Member's Quarterly Winter 2020 Edition

Feature

# Social Media Investigations in the Workplace

*Factors to consider before you launch*

**Brian Sartorelli**
*Pesident, CEO, IRM (Investigative Research Management)*

Social media investigations are becoming increasingly popular as an effective tool for conducting background investigations into potential hires, fraudulent Workplace Safety and Insurance Board (WSIB) cases and unexplained absenteeism in the workplace. Social media listening is also an effective means to monitor and detect risk and threat situations in the workplace. A detailed social media search can allow employers access to valuable information they would otherwise not have. In our connected society, people are accustomed to sharing intimate details of their daily lives on various social media platforms such as Facebook, Twitter or Instagram, to name a few. Moreover, they don't always appreciate the implications of this or the extent to which their posts can be viewed and recovered.

## Social media investigations as part of the hiring process

Intelligence-led investigations (gathering information prior to commencing physical surveillance) have not only improved investigation success rates, but also saved the employer money. Intelligence obtained through social media is an excellent example of this benefit.

Consider an applicant who has applied for a position within your firm. From all outward appearances, this individual appears to be an ideal candidate and there is nothing in the interview process or the applicant's resume that would indicate otherwise. However, during a pre-employment screening, a review of public social media accounts reveals numerous posts relating to drug use, hate speech or posts indicating that the applicant will call in sick in favour of camping with friends. This new information provides valuable insight and intelligence the client can utilize to make a more informed decision regarding the applicant's suitability.

Social media is also a useful tool when considering partnerships with other businesses or Request for Proposal (RFP) applicants. Negative reviews, lawsuits and information about financial status can be obtained through social media and open source intelligence investigations. With such critical intelligence available prior to the signing of a contract, there is less risk of partnering with someone who may have recently declared bankruptcy or been twice sued, for example.

## Utilizing social media intelligence for WSIB claims

Your organization has an employee who is currently on leave due to a workplace injury. After reviewing the employee's file, the client identified several red flags, such as:

- Subject is eager for a quick settlement
- Instant legal retention
- Injuries are inconsistent with the accident
- Subject has a long claims history
- Subject isn't available during work hours

Member's Quarterly Winter 2020 Edition

## Feature continued

- No witnesses to the accident
- Subject has unrealistic physical limitations
- Incident occurs parallel to news of layoff, termination or transfer.

After noting these red flags, the raw data would be provided to your investigative partners. Raw data is compiled from the original employment file and would include information such as the employee's address, phone number, date of birth, employment history, family status and the reported injury. After reviewing this data and ensuring it is accurate, certified OSINT professionals will commence an intelligence-led social media investigation by searching, analyzing and documenting public posts.

Historically, reviews of social media accounts have allowed professionals to locate detailed vacation logs, and uncovered the subject engaging in hobbies (such as hiking, surfing or skateboarding) while allegedly injured or pursuing alternative employment. Additionally, this intelligence may provide valuable clues as to when or where surveillance would be best conducted, based on the time the subject most frequently posted online.

### Using social media to investigate employee absenteeism

Social media investigations aren't only relevant to investigating employees on a claim. Employers may also consider reviewing the social media activities of staff who are frequently away from the workplace due to reported sickness or injuries. Professional social media investigations have unearthed various activities by employees who are supposed to be off sick, including hunting trips, Black Friday shopping as well as alcohol and drug dependencies.

Many individuals, HR and CEOs alike, check into the social media and report they have "done some digging". Several dangers present themselves through viewing a person's profiles without the proper training and tools, including: alerting the subject of the investigation; gathering potential evidence that is not in accordance with the rules of evidence; not documenting properly; jeopardizing future investigations or surveillance.

### Steps to take before conducting your own social media investigation

Before conducting your own investigation, it's important to consider if you're equipped to do so. Social media investigations should only be considered when using alias accounts and IP blockers. Digital footprints, such as code which cannot be controlled by the user, are often left behind during such explorations. If a subject becomes aware that their boss has recently been looking at their social media account, the investigation may be compromised before it begins. As such, it is of utmost importance that prior to conducting a social media review, you consult an experienced professional investigator.

In conclusion, billions of public social media posts provide an enormous amount of information that can be used to investigate most workplace scenarios. This investigation should be carried out with the utmost respect to one's personal expectation of privacy and conducted by trained professionals. Social media investigations will save employers thousands of dollars when conducted with caution and expertise.

*Brian Sartorelli is President and CEO of Investigative Risk Management and can be reached via email at brians@irmi.ca.*