

Pre-employment steps protect company connections

20 April 2017 7:06am

Disputes about company information theft and LinkedIn connection ownership are rife, but can be prevented with steps taken early in the employment relationship, a law specialist says.

As social media continues to become an "all-encompassing workplace tool", developments in the area of who 'owns' assets such as LinkedIn contacts will be ongoing, and [Bespoke](#) special counsel **Ryan Solomons** predicts a landmark decision on the issue within two to three years.

HR, as "the gatekeeper" to employee conduct, expectations and obligations, has an important role to play in safeguarding the employer's intellectual and commercial property, he notes – the department should "set the scene" for employee obligations, maintain awareness, and monitor staff to ensure compliance.

"If they're on top of that, when things do go wrong and lawyers do get involved, if they've done their job right, then it's much easier for the lawyers to come in and do theirs."

An ex-employee's LinkedIn connections are "very unlikely" to qualify as trade secrets that belong to their former employer and can be legally defended as such, but there are other ways employers can protect their business-related social media connections, Solomons says.

He says the key is to act when an employee commences employment, by:

- incorporating restraint of trade clauses that explicitly refer to the use of social media connections into employment contracts, and including terms that restrict the use of an employee's social media profile (such as updating, publishing or sharing content) during the post-employment restraint period;
- instructing the employee to open a new premium LinkedIn account (which the employer will pay for and close at the conclusion of their employment);
- obtaining a list of the employee's current social media connections, and stipulating in the employment contract that connections gained during the course of employment are the employer's property; and
- developing robust guidelines and policies around the appropriate use of social media during employment and the post-employment restraint period, and providing training to ensure employees understand their obligations.

The challenges associated with protecting information on LinkedIn are heightened by a lack of case law to set precedent, Solomons says.

But the fact there are few rulings shouldn't cause HR professionals to dismiss the issue – it doesn't mean there aren't disputes in this area, only that they are often settled out of court, because parties lack the resources or drive to pursue litigation.

Some disputes have touched on the matter: a 2012 case saw an employer attempt to assert ownership of an employee's LinkedIn connections – but it [didn't proceed to judgment](#) – and a [2013 case](#) saw the Fair Work Commission accept that an employee who was sacked for using LinkedIn to solicit customers had breached his post-employment restraints – but the nature of LinkedIn connections, and whether they can be considered "confidential", was not discussed.

Meanwhile a [2013 case in the UK](#) saw the High Court of Justice order an ex-employee who managed LinkedIn groups on the company's behalf to hand over the account after accepting allegations it had been used for solicitation.

Related premium content

- [Stop LinkedIn contacts walking out the door with exiting employees](#)
- [How to navigate the legal risks of LinkedIn](#)
- [Employer out of pocket despite damages for IP breach](#)
- ["Patently unreasonable" restraint a lesson for HR](#)

Related content

- [Stop LinkedIn contacts walking out the door with exiting employees](#)
- [How to navigate the legal risks of LinkedIn](#)
- [Employer out of pocket despite damages for IP breach](#)
- ["Patently unreasonable" restraint a lesson for HR](#)