

Swaab Update: Social Media

JULY 2013

Our Meritas affiliate firm in Ohio, Kohrman Jackson & Krantz, brought to our attention the Ohio senate bill 45, which will prohibit employers “from requiring (a job) applicant or employee to provide access to private electronic accounts of the applicant or employee.” We have previously **commented** on the legal risks in Australia for employers and potential employees who might make this type of request or use information obtained as a result.

We conducted a survey of employees and employers to gain deeper insight in to how Australians feel about this issue and have compared the results with our friends in the USA. The following report outlines some of our key findings and insights in to this challenging area of technology in the workplace.

THE SURVEY

Our survey entitled *Do we need social media password privacy laws?* indicated that the majority of responding employers were not asking for login or password details of job applicants and also indicated that 90% of them have also not been asked for details themselves. Of those 10% of employers that had asked job applicants for their login details, two employers had not employed a job applicant when they refused to disclose their social media login details.

Two thirds of our respondents believed that regulation is not needed with regard to asking job applicants and employees for their social media login details. However, there is a move towards viewing the publicly accessible content of job applicant’s social media accounts.

We found it interesting to note that 62% of employers surveyed had said that they have viewed an employee’s social media posts, while another 55% of those surveyed believed that employees should have an expectation of privacy of their posts to social media.



LEGISLATIVE MOVES IN THE USA

There have been developments in the US around making it unlawful to require job applicants or employees to provide access to their private electronic accounts such as Facebook, Twitter or LinkedIn.

Currently, legislation making it unlawful to require employees or job applicants to provide login details has been passed by 28 states. There have also been moves to introduce Federal legislation to the same effect and a *Social Networking Online Protection Act* has been proposed.

These moves have been in response to concerns that employers are requesting access and if access is refused employers are then not hiring that particular job applicant. Issues of coercion and of maintaining privacy have led to a number of US states moving on the issue. Legislators have also been concerned that in the current depressed job climate employees with reduced bargaining power are more susceptible to employer demands.

Although no legislation exists in Australia there are legal risks for an employer (or potential employer) that requests or uses information obtained to make their decision. Legislative developments in the US may well lead to moves to regulate business activity in a similar way in Australia.



DO WE NEED SOCIAL MEDIA PASSWORD PRIVACY LAWS?

What can be seen publicly on social media from the “outside in” is often very different from what a contact (friend, follower, connection) or an individual user on the “inside” can see. When logged in to a social media account an individual can view their contacts, messages, commentary, and various other personal information that an outsider would not be able to view.

It is because of the more private nature of social media content which logged in users have access to that there has been concern about employers asking job applicants and employees for their social media login details. Some employers have evidently been motivated to view a job applicant or employee’s social media presence from the inside out.

This can be seen as a dangerous move. It is often a breach of the terms and conditions placed on social media users by social media platforms such as Facebook or LinkedIn to disclose their login details to third parties. Employers have, possibly unwittingly, been causing job applicants and employees to breach these terms and conditions.

The only plausible reason to seek an insider view of someone’s social media presence is to obtain personal information about that person. What employers do with that personal information will vary, however it is possible that finding certain personal information may influence them in hiring an applicant or terminating an employee.

Employers with a public profile and a recognisable brand need to consider the possible adverse publicity (frequently via social media) they may receive if they discriminate between job applicants on the basis of who provided personal social media access and who didn’t or what information they found upon being granted access.

SOCIAL MEDIA SURVEILLANCE AT WORK

Many employees in Australia are already under surveillance at work. This can include every key stroke they enter into their computers or other electronic equipment in addition to video camera recording of premises, telephone call recording, swipe card access recording, GPS tracking and many other surveillance techniques.

In New South Wales the *Workplace Surveillance Act 2005* (NSW) regulates these surveillance activities. Under the Act employees must be notified of any overt surveillance at least 14 days prior to the surveillance commencing. Notification must outline:

- the type of surveillance to be carried out (for example camera, computer, or tracking);
- how the surveillance will be carried out;
- when the surveillance will start;
- whether the surveillance will be continuous or intermittent; and
- whether the surveillance will be for a specified limited period or ongoing.

This requirement means that employment contracts and enterprise agreements now frequently contain workplace surveillance clauses notifying employees of surveillance in their workplace.

Computer surveillance is surveillance by means of software or other equipment that monitors or records the information input or output, or other use, of a computer including, the sending and receipt of emails and the accessing of internet websites. Under the Act there are two requirements for carrying out computer surveillance:

- Computer surveillance of an employee can only be carried out in accordance with a policy of the employer on computer surveillance of employees at work; and
- The employee must be notified in advance of the policy in a way which makes it reasonable to assume the employee is aware of and understands the policy.

WHAT SHOULD I TAKE AWAY?

Employers need to be aware of the difficulties in navigating social media, both in recruitment procedures and during employment. It is vital to ensure organisations have social media policies addressing these issues, especially when it comes to commentary by employees on social media.

Employees need to be aware of the consequences of social media posting and be prepared to respond to questions regarding access to their social media accounts by prospective or current employers.

Creating a workplace with a culture of respect, mutual confidence and clear employer expectations will help prevent social media issues getting out of hand.

AUTHORS



Naomi Messenger
SPECIAL COUNSEL

T + 61 2 9233 5544
E nkm@swaab.com.au



Amber Burgess
MARKETING & BUSINESS
DEVELOPMENT MANAGER

T + 61 2 9233 5544
E ajb@swaab.com.au

For media enquiries, please contact Amber Burgess.

US Commentary provided by Jonathan Hyman,
Partner, Kohrman Jackson & Krantz.

Level 1, 20 Hunter Street, SYDNEY NSW 2000
T +61 2 9233 5544 | F +61 2 9233 5400
E mail@swaab.com.au | W www.swaab.com.au