American Educational Institute, Inc.

CLAIMS LAW UPDATE

A SUPPLEMENT TO CLAIMS LAW COURSES IN CASUALTY, PROPERTY, WORKERS COMPENSATION, FRAUD INVESTIGATION AND AUTOMOBILE

Winter, 2013

PRE-TRIAL DISCOVERY AND SOCIAL NETWORKING

[Ref. Pleadings and Practice, Para. 3.02]

You are a claims professional handling a case in which the claimant alleges that he suffered permanent bodily injuries as a result of your insured's negligence. Counsel has been appointed to represent the insured and a routine discovery request has revealed that the claimant maintains a Facebook account. The claimant, however, has chosen to make his account private, meaning it cannot be viewed by the general Facebook community or the public at large. The claimant has restricted access to a few chosen friends and family members.

Your investigation has also revealed that the claimant's sister maintains a Facebook account that is open to the general Facebook community, and she has posted a photo of her and the claimant skiing. The photo appears to have been taken after the claimant's accident with the insured and directly contradicts his claim that he is totally disabled as a result of the accident.

Based on this photo, you instruct defense counsel to send a discovery request to the claimant, requesting him to voluntarily provide access to his Facebook page. The claimant, however, refuses to comply, arguing that even though Facebook is on the Internet, he has a reasonable expectation of privacy because access to the account is limited to chosen friends and family. At this point, the only recourse is to file a discovery motion with the court.

Before addressing how courts analyze social networking discovery requests, however, it is important to understand how these sites function and the effect of a federal law known as the Stored Communications Act.

HOW SOCIAL NETWORKING SITES OPERATE

In *Trail v. Lesko*, 2012 Pa. Dist. & Cnty. Dec. LEXIS 194 (Allegheny Co. Com. Pl. 2012) a Pennsylvania court provided a useful description of online social networking and a basic explanation of how social networking sites such as Facebook work. It's important to emphasize that Internet technology is constantly changing so the court's description of Facebook might not accurately depict precisely how Facebook operates today, but the court's summary is a useful framework for our discussion of the cases that follow. The court said:

Social networking sites are web-based services that allow individuals to construct a

> public or semi-public profile with a bounded system, choose from a list of other service users with whom they intend to share a connection, and navigate among those connections and those made by others within the system. Users create a unique user identity, establish relationships with others who have done the same, join communities of users who share connections, and exchange information among one another.

The Pennsylvania court went on to summarize how Facebook operates:

> Social networking sites like Facebook utilize "Web 2.0" technology, which allows users to create and edit content on a web page while interacting with other users simultaneously in real time. With respect to Facebook, an individual initially 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. Once a profile is established, the user is encouraged to connect with other Facebook users – so-called "Friends" – with whom they exchange limited access to their respective profile pages and the ability to post pictures, comments and other content thereon. Each time content is posted directly to a user's profile page, the recipient user has administrative capability to delete the offered content from his or her own profile.

The court also described a Facebook activity known as "tagging":

> In a departure from the control generally afforded a user over the content of his or her own profile page, Facebook employs a system whereby users may "tag" others in photographs and other content, thereby establishing a link from that content to the tagged user's profile page. For example, User A "tags" User B in the photo. Once tagged, the photo on User A's profile page will contain a link directing individuals to User B's profile. While User B's profile will indicate that he or she has been tagged in User A's photo, and the tagged photo will unwittingly appear among the pictures that User B has selected for publication on his or her own profile page.

The court went on to discuss tagging and user privacy, with the most significant point being that only the person who posted the photo has the power to completely remove it:

> A user who has been tagged has the ability to "untag" the photo and, by altering Facebook's default privacy settings, may restrict the class of individuals who are authorized to view the tagged content. However, even if untagged or otherwise restricted by our tagged user, the photo will be available for viewing on the page of the user who initially posted it. Only the user who posted the photo is able to remove it from the website altogether. Once a Friend posts a photo of our user, any Friends of the posting user, including our user (or opposing counsel armed with our user's login information) may peruse Friends' photos to locate any material, including unauthorized material.

Finally, the *Trail* court discussed the volume of information stored on Facebook and, most importantly, the mechanisms available to a user to restrict public access:

> The sheer volume of potentially relevant information is staggering. In the aggregate users collectively update their "statuses" (a short indication of what's on a user's mind at a given moment, posted to their own profile page) more than 60 million times

> each day. Individual users create on average 90 pieces of content every month (photos, status updates, comments or other posts) with fully half of all Facebook users accessing their individual profiles on a given day. Facebook users collectively upload 300 million photos to the site each day. ... Sites like Facebook collect and store "metadata" about their users, which might reveal more about an individual's use of the site, their Friends' identities, what a user saw on another user's profile, and may track a user's general Internet activity. All of this data is potentially discoverable under the proper circumstances.
>
> Not all information posted on Facebook by a user is universally public, viewable by anyone with an Internet connection or even all other Facebook subscribers. By adjusting Facebook's default privacy settings, each user is empowered to limit the classification of persons (and, in some cases, specific individuals) who are permitted access to a user's profile page and the content contained therein. Although some information is always considered public and accessible to everyone, other information is accessible only by those people to whom the user grants access, usually limited to the user's Friends or Friends of those Friends. Finally, users can exchange messages not unlike traditional email, which, like email, are only accessible to the sender and recipients.

Social media discovery issues typically arise from two similar situations. First, suppose a claimant alleges that he is completely disabled as the result of a car accident caused by the insured. The claimant has a social networking webpage and the public portions of that page state that the claimant is an avid skier. They also display photos of the claimant skiing that appear to have been taken after the claimant's accident with the insured. An investigator or attorney working on behalf of the insured sees these photographs and seeking evidence relevant to the insured's defense, wants to view the private portions of the claimant's account or those portions that the claimant has limited to his selected group of Friends. The legal issue is whether the insured or his representatives can access information stored on the claimant's account that the claimant deems to be private.

The second situation arises when the claimant's social networking profile is private and limited to the claimant's Friends, but one of the claimant's Friends has made his own profile page available to the general public. Now suppose that the claimant's Friend posts a photo of the claimant participating in a volleyball game during the time period the claimant contends that he was totally disabled and the insured, or an investigator or attorney acting on the insured's behalf, visits the Friend's webpage and sees this photo. Unlike the first example, the incriminating evidence was discovered on a Friend's page and not the claimant's profile page. In both situations, the investigator legally obtained incriminating evidence. And in both cases, the question is whether this will allow the investigator to access private portions of the claimant's account.

In most cases involving social networking discovery requests, the claimant will refuse access to the private aspects of his social networking account. Logically, one might expect that this information would be discoverable by simply subpoenaing the website itself. However, as will be discussed in more detail below, a federal law known as the Stored Communications Act makes obtaining information from websites such as Facebook extremely difficult.

THE SIGNIFICANCE OF THE STORED COMMUNICATIONS ACT

The Stored Communications Act (SCA), 18 USC § 2701, is part of a broader federal law known as the Electronic Communications Privacy Act. The SCA is significant because social networking sites have argued that, under the SCA, they are not required to respond to civil subpoenas and courts have agreed with this argument. A California appellate court provided a good explanation of how the

SCA works in *Juror Number One v. The Superior Court of Sacramento County*, 142 Cal. Rptr. 3d 151 (Cal. App. 2012):

> Congress passed the SCA as part of the Electronic Communications Privacy Act of 1986 ... to fill the gap in the protections afforded by the Fourth Amendment. As one commentator observed: The Fourth Amendment offers strong privacy protections for our homes in the physical world. Absent special circumstances, the government must first obtain a search warrant based on probable cause before searching a home for evidence of a crime. When we use a computer network such as the Internet, however, a user does not have a physical 'home,' nor really any private space at all. Instead, a user typically has a network account consisting of a block of computer storage that is owned by a network service provider, such as America Online or Comcast. Although a user may think of that storage space as a 'virtual home,' in fact that 'home' is really just a block of ones and zeros stored somewhere on somebody else's computer. This means that when we use the Internet we communicate with and through that remote computer to contact other computers. Our most private information ends up being sent to private third parties and held far away on remote network servers. ... The Fourth Amendment provides no protection for information voluntarily disclosed to a third party, such as an Internet service provider (ISP).
>
> To remedy the situation, the SCA creates a set of Fourth Amendment-like protections that limit both the government's ability to compel ISP's to disclose customer information and the ISP's ability to voluntarily disclose it. ... "The SCA reflects Congress's judgment that users have a legitimate interest in confidentiality of communications in electronic storage at a communications facility. Just as a trespass protects those who rent space from a commercial storage facility to hold sensitive documents, the SCA protects users whose electronic communications are in electronic storage with an ISP or other communications facility."

The SCA has an exception for criminal subpoenas but no such exception for civil subpoenas. Social networking sites have successfully argued that they are prohibited by the SCA from responding to civil subpoenas. If the SCA affords social networking sites protection from responding to civil subpoenas and the claimant refuses to voluntarily comply with discovery requests, how can information stored on these sites be obtained?

OBTAINING DISCOVERY OF SOCIAL NETWORKING INFORMATION

Courts that have considered this issue have held that under the proper circumstances, a website user can be compelled to provide information. Thus, if a claimant makes his physical or emotional well being an issue in a lawsuit, it is possible to compel the claimant to produce private photographs, e-mails, or documents that deal with the claimant's physical or emotional state and that are stored on the claimant's social networking sites.

Whether information on social networking sites is discoverable depends on the resolution of two legal issues. First, the party seeking the information must prove that it is relevant or show that it will lead to the discovery of relevant evidence. If the party seeking the information satisfies this requirement the second question becomes whether requiring the website user to provide the information is a violation of the user's privacy rights.

Generally, the first legal issue is the most critical. Most courts have ruled that once the first burden is satisfied any expectation of privacy with respect to information on social networking sites does not preclude the discovery of relevant information.

In *Romano v. Steelcase, Inc*., 907 N.Y.S. 2d 650 (N.Y. Sup. Ct. 2010), the plaintiff claimed she was permanently injured as the result of an accident caused by the defendant and that her injuries left her confined to her home. According to the defendant, however, the public portions of the plaintiff's MySpace and Facebook profiles revealed that the plaintiff had an active lifestyle and that she traveled to Florida and Pennsylvania during a time when her alleged injuries would have prevented travel. As a result, the defendant served a discovery request seeking "authorizations to obtain full access to and copies of Plaintiff's current and historical records/information on her Facebook and MySpace accounts." The plaintiff refused to comply. The issues before the court were whether the discovery request could lead to relevant evidence and whether allowing access to the plaintiff's private portion of her online accounts would violate the plaintiff's privacy. Regarding the first question, the court ruled in favor of the defendant:

> The information sought by the defendant regarding plaintiff's Facebook and MySpace accounts is both material and necessary to the defense of this action and/or could lead to admissible evidence. In this regard, it appears that plaintiff's public profile page on Facebook shows her smiling happily in a photograph outside the confines of her home despite her claim that she has sustained permanent injuries and is largely confined to her house and bed. In light of the fact that the public portions of Plaintiff's social networking sites contain material that is contrary to her claims and deposition testimony, there is a reasonable likelihood that the private portions of her sites may contain further evidence such as information with regard to her activities and enjoyment of life, all of which are material and relevant to the defense of this action.

On the issue of the plaintiff's privacy, the court held that her concerns were outweighed by the defendant's need for the information. While the issue of privacy and online social networking had not yet been addressed in New York, the court drew a comparison between social networking and e-mails, with respect to which the Second Circuit had already ruled there is no legitimate expectation of privacy when the e-mail reaches the recipient. The *Romano* court said:

> Indeed, as neither Facebook nor MySpace guarantee complete privacy, plaintiff has no legitimate reasonable expectation of privacy. In this regard, MySpace warns users not to forget that their profiles and MySpace forums are public spaces, and Facebook's privacy policy sets forth that: You post User Content ... on the Site at your own risk. Although we allow you to set privacy options that limit access to your pages, please be aware that no security measures are perfect or impenetrable. ...When you use Facebook, certain information you post or share with third parties (e.g., a friend or someone in your network), such as personal information, comments, messages, photos, videos ... may be shared with others in accordance with the privacy settings you select. All such sharing of information is done at your own risk. Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listing or other items, this information may become publicly available.

The New York court concluded that the plaintiff did not have a reasonable expectation of privacy because she knew that her information may become public. According to the court, the plaintiff consented that her personal information would be shared with others when she created the Facebook and MySpace accounts, notwithstanding her privacy settings. Moreover, there was no other way for the defendant to access the information and photographs that were on the social networking sites.

Zimmerman v. Weis Markets, Inc., 2011 Pa. Dist. & Cnty. Dec. LEXIS 187 (Northumberland Co. Com. Pl. 2011) involved a motion to compel disclosure and preservation of a plaintiff's Facebook and MySpace information. The plaintiff was an employee of a subcontractor of defendant

Weis Markets and was injured in a forklift accident while working at the defendant's warehouse. The plaintiff filed suit against the defendant, claiming that his left leg was permanently injured and scarred. During his deposition, the plaintiff contended that he stopped wearing shorts because he was embarrassed by the scar. The defendant, however, reviewed the public portions of the plaintiff's Facebook page and discovered that his interests included "bike stunts" and "ridin'." A review of his MySpace page revealed photos depicting the plaintiff with his motorcycle both before and after the accident, including photos of the plaintiff in shorts with the scar from the forklift accident clearly visible.

The defendant filed a motion to compel, seeking access to the non-public portions of the plaintiff's Facebook and MySpace pages to determine whether there was any other evidence relevant to the plaintiff's claim for damages. The plaintiff countered that his privacy interests outweighed the defendant's need for discovery of this material.

The Pennsylvania court, following the New York court's decision in *Romano*, ruled in favor of the defendant and held that disclosure of the requested information outweighed the plaintiff's privacy interests. The court said:

> 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.

The court was careful to restrict its ruling to the facts at hand, warning that "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." The court also ruled that its decision should not be construed as carte blanche entitlement to Facebook and MySpace passwords, user names, and log in names as part of discovery every time a personal injury plaintiff with an online social profile files suit. According to the court, there must be a threshold showing that relevant information exists in the non-public portions of the accounts.

In *Tompkins v. Detroit Metropolitan Airport*, 278 F.R.D. 387 (E.D. Mich. 2012), the court denied an overly broad discovery request relating to a claimant's Facebook account. The case involved a slip and fall at Detroit Metropolitan Airport. During discovery, the defendant requested the plaintiff to sign a release of records for her entire Facebook account, including those sections designated as being private and not available to the general public. The plaintiff objected and the defendant made a motion to the court, relying on the New York court's decision in *Romano* and a Pennsylvania case, *McMillen v. Hummingbird Speedway*, 2010 Pa. Dist. & Cnty. Dec. LEXIS 270 (Pa. Comm. Pl. 2010). The court began its discussion by analyzing these two cases:

> In both cases, the public profile Facebook pages contained information that was clearly inconsistent with the plaintiffs' claims of disabling injuries. In *McMillen*, the plaintiff alleged "substantial injuries, including possible permanent impairment, loss and impairment of general health, strength, and vitality, and inability to enjoy certain

> pleasures of life." However, the public portion of his Facebook account contained comments about his fishing trip and his attendance at the Daytona 500 race in Florida. In *Romano*, the plaintiff claimed that she had sustained permanent, serious injuries that caused her to be largely confined to her house and bed. The public portions of her Facebook and MySpace accounts showed that to the contrary, "she had an active lifestyle and [had] traveled to Florida and Pennsylvania during the time period she claims that her injuries prohibited such activity."

The *Tompkins* court then compared these cases to the discovery requests before it and concluded that the defendant failed to prove that the plaintiff's Facebook account would reveal relevant information. Ruling against the defendant and in favor of the plaintiff, the court discussed the importance of the relevancy standard and the shortcomings of the defendant's argument:

> I agree 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. Nevertheless, the Defendant does not have a generalized right to rummage at will through information that Plaintiff has limited from public view. Rather, consistent with Rule 26(b) and with the cases cited by both Plaintiff and Defendant, there must be a threshold showing that the requested information is reasonably calculated to lead to the discovery of admissible evidence. Otherwise, the Defendant would be allowed to engage in the proverbial fishing expedition, in the hope that there *might* be something of relevance in Plaintiff's Facebook account.
>
> The Defendant claims that the Plaintiff's public postings, as well as some surveillance photographs, show the relevance of the private postings. They do not. The public postings, attached to Defendant's motion as Exhibit B, are photographs showing the Plaintiff holding a very small dog and smiling, and standing with two other people at a birthday party in Florida. Unlike the situations in *McMillen* and *Romano*, these pictures are not inconsistent with Plaintiff's claim of injury or with the medical information she has provided. She does not claim that she is bed-ridden, or that she is incapable of leaving her house or participating in modest social activities. The dog in the photograph appears to weigh no more than five pounds and could be lifted with minimal effort.

Accordingly, the court ruled in favor of the plaintiff and denied the defendant's request to access the plaintiff's Facebook account.

CONCLUSION

The claims professional should be aware that the issue of whether information stored on social networking sites is discoverable is not limited to bodily injury claims. *Mackelprang v. Fidelity National Title Agency*, 2007 U.S. Dist. LEXIS 2379 (D. Nev. 2007) and *Equal Employment Opportunity Commission v. Simply Storage Management*, 2010 U.S. Dist. LEXIS 52766 (S.D. Ind. 2010) both involved emotional distress claims arising out of sexual harassment in the workplace. The analysis applied by these courts, however, was similar to the analysis used by other courts in bodily injury claims. Information stored on social networking sites is discoverable, even if the website user has made the information private, if the party seeking the information can prove that it is relevant or that access to the private portion of the website user's account would lead to the discovery of relevant information. If this burden is satisfied, most courts hold that the discovery of this information does not infringe on the website user's privacy rights, even if the information was not made available to the general public.