CYBER SNOOPING...
legitimate screening method, or a step too far?

In a recent survey conducted by Reppler, a social media monitoring service designed to help users manage their online image across different social networks, it is clear that more and more recruiters and HR professionals are screening candidates via social media.

Is this a legitimate screening method or simply cyber snooping?

Whether you believe it's right or not, the survey shows that 91% of the 300 recruiters surveyed confirmed that they screen prospective employees online, using FaceBook, Twitter and LinkedIn as their primary snooping grounds.

Interestingly, nearly half indicated that they would conduct the online search before considering bringing in the candidate and 69% admitted to rejecting a candidate based on their findings, making it even more critical that individuals hoping to secure new job opportunities maintain their social media profiles at all times.

The top reasons for rejecting candidates included:

- Inappropriate photos and comments, especially those alluding to drink/drug abuse
- Negative comments, or leaked information about a previous employer
- Admitted lying about qualifications, experience or other critical information

Of course, the tool also has had a positive impact with an equal number of respondents saying that they hired someone on the basis of their social media profile. In these cases, the primary motivating factors for hiring included:

- Positive impression of their personality/culture fit to the employer organisation
- Profile reaffirmed their professional traits including qualification, knowledge, skills and references

How do you ensure that you're working within the scope of the law?

If you, like the majority of recruiters, want to do as much vetting as possible on candidate, then you need to be sure that you do so within the bounds of the law and ethical practice. Below are 10 tips to help you.

1. **Only search public content.** Information that is available in the public domain may be reasonably accessed by anyone, including recruiters or potential employers. Never expect a candidate to provide access details to their social media profiles as this would definitely fall foul of ethical and legal requirements. In fact, due to the increasing number of employers expecting this of potential employees, a specific law forbidding this exact practice was recently passed in the US.
2. **Comply with terms of service for each social media site.** Just because the information is publicly accessible doesn't mean that you are legally entitled to use it. Do your research on the various sites' requirements and base your social media screening policy on this.
3. **Keep your "Ethics Radar" on.** All actions should be able to be held up to the highest ethical standards and the scrutiny of your client and candidate. It is, for example, never okay to try and conduct a search via the "back door" such as "friending" the person or joining their network for the sole intention of snooping.
4. **Search in a uniform manner.** If you're going to make this part of your recruitment screening process, be sure to do so uniformly for all candidates, including using the same search tools and canvassing the same sites.
5. **Develop a clear policy and procedure.** If you're going to do it, do it properly. Take on board the research into the various site requirements and document the policy and procedures you'd follow. This will ensure transparency, uniformity and mitigate risk.
6. **Notify candidates of your intention to search this way.** Give candidates the opportunity to update their profile settings to private and to understand the possible consequences of not doing so. It may be an idea to get their express permission to do so, as you would for other background checks during the process.
7. **Ensure that you have the right person.** As you can imagine there is a high chance of finding many "Joe Smith's" in cyberspace so before acting on any information you may find, be sure that this really is the "Joe Smith" you're considering for employment.
8. **Interrogate the information.** Not all information online is accurate or authentic, particularly if it has been posted by a third party. Before making any assumptions, consider the source of the information and other mitigating circumstances and be reasonable in your decision making as a result.
9. **Document the legitimate, non-discriminatory reasons for your hiring decisions,** especially if you employ cyber screening as part of your process. You need to ensure that you don't find yourself at the wrong end of a discrimination claim at the CCMA.
10. **Train your team.** If you expect individual recruiters to do this as part of their recruitment process, be extremely clear about your expectations. Set a policy and train your consultants on the acceptable way in which to do this so that you protect yourself.

While you're considering how your candidates would fare if screened, think about your own profiles. Perhaps it's a good time to re-assess your online persona and at least adjust your privacy settings.

How does Reppler work? Reppler helps to manage online image by showing users how they are perceived across social networks, by telling users the makeup of their social network connections, and by identifying any potential issues and risks. TrustedID's social media monitoring service is free and supports various social networking services, like Facebook, Twitter, and LinkedIn.