Investigators warned about privacy rules in social media checks

Laws evolving as companies turn to web sites for information on employees

BY CHARLOTTE SANTRY
Law Times

The explosion of social media provides a wealth of digital material for fraud investigators to scrutinize, but the growing emphasis on privacy means an awareness of the rapidly evolving legal landscape is crucial.

At the Internal Investigations Forum held in Toronto on June 17, Alex Popovic, Sun Life Financial's associate vice president of enterprise investigations, said: "There are an increasing amount of limitations on what we can, or cannot, do in digital data."

In March 2013, the Supreme Court of Canada ruled that police must obtain a wiretap in order to seize text messages.

The court set the threshold for gaining authorization for an order at the "highest level of the spectrum," said Popovic.

He added: "We can infer that there will be a high standard when it comes to investigating communications, be it oral, written or digital."

Popovic trained as a lawyer before becoming an inspector with the Royal Canadian Mounted Police and then switching his attention to internal fraud investigations.

His company uses social media only if the person under investigation is aware of what it's doing. Even then, a limited number of trained individuals who are aware of the relevant regulations and laws will carry out the search.

He warned: "If your internal investigation is already set on a foundation that's very quaky, it may actually compound the issue that you have and you could end up being at the wrong end of an investigation or prosecution or litigation."

The 2012 case of *R. v. Cole* recognized an employee's reasonable expectation of privacy on a work computer. It involved a high school teacher whose laptop, issued by the school board, contained photos of a partially nude and underage female student. The judge found a violation of the teacher's rights when police conducted a warrantless search of the computer.

Even where searches are valid, confirming information on Facebook and Twitter can be problematic, said Popovic.

For example, people often use these platforms to boast and investigators must remember that someone else may have accessed their password. Investigators' misconceptions could also cause them to take status updates out of context.

In addition, some sites, such as LinkedIn, make covert surveillance difficult. "Be aware that many of those sites track you and will tell the owner that you've been there and it's quite visible and easy for them to see that you've been there," noted Popovic.

Investigators also need to be aware of another case seen as setting the tone for actions involving privacy and electronic information.

Jones v. Tsige dealt with a bank worker who accessed the financial records of her partner's ex-wife. The Ontario Court of Appeal found an invasion of the appellant's privacy and created the tort of intrusion upon seclusion in response.

The speed at which the laws are changing and gaining new interpretations is creating confusion, according to Popovic.

The lack of consensus over how to interpret some of these rulings was evident at the Canadian Corporate Counsel Association's spring conference when Lyndsay Wasser, a partner and employment lawyer at McMillan LLP, advised caution over searching job candidates' social media postings.

She later explained to *Law Times* that social media searches should only take place following a conditional offer of employment if the company has warned the candidates in advance. At the time, Brian Smeenk, a partner with Fasken Martineau DuMoulin LLP's labour, employment, and human rights group, said it was "preposterous" to suggest avoiding social media searches.

Employers, who reportedly face increased resumé fraud in a stagnant labour market, may greet Smeenk's advice with relief.

Employers can glean a lot of information just by asking probing, thoughtful questions at the interview stage, says Amanda McLachlan.

A survey by Britain's fraud prevention service found that employee fraud — including deception in the hunt for employment — increased by 40 per cent between 2012 and 2013, a period in which that country entered a double-dip recession.

Statistics Canada figures released two weeks ago reveal average monthly employment growth in the first six months of 2013 was nearly half of the activity seen in the previous six months. Could difficult market conditions lead to a jump in fraud cases in Canada that's similar to the experience in Britain?

"There's some suggestion that resumé fraud is on the rise, especially when there's a tough job market," says litigator Amanda McLachlan of Bennett Jones LLP. "There are certainly things that people can do."

While acknowledging the potential risks highlighted by Wasser and Popovic around carrying out social media searches, McLachlan says it's fine to check resumés against LinkedIn profiles in order to look for discrepancies.

However, employers can also glean a lot of information just by asking probing, thoughtful questions at the interview stage, she argues.

Past salaries can be difficult to prove beyond asking a former employer, McLachlan notes.

And perhaps surprisingly, she says it's also worth verifying voluntary work listed on a resumé, especially if it might give a candidate the edge over an equally qualified peer. "It's easy to mislead employers.... I don't think people check that much," she says.

Diligent background checks are even more important for high-profile appointments to roles in which employees will be privy to very sensitive information.

This issue arose recently in the case of Edward Snowden, the former CIA and National Security Agency employee who leaked details to the press about mass phone-tapping operations.

The external organization that screened Snowden for security clearance is currently under investigation for systematically failing to conduct thorough background checks.

There have been suggestions that officials should have picked up on the ideologies that led Snowden to blow the whistle sooner.

Private investigators will often delve into an individual's family background, credit history, and lifestyle.

The digital age can be a hindrance when it comes to probing someone's past, says Ron Wretham, one of the chief executive officers of Investigative Solutions Network Inc. "With the proliferation of the Internet, people are able to purchase false documents like high school diplomas, university degrees."

Increased labour mobility means employers take on staff from all over the world. It's important to ensure any global institutions have accreditation before tracking them down to check whether they issued documents attached to candidates' files, he adds.

Jim Downs, managing director of MKD International Inc., says privacy restrictions often seem to help wrongdoers rather than protect the public. Clients, he notes, need to know that potential hires who may be overseeing global business deals haven't struggled with money issues in the past or displayed inappropriate behaviour towards colleagues. "There's so much at stake, they want to make sure the person is what they report to be and has no baggage attached," he explains.

Beyond the recent legal decisions involving digital information, there are also strict rules governing surveillance. For example, current laws may classify a venue as private even if activities are taking place with the curtains wide open, says Downs.

Asked about the worst case he has come across in the course of investigating candidates for very well-remunerated, senior positions, he says: "If someone was standing in front of a schoolyard every day watching kids ... that's nice to know. That's not going to show on any document." **LT**