Second, Rule 4.4(a) prohibits lawyers from actions “that have no substantial purpose other than to embarrass, delay, or burden a third person . . .” Lawyers who review juror social media should ensure that their review is purposeful and not crafted to embarrass, delay, or burden the juror or the proceeding.

**Discovery of Juror Misconduct**

Increasingly, courts are instructing jurors in very explicit terms about the prohibition against using ESM to communicate about their jury service or the pending case and the prohibition against conducting personal research about the matter, including research on the Internet. These warnings come because jurors have discussed trial issues on ESM, solicited access to witnesses and litigants on ESM, not revealed relevant ESM connections during jury selection, and conducted personal research on the trial issues using the Internet.9

In 2009, the Court Administration and Case Management Committee of the Judicial Conference of the United States recommended a model jury instruction that is very specific about juror use of social media, mentioning many of the popular social media by name.10 The recommended instruction states in part:

> I know that many of you use cell phones, Blackberries, the internet and other tools of technology. You also must not talk to anyone at any time about this case or use these tools to communicate electronically with anyone about the case . . . You may not communicate with anyone about the case on your cell phone, through e-mail, Blackberry, iPhone, text messaging, or on Twitter, through any blog or website, including Facebook, Google+, My Space, LinkedIn, or YouTube. . . . I expect you will inform me as soon as you become aware of another juror’s violation of these instructions.

These same jury instructions were provided by both a federal district court and state criminal court judge during a three-year study on juries and social media. Their research found that “jury instructions are the most effective tool to mitigate the risk of juror misconduct through social media.”11 As a result, the authors recommend jury instruction on social media “early and often” and daily in lengthy trials.12

---

9. For a review of recent cases in which a juror used ESM to discuss trial proceedings and/or used the Internet to conduct private research, read Hon. Amy J. St. Eve et al., *More from the #Jury Box: The Latest on Juries and Social Media*, 12 Duke Law & Technology Review no. 1, 69-78 (2014), available at http://scholarship.law.duke.edu/cgi/viewcontent.cgi?article=1247&context=dltr.


11. *Id.* at 66.

12. *Id.* at 87.
Analyzing the approximately 8% of the jurors who admitted to being “tempted” to communicate about the case using social media, the judges found that the jurors chose not to talk or write about the case because of the specific jury instruction not to do so.

While juror misconduct via social media itself is not the subject of this Opinion, lawyers reviewing juror websites and ESM may become aware of misconduct. Model Rule 3.3 and its legislative history make it clear that a lawyer has an obligation to take remedial measures including, if necessary, informing the tribunal when the lawyer discovers that a juror has engaged in criminal or fraudulent conduct related to the proceeding. But the history is muddled concerning whether a lawyer has an affirmative obligation to act upon learning that a juror has engaged in improper conduct that falls short of being criminal or fraudulent.

Rule 3.3 was amended in 2002, pursuant to the ABA Ethics 2000 Commission’s proposal, to expand on a lawyer’s previous obligation to protect a tribunal from criminal or fraudulent conduct by the lawyer’s client to also include such conduct by any person. Model Rule 3.3(b) reads:

(b) A lawyer who represents a client in an adjudicative proceeding and who knows that a person intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding shall take reasonable remedial measures including, if necessary, disclosure to the tribunal.

Comment [12] to Rule 3.3 provides:

Lawyers have a special obligation to protect a tribunal against criminal or fraudulent conduct that undermines the integrity of the adjudicative process, such as bribing, intimidating or otherwise unlawfully communicating with a witness, juror, court official or other participant in the proceeding, unlawfully destroying or concealing documents or other evidence or failing to disclose information to the tribunal when required by law to do so. Thus, paragraph (b) requires a lawyer to take reasonable remedial measures, including disclosure if necessary, whenever the lawyer knows that a person, including the lawyer’s client, intends to engage, is engaging or has engaged in criminal or fraudulent conduct related to the proceeding.

Part of Ethics 2000’s stated intent when it amended Model Rule 3.3 was to incorporate provisions from Canon 7 of the ABA Model Code of Professional

---

Responsibility (Model Code) that had placed an affirmative duty upon a lawyer to notify the court upon learning of juror misconduct:

This new provision incorporates the substance of current paragraph (a)(2), as well as ABA Model Code of Professional Responsibility DR 7-102(B)(2) (“A lawyer who receives information clearly establishing that a person other than the client has perpetrated a fraud upon a tribunal shall promptly reveal the fraud to the tribunal”) and DR 7-108(G) (“A lawyer shall reveal promptly to the court improper conduct by a venireperson or juror, or by another toward a venireperson or juror or a member of the venireperson’s or juror’s family, of which the lawyer has knowledge”).

Reporter’s Explanation of Changes, Model Rule 3.3.14

However, the intent of the Ethics 2000 Commission expressed above to incorporate the substance of DR 7-108(G) in its new subsection (b) of Model Rule 3.3 was never carried out. Under the Model Code’s DR 7-108(G), a lawyer knowing of “improper conduct” by a juror or venireperson was required to report the matter to the tribunal. Under Rule 3.3(b), the lawyer’s obligation to act arises only when the juror or venireperson engages in conduct that is fraudulent or criminal.15 While improper conduct was not defined in the Model Code, it clearly imposes a broader duty to take remedial action than exists under the Model Rules. The Committee is constrained to provide guidance based upon the language of Rule 3.3(b) rather than any expressions of intent in the legislative history of that rule.

By passively viewing juror Internet presence, a lawyer may become aware of a juror’s conduct that is criminal or fraudulent, in which case, Model Rule 3.3(b) requires the lawyer to take remedial measures including, if necessary, reporting the matter to the court. But the lawyer may also become aware of juror conduct that violates court instructions to the jury but does not rise to the level of criminal or fraudulent conduct, and Rule 3.3(b) does not prescribe what the lawyer must do in that situation. While considerations of questions of law are outside the scope of the Committee’s authority, applicable law might treat such juror activity as conduct that triggers a lawyer’s duty to take remedial action including, if necessary, reporting the juror’s conduct to the court under current Model Rule 3.3(b).16


15. Compare MODEL RULES OF PROF’L CONDUCT R. 3.3(b) (2002) to N.Y. RULES OF PROF’L CONDUCT, R. 3.5(d) (2013) (“a lawyer shall reveal promptly to the court improper conduct by a member of the venire or a juror….”).

16. See, e.g., U.S. v. Juror Number One, 866 F.Supp.2d 442 (E.D. Pa. 2011) (failure to follow jury instructions and emailing other jurors about case results in criminal contempt). The use of criminal contempt remedies for disregarding jury instructions is not confined to improper juror use of ESM. U.S. v. Rowe, 906 F.2d 654 (11th Cir. 1990) (juror held in contempt, fined, and dismissed from jury for violating court order to refrain from discussing the case with other jurors until after jury instructions delivered).
While any Internet postings about the case by a juror during trial may violate court instructions, the obligation of a lawyer to take action will depend on the lawyer’s assessment of those postings in light of court instructions and the elements of the crime of contempt or other applicable criminal statutes. For example, innocuous postings about jury service, such as the quality of the food served at lunch, may be contrary to judicial instructions, but fall short of conduct that would warrant the extreme response of finding a juror in criminal contempt. A lawyer’s affirmative duty to act is triggered only when the juror’s known conduct is criminal or fraudulent, including conduct that is criminally contemptuous of court instructions. The materiality of juror Internet communications to the integrity of the trial will likely be a consideration in determining whether the juror has acted criminally or fraudulently. The remedial duty flowing from known criminal or fraudulent juror conduct is triggered by knowledge of the conduct and is not preempted by a lawyer’s belief that the court will not choose to address the conduct as a crime or fraud.

Conclusion

In sum, a lawyer may passively review a juror’s public presence on the Internet, but may not communicate with a juror. Requesting access to a private area on a juror’s ESM is communication within this framework.

The fact that a juror or a potential juror may become aware that the lawyer is reviewing his Internet presence when an ESM network setting notifies the juror of such review does not constitute a communication from the lawyer in violation of Rule 3.5(b).

If a lawyer discovers criminal or fraudulent conduct by a juror related to the proceeding, the lawyer must take reasonable remedial measures including, if necessary, disclosure to the tribunal.