Help! My Employer is Stalking me on Facebook! Privacy in the Social Media Age.

By Ed Forman

June 1, 2017

To a certain extent, employers have always tried to monitor their employees' conduct outside of the workplace. Many employers require employees to disclose criminal charges or convictions. Further, employees are often required to refrain from conduct such as drug or alcohol abuse, or any other off-work conduct which might embarrass the company.

In the Workers' Compensation context, employers have frequently monitored their employees in the hope that they can show their claims are fraudulent. Although some are urban legends, we have all heard the stories of private investigators photographing employees working on their house or windsurfing while they were supposedly medically unable to work.

The advent of social media has made stalking employees far easier than it ever has been before. Rather than paying a private eye, employers can find out a good deal about their employees' non-work activities at the click of a mouse. There are even stories of employers requiring employees to provide them with their social media passwords as a condition of employment.

Claims of fraud discovered on social media are usually exaggerated and are frequently downright wrong – that windsurfing pic on Facebook could be three years old. Nevertheless, anyone who represents injured workers should be concerned about an unfortunate photo turning up at their next hearing. In addition to fraud concerns, social media posts may also tie employees to illegal activities such as drug use. This could jeopardize their employment, prejudice their claims, and potentially provide a defense to an employer under the 1995 Ohio Supreme Court case of *State ex rel. Louisiana-Pacific Corp. v. Industrial Commission*.

While some of these concerns can be addressed with a stern admonition to your client to not post anything she or he would not want their employer or mother to see, this is hardly a fool-proof method. Damaging information may have been published before you speak to your client, or your client may just refuse to listen to your sound advice and counsel.

If an employer is using social media information against your client, it is certainly fair to explore whether the employer obtained the media legally. Whether it is or is not generally boils down to whether your social media information is public or private in nature.

A good way to understand the legality of online snooping is to think of it in terms of a physical search. If you are on a public roadway or in your front yard visible from the street, you have no expectation of privacy. A private investigator has the right to follow your car or take pictures of you in your visible yard, because you are intentionally exposing yourself to public view.

It is not legal, however, to peek over your privacy fence or to come onto your property and look into your windows. This is because you have a right to privacy in areas that you reasonably expect to be private. If someone physically invades your private area, they may be subject to a civil suit for invasion of privacy, as well as criminal prosecution for trespassing. It is also important that you have taken steps to keep your private areas private, for example putting up curtains.

In the 2013 case of *Ehling v. Monmouth-Ocean Hosp. Serv. Corp.*, 872 F. Supp. 2d 373, a New Jersey Federal District Court found that social media accounts are internet service providers (ISP's) under the Federal Stored Communication Act, 18 U.S.C. § 2701, and thus are subject to that Act. With respect to sites like Facebook and MySpace, *Ehling* found that they are ISP's with respect both to private messages *and* "wall posts."

Under the FSCA, it is illegal to both intentionally access a facility through which an electronic communication service is provided without authorization *or* to intentionally exceed an authorization to access that facility. In addition to criminal penalties, the FSCA provides a civil action for anyone whose information is illegally accessed in section 18 U.S.C. § 2707. A plaintiff in an FSCA case may obtain actual damages or $1,000.00 per violation, whichever is greater, punitive damages, attorney fees, and costs.

Ehling, however, drew a distinction between private information stored by the ISP, which is protected by the FSCA, and public information which is not. Similar to the front lawn in the physical example above, a public social media account is likely fair game for employers. The Court held that "it strikes the Court as obvious that a claim to privacy is unavailable to someone who places information in an indisputably public medium, such as the internet, without taking any measures to protect the information."

With many social media sites, you have a good deal of control over what information about you is disclosed and who it is disclosed to. Facebook, for example, allows you to set your profile to public or private and to control the audience for various posts. A tremendous amount of people, however, have either a fully or partly public account, which means that information can be seen by anyone who has a Facebook account.

In addition to public accounts, social media information is typically shared with other users. Using the example of Facebook again, some or all information is shared with "friends," which probably includes some friends from work. Unsurprisingly, work friends from time to time willingly or unwillingly disclose your social media information to management.

A typical reaction to this is to point out that disclosing information to a friend is not the same thing as disclosing it to your boss, and this is very true. In *Ehling*, however, the Court found that once you voluntarily give your information to your friends they are free to do anything with it that they like, including giving it to your employer. *Ehling* requires that giving this information to any employer must be voluntary, without any coercion or pressure. Basically,

if your "friend" decides on their own to provide information to your employer, it is voluntary, but if your employer is going around asking if anyone has access to your social media account, this is coercion.

Coerced or underhanded access to social media information will likely violate the FSCA. In addition to requesting access from other employees, this would include setting up phony accounts or using the saved login data of either the employee in question or another employee.

Accessing social media data by any method can be very dangerous for an employer. This is in part caused by the fact that you are not just accessing the employee's information, but that of all her or his' friends and contacts which could well be deeply personal. While they have no right to privacy if the employee voluntarily discloses it, if you access it improperly you may be looking at a lawsuit from not one but potentially hundreds of people. It also has a significant yuk factor – I would not want to be in the position of arguing that because you required an employee to turn over their social media password as a condition of employment in case it was needed for "work reasons," that you therefore had the right to read private messages from their Aunt Judy in which she reveals she has breast cancer. Remember, exceeding authorization is just as bad as no authorization.

Further, in addition to the FSCA, Ohio law recognizes an invasion of privacy tort claim for the wrongful intrusion into one's private activities and for the publicizing of one's private affairs with which the public has no legitimate concern. This protection may actually be broader than the FSCA, and entitles a prevailing plaintiff to compensatory damages and potentially punitive damages.

Finally, reviewing social media accounts – even public accounts – can lead to other trouble. Pictures might reveal that an employee has a disability or is in an interracial relationship, which in the hands of the wrong manager could easily result in a lawsuit. You would not want to be in a position where an employee is terminated the day after a manager viewed a post in which an employee revealed that they were HIV positive.

In sum, in order to protect your clients, you need to be vigilant that their social media data is not being illegally obtained. Filing a workers' compensation claim is not an invitation to have your private information accessed and used against you. If employers are breaking the law, they need to be held accountable.

Ed Forman is an attorney with the Columbus law firm of Marshall and Forman LLC, where he works in the areas of employment and civil rights law. You can learn more about Ed and his practice at www.marshallforman.com.