

**TRAPPED BY THE WEB:  
USING SOCIAL NETWORKING SITES TO  
INVESTIGATE WORKERS' COMPENSATION CLAIMS**

*William Craft, San Jose*

Defendants often wonder about the real lives of applicants, and whether the applicants' injuries and symptoms are legitimate. What if an adjuster could glimpse into a world where an applicant with a claimed knee injury told all of his friends about an all-day Yosemite Hike complete with pictures? What if an applicant who claimed she could not be around crowds went to three house parties over the weekend? Thanks to the new wave of social networking on the internet, it has become possible to see where an applicant spends his time, what activities he participates in, and more.

MySpace, Facebook, Twitter and Foursquare are the some of the biggest social networking sites on the Internet. These sites allow people to share intimate details of their daily lives with friends and family via the World Wide Web. People post status updates on these sites with everything from what they had for dinner, to how much fun they had at Mardi Gras this year.

Because these sites provide intimate information about people's lives based on their own statements, the information can be very useful in legal investigations. Investigators have entered the online profiles of litigants to determine whether statements made during legal proceedings are consistent with their diary-like Facebook postings.

**What is a Social Networking Site?**

With most social networking sites, the user creates a profile where he is able to "post" information that can be viewed by other internet users. The information typically includes general information such as: town of residence, date of birth, relationship status, and employer. The user can then update his profile with recent activities and can even post pictures.

Take Facebook, for example. A user can post new information on his "wall" or comment on information a friend has posted. This creates a network of communication between Facebook users where information is exchanged about different events by many different people.

Other social networking sites offer similar features with some unique differences. Twitter allows the user to "tweet" his or her current status using only 140 characters. This allows the user to post a small amount of information, also known as "microblogging." Users typically post the same information they would on Facebook.

Most sites allow users to "link" their profiles with those of other sites. Linking allows a user to post information on one site and have that post appear on all of his or her other social networking profiles.

**Are Posts Private?**

When information posted online is accessible to the general public, the opposing party investigating the claim may freely discover that information.<sup>1</sup> Thus, if an applicant posts information on Facebook or MySpace that can be viewed without permission from the applicant, that information can be obtained by the defense and used in court.

### **How Do You Use Social Networking Sites to Investigate Claims?**

Every social networking site has a search engine built into the site itself, where one can search to see if a particular person uses that site. It is helpful not only to have the applicant's name, but also his city of residence and date of birth. If you are not sure which site to start with, a general "Google" search may help find the sites used by a particular person. Again, to make sure the results actually pertain to the applicant in question, it would be wise to use more than just a name.

Information regarding an applicant's social networking usage can be obtained during deposition. The deposing attorney may seek information from the applicant such as his email address and social networking sites used regularly. However, asking for such direct information may tip off the applicant or his attorney to your intent to investigate online profiles. The applicant may then be more careful about his social networking postings. Discretion in this regard is required. The most helpful information to identify the applicant online is his email address. This can generally be obtained at deposition in the guise of a routine question.

### **Can Web Information Be Used In Workers' Compensation Cases?**

An applicant's subjective physical or emotional complaints often affect the amount of benefits received. As such, a major issue in most cases is determining the validity of his complaints. The applicant's statements are often the only source of evidence regarding how the injury occurred and the resulting disability. Thus, the injured worker's credibility is always at issue. It is not uncommon for an applicant to exaggerate symptoms during a deposition, or when discussing his injury with a physician. Therefore, objective evidence of the applicant's true abilities is crucial to the defense of a case.

### **Mrs. Wenneker's Wild Weekend**

Recently, the Workers' Compensation Appeals Board granted a Petition for Removal based on information obtained from an applicant's online comments, which potentially contradicted her trial testimony. In *Wenneker v. County of Contra Costa, et. al.*,<sup>2</sup> applicant claimed both orthopedic and psychiatric disability. Ms. Wenneker testified at trial that her hands were useless due to constant numbness and pain, and that her neck pain was "horrible" and hurt 24 hours a day. Ms. Wenneker even brought a pillow to court, using it to keep her arms extended and to lie down during a break in the trial. Ms. Wenneker also testified that she does not drive because the

---

<sup>1</sup> See 18 U.S.C. section 2511(2)(g).

<sup>2</sup> ADJ2954617 (12/17/09).

vibrations affect her neck and arms.<sup>3</sup> As for her psychiatric claim, Ms. Wenneker testified at trial that she suffered panic attacks around people and noise. Moreover, she testified that she does not leave her room for weeks at a time, does not see anyone, and does not socialize.

After trial, Defendants petitioned for removal based on information obtained from Ms. Wenneker's blog and her Twitter account. First, Ms. Wenneker posted information regarding a trip to Southern California to visit her daughter in 2007 on her blog, LAStarz. This directly contradicted trial testimony that her last trip to Southern California was in 2003. Second, Defendants discovered comments made online from after the trial, stating **"I won't be around much for the next 9 days or so," "I went to LA for the pre-Oscars festivities, then to New Orleans for a wicked and wild Mardi Gras vacation,"** and later posted, **"it was a bangin, bared butts, boobalicious blast."**<sup>4</sup>

The Board granted Defendant's Petition for Removal, noting that "post trial surveillance evidence also may be admitted if it rebuts or impeaches an applicant's trial testimony regarding his or her physical limitations or the activities that he or she can perform."<sup>5</sup> The Board goes on to cite Labor Code section 5704, which states "an opportunity shall be given to produce evidence in rebuttal" and that "improper restrictions on the right to present evidence in rebuttal is a deprivation of the constitutional guaranty of due process."<sup>6</sup> The Board remanded the matter back to the WCJ for a new trial and decision on whether any, or all, of the evidence should be admitted.<sup>7</sup> Further, the Board ordered that, if any or all of the evidence is admitted, the matter should be taken off calendar to allow time for Defendants to serve the evidence on applicant and for applicant to obtain rebuttal evidence.

Although we do not know the outcome of *Wenneker* on remand, it appears from the Board's decision that evidence obtained from postings on blogs and Twitter can be admissible if offered as rebuttal evidence.

### ***Sub Rosa: Location, Location, Location***

In order to obtain surveillance footage of an applicant, the investigator has to know the applicant's current location. This predictably results in footage taken within a close proximity of locations known to the defense, such as the applicant's home and outside the doctor's offices. Of course, applicant attorneys are aware that these are the common locations for *sub rosa* investigations and advise clients accordingly. Thus, surveillance taken of an applicant when he or she least expects it would be the most revealing.

---

<sup>3</sup> *Id.* at 3.

<sup>4</sup> *Id.* at 5.

<sup>5</sup> *Id.* at 7 (citing *De La Rosa v. Workers' Comp. Appeals Bd.* (2004) 69 Cal.Comp.Cases 151 (writ den); *Weeishaar v. Workers' Comp. Appeals Bd.* (1996) 61 Cal.Comp.Cases 706 (writ den.)).

<sup>6</sup> *Id.* (citing *Pence v. Industrial Acc. Com.* (1965) 63 Cal.2d 48, 50-51; accord: *Heggin v. Workmen's Comp. Appeals Bd.* (1971) 4 Cal.3d 162, 175.).

<sup>7</sup> *Id.* at 9.

Luckily, one of the common practices on social networking sites is to post a current status, indicating current location and activities. This is common on sites such as Twitter and Facebook. Another site, currently not quite as popular as Twitter or Facebook, is Foursquare. Foursquare is specifically intended as a site to post one's current location and activities. Thus, finding an applicant on this site could give you a continuous stream of information regarding the applicant's location.

### **Making Friends and Influencing People**

While there is no legal or ethical concern when discovering publicly available information, most social networking sites allow users to set various levels of privacy for their online profile. For example, Facebook allows for three levels of privacy regarding who is allowed to see the information posted. These levels can be separately set for different pieces of information, such as pictures, wall posts, and comments. These three levels are "*Everyone*," "*Friends of Friends*," and "*Friends*." If a profile is set so that only Friends can view the page, an investigator will not be able to access the information posted without the permission from the owner of the profile. This requires that the person requesting access send a friend request, also known as "*friending*." If the request is accepted, the profile can be viewed by the investigator.

Thus, the question arises, what if an applicant has set his or her profile so that only "Friends" can view his or her posts? Can you send a Friend request hoping that the applicant will accept without scrutinizing who you are and what your intentions may be? While there are rules regarding investigation techniques in general, there are few authorities directly addressing these questions as they pertain to social networking.

The Philadelphia Bar Association issued a Decision in March 2009, finding that this type of friending would violate Pennsylvania Profession Conduct Rule 8.4 as it constitutes a "deceptive practice."

Further, the Decision found that the plaintiff's willingness to accept the friend request did not absolve the investigating attorney of the unethical practice, stating, "Deception is deception, regardless of the victim's awareness in her interactions on the internet and susceptibility to being deceived." The opinion further analogized this type of friending practice with video surveillance, finding that this would be more like using a hidden camera inside someone's home as opposed to taking video footage of them while they were in public.

California does not yet appear to have addressed this question as clearly as the Philadelphia Bar Association. However, current California laws and case precedent would suggest that the result would likely be similar.

In an analogous workers' compensation case, an investigator posed as a friend to an applicant, drank with him, then convinced him to go horseback riding. The California Supreme Court held: "The carrier should not profit from its own deceitful conduct. The investigators feigned

friendship and concealed their employer's identity [...]”<sup>8</sup> Clearly, actively deceitful behavior by an investigator, including gaining friendship under false pretenses is not appropriate for a Sub Rosa investigation.

### **Forced Entry: The Use of a Subpoena**

If an applicant has set strict privacy settings, and there is no legal way to friend him, it may be necessary to subpoena the records from the social networking site directly.<sup>9</sup> Social networking sites, such as Facebook, specifically allow information to be divulged pursuant to a subpoena.<sup>10</sup> However, the subpoena can be opposed by an applicant using the Stored Communications Act (SCA).<sup>11</sup> In general, the SCA “creates a set of Fourth Amendment-like privacy protections by statute, regulating the relationship between government investigators and service providers in possession of users’ private information.”<sup>12</sup>

There are very few cases discussing the applicability of the SCA to social networking sites. However, one recent case, *Buckley H. Crispin v. Christian Audigier Inc.*,<sup>13</sup> examined this issue and determined that the outcome turned on plaintiff’s privacy settings. In *Crispin*, the United States District Court, Central District of California, reviewed the trial court’s ruling on a motion to quash a subpoena requesting profile information and email messages from MySpace and Facebook.

The *Crispin* court first discussed the different types of Internet Service Providers (ISP) subject to the SCA and determined whether MySpace and Facebook fall under these categories. After an exhaustive review of the functions of both of these sites, the court determined that email type messages sent using MySpace and Facebook are “inherently private such that stored messages are not readily accessible to the general public.”<sup>14</sup> Thus, the portion of the subpoena requesting email messages sent using social networking sites was quashed. However, with respect to the request for Facebook wall postings and MySpace comments, the court found that there would have to be a determination of whether plaintiff’s privacy settings allowed access by the general

<sup>8</sup> *Redner v. Workmen’s Compensation Appeals Board*, 5 Cal. 3d 83 (1971).

<sup>9</sup> See Title 8 of the California Code of Regulations section 10532 and California Code of Civil Procedure section 1987.

<sup>10</sup> The Facebook terms of use state: “[...] we believe the sharing is permitted [...] when legally required to do so. For example: [...] To respond to legal requests and prevent harm. We may disclose information pursuant to subpoenas, court orders, or other requests (including criminal and civil matters) if we have a good faith belief that the response is required by law. [...] We may also share information when we have a good faith belief it is necessary to prevent fraud or other illegal activity, to prevent imminent bodily harm, or to protect ourselves and you from people violating our Statement of Rights and Responsibilities. This may include sharing information with other companies, lawyers, courts or other government entities.”

(<http://www.facebook.com/help/?safety=law#!/policy.php>)

<sup>11</sup> 18 U.S.C. sections 2701-11.

<sup>12</sup> Orin S. Kerr, *A User’s Guide to the Stored Communications Act, and a Legislator’s Guide to Amending It*, 72 Geo. Wash. L. Rev. 1208 (2004).

<sup>13</sup> *Buckley H. Crispin v. Christian Audigier, Inc.*, 2:09-cv-09509, in the U.S. District Court for the Central District of California.

<sup>14</sup> *Crispin* at 36.

public.<sup>15</sup> As such, the case was remanded to the trial court for further proceedings regarding plaintiff's privacy settings.

*Crispin* illustrates the importance of privacy settings when using social networking sites. As with friending, if the applicant has set his or her profile so that only "friends" may view his or her posts, even a subpoena may not allow the defense to access that information. The court does not go as far as to describe exactly what level of privacy set by the plaintiff would evoke the protection of the SCA.

Further, if the information is publicly available, a subpoena would not be necessary. However, what if posts were publicly available, but later deleted? In that event, it is likely a subpoena would be necessary since the information is no longer on the internet. The subpoena would likely be successful given that the information was publicly available when it was posted. This is in contrast to the situation discussed in *Crispin*, where the information may, or may not, have been publicly available from the start. If the information was never publicly available, the subpoena would likely be quashed pursuant to the SCA.

## **Conclusion**

Investigations using social networking sites can be a useful and inexpensive tool to investigate applicants regarding various aspects of his or her workers' compensation claim. Applicants will often post information online that he or she would otherwise have kept hidden from adjusters, attorneys or investigators. This information is often more useful than information obtained at deposition or medical examination due to its unguarded nature. However, these investigations must be conducted in accordance with current laws regulating legal investigations. Thus, when an applicant has elected to limit the availability of the posted information to his or her "friends," ethical and criminal restrictions must be considered when continuing the investigation.

---

<sup>15</sup> *Id.*