LexisNexis

Australian
Intellectual Property Law
Bulletin

2020 . Vol 32 No 9

Contents

Information contained in this newsletter is current as at February 2020

LexisNexis Butterworths

Australian
Intellectual Property Law
Bulletin

Who owns your online friendships? Establishing rights over social media connections

Stephanie McHugh *RUSSELL KENNEDY LAWYERS*

Introduction

When you now meet a new professional connection, you can share your personal LinkedIn QR "quick response" codes for reciprocal scanning and become social media connections in an instant. Such is the prevalence of social media in our lives — and increasingly in our professional careers. Many employees are actively encouraged to grow their employer's social media accounts — as well as their own social media presence, with some employers even funding external networking and "personal brand" training for their employees. In the client services industry, there is clear logic behind these types of investments. An employee with an engaging social media persona and large network can attract a greater client pool, which can be capitalised on at some future point to the benefit of an employer. However when an employment relationship sours, the extent to which an employer can own or exercise control over social media accounts and connections created during employment can be a critical issue.

Ownership of social media connections has been considered in cases globally — but no Australian court has yet ruled definitively on the issue. While we wait for judicial guidance, there are a number of proactive steps employers can take if they consider that employees' social media connections are valuable to the business and worth protecting.

Protecting client contact details

When an employment relationship ends, an employee is free to compete with their former employer. From a public policy perspective, employers should not be able to prevent "mere competition" in the absence of a valid contractual restraint. Yet employees are subject to duties of confidentiality in both common law and equity, and have long been prohibited from disclosing or misusing their employer's confidential information or trade secrets obtained during the course of their employment.

In *Wright v Gasweld Pty Ltd*,[1] the following five factors were provided as key considerations in determining whether information is properly classified as "confidential":

- the fact that skill and effort were expended to acquire the information
- the fact that the information is jealously guarded by the employer, is not readily made available to employees and could not, without considerable effort or risk, be acquired by others
- the fact that it was plainly known to the employee that the material was regarded by the employer as confidential
- the fact that the usages and practices of the industry support the assertion of confidentiality, and
- the fact that the employee in question has been permitted to share the information only by reason of seniority or high responsibility within the employer's organisation

A departing employee may not take customer or client lists — or otherwise deliberately memorise them — for use in a competing role after their employment ends.[2] In *Forkserve Pty Ltd v Jack*,[3] the New South Wales Supreme Court held that business cards containing names and telephone numbers, taken by an employee who resigned to set up a competing business, did not constitute a confidential client list.[4] The court noted that employees were not instructed by their employer to obtain clients' business cards and that their retention was not subject to any confidentiality agreement.

Conversely, in *NP Generations Pty Ltd v Feneley*,[5] the South Australian Supreme Court ruled that an employee who kept an address book with the contact details of her employer's clients was obliged to hand over that information when her employment ended. The address book in that case was prepared by the employee during the course of employment using the employer's "rent roll", which listed details of the owners of rental properties the employer managed. The court noted that the address book was compiled directly from the "rent roll" and was treated as confidential by other employees.

Because of this, it could only be used for the legitimate purposes for which it was created during employment, but not for any other purposes after the employment ended.

But what about virtual "client lists" in the form of social media connections? Can an employer exploit an employee's social media connections if they can be properly characterised as confidential information?

What does the case law say?

United States

In the United States case of *Eagle v Morgan*,[6] Dr Linda Eagle, a founder of a company called Edcomm, created a personal LinkedIn account using her work e-mail address.

When Eagle's employment was terminated, Edcomm accessed her LinkedIn account, changed the password and updated the account with details of the new CEO. LinkedIn later stepped in and gave access back to Eagle, who sued her former employer for misappropriation of identity among other causes of action.

Edcomm was of the view that they owned LinkedIn accounts created with Edcomm email addresses at their direction and during working hours. They had urged employees to create LinkedIn accounts and developed social media content guidelines, but the court noted that Edcomm did not require their employees to have LinkedIn account and did not pay for employees' accounts. In finding for Eagle in her claim for misappropriation of identity (but awarding zero dollars for compensatory damages), it was of significance that no policy had been introduced informing employees that their LinkedIn accounts were the property of Edcomm.

In *Christou v Beatport LLC*,[7] the court went so far as to accept that a list of MySpace friends constituted a trade secret. This position differs from an earlier decision in *Sasqua Group Inc v Courtney*,[8] where it was held that because client details listed in a recruitment database were also available to the public via Facebook and LinkedIn, the information in the database could not properly be considered a trade secret. In that case, the departing employee (who was not subject to any contractual restraints) did not take the client database with her, but contacted individuals after the termination of her employment by conducting Google, Facebook and LinkedIn searches to obtain their details.

United Kingdom

The primary decision in the United Kingdom on ownership of social media connections is *Hays Specialist Recruitment (Holdings) Ltd v Ions*,[9] which was an application by Hays for pre-action disclosure. Mr Ions left Hays to set up a competing recruitment business and it was revealed that, while still employed by Hays, Ions invited at least two recruitment candidates to be his connections on LinkedIn. Hays believed that Ions used confidential client contact details to invite candidates to join his network, with the intention of later leveraging those connections in his new business. The High Court said:[10]

> This is not a case of a former employee remembering some contact details after the termination of his employment. The transfer to his network occurred during his employment and the list was such that he could not recreate it once he deleted it.

Ions was ordered to disclose to Hays communications with LinkedIn connections he made in his capacity as a Hays employee.

In *Whitmar Publications Ltd v Gamage*,[11] another High Court case decided 5 years after *Hays*, three employees resigned to set up a competing publications business. Whitmar alleged the employees misappropriated confidential information. One specific accusation was that one of the employees, Ms Wright, refused to provide Whitmar with the user name and password of four LinkedIn groups she managed on behalf of Whitmar as part of her duties. In managing the groups, Wright used Whitmar's computers and it was noted that she did not have a computer at her home. Sometime after the employees resigned, it appeared the LinkedIn groups were used to invite individuals to an event of the new business. The court held that the LinkedIn groups operated for Whitmar's benefit and promoted its business.

Whitmar sought various forms of relief, including an injunction to restrain the use of its confidential information, delivery up of its confidential information and a limited forensic inspection of the employees' computers, which was granted by the court.

Australia

No Australian court has yet made a definitive ruling on the question of social media connection (or account) ownership. The issue was raised, however, in *Naiman Clarke Pty Ltd v Tuccia*.[12] Ms Tuccia was employed by Naiman Clarke as a legal recruiter and when she left to work for a competitor it was alleged that, while employed by Naiman Clarke, she used a spreadsheet containing names of lawyers who had dealt with her employer to connect with them on LinkedIn and later used those connections in her new role.

Naiman Clarke argued that the information in the spreadsheet was confidential information and that by making LinkedIn connections from the spreadsheet and then engaging with those connections in her new role, Tuccia breached the confidentiality provisions in her employment agreement and under the general law.

Naiman Clarke sought a variety of remedies including an injunction requiring Tuccia to delete the relevant connections from her LinkedIn profile.

This case was ultimately discontinued, without the court making an explicit finding as to the ownership of the connections. Had this case progressed to a decision, it would have been the first time this issue was fully considered in Australia.

According to the court in the 2017 decision of *Sprout Network Pty Ltd v Roth*,[13] since the names and email addresses of specific clients were freely available on the internet, those contact details were "not really confidential at all". In that case, Sprout Network sought interlocutory relief against a former employee who set up a competing business and emailed clients, many which were already his LinkedIn connections, encouraging them to contact him through LinkedIn.

The court said that the employee likely had the names and email address of the clients in his memory through his extensive dealings with them over the years, and it was significant that the employee was never expressly told that the names and email address of the clients constituted confidential information.

Case law takeaways

From the cases across the United Kingdom, United States and Australia, it appears that relevant factors may include whether:

- the employer has directed the employee to create the social media account
- the social media account is created using a business email address
- connections are made with clients of an employer during the course of employment
- the employer has told the employee that certain connections will constitute the employer's confidential information
- the employer paid for the employee's social media account
- client contact details are readily available to the public on the internet, and
- the contact details could be remembered after the termination of employment

LinkedIn's position

By signing up to join LinkedIn, a user is deemed to accept the terms of LinkedIn's User Agreement.[14] Clause 8.2(e) prohibits users from disclosing information without consent, and provides an example of disclosing the confidential information of an employer.

Clause 2.2 of the User Agreement makes clear that:

> As between you and others (including your employer), your account belongs to you. However, if the Services were purchased by another party for you to use (e.g. Recruiter seat bought by your employer), the party paying for such Service has the right to control access to and get reports on your use of such paid Service; however, they do not have rights to your personal account.

By expressly stating that an employee's account will not belong to their employer, LinkedIn appears to be weighing into the debate over social media account and connection ownership. However the qualifier relating to circumstances where paid services are used adds another level of complexity to the issue. It is unclear whether this also applies if an employer pays for their employee to use LinkedIn Premium — which is available on a fee-paying subscription basis and gives subscribers access to enhanced features on LinkedIn. For employees who use this service, LinkedIn recommends that employees file an expense report with their employer after they receive a purchase receipt. It remains to be seen whether reimbursing an employee who has paid for a LinkedIn Premium service will be sufficient to entitle employers to have access to or control of their employees' accounts.

What can employers do?

In the absence of a ruling by an Australian court on the issue of ownership of social media connections, employers can implement measures to discourage employees from misusing social media connections to the employers' detriment.

However, employers should keep in mind that any proposed measures need to be reasonable in order for them to be enforceable. The actual value of an employee's social media connections to the business should therefore be carefully analysed. For example, if a strict social media policy regulating connections was introduced without explanation as to why those connections should be regulated — could this potentially create a damaging backlash and feelings of mistrust towards senior management among employees?

Create comprehensive social media policies

One option employers have is to create (or update) a social media policy. Many years have passed since the Fair Work Commission recognised that social media policies can be a necessary tool to protect legitimate business interests.[15] Any social media policy must be comprehensive and clearly set out expectations around social media use. The policy should cover social media use both inside and outside of working hours and, given the potential uncertainty around the issue, expressly deal with social media connections if they are considered to be valuable by an employer. This may include:

- differentiating between personal connections and professional connections — for example by requiring employees to list all their current connections upon commencing employment

- obliging employees to actively establish LinkedIn (or other social media) connections as part of their role
- clarifying that any connections made as a result of an employee performing their duties constitutes the "confidential information" of the employer
- reminding employees that any connections cannot be used to the detriment of the employer, whether during employment or after it ends
- stating that the employer may conduct audits and inspections of professional and personal social media accounts (where reasonable)
- setting out the potential actions the employer may take — including disciplinary action — if the policy is breached, and
- informing employees that they may be required to delete any connections made as part of their role upon termination (and not add them as a connection again for a set period of time)

Once a social media policy reflects the business's position on ownership of social media connections, it is essential that employees are told why the policy exists and how it can be accessed. As is often said, policies are worthless if employees are not made aware of them and if they are not updated regularly to account for changes in the law, technology, societal values and business practices generally.

Review employment agreements

Confidential information

All employment agreements should contain some form of a confidentiality clause obliging employees to protect the confidential information of their employer both during and after employment.

Where necessary, the definition of "confidential information" in employment agreements should be carefully drafted to capture social media connections made by an employee in the performance of their duties. This may involve expanding the definition of "client list" to include such connections.

Agreements should also expressly state the manner in which employees can and cannot use social media connections, and require employees to delete particular connections at the direction of their employer at the end of their employment (an obligation which also may be reiterated in a social media policy, as discussed above).

Post-employment restraints

Employers may also consider including restraint provisions in their employment agreements. However it is important to remember that restraint of trade clauses are prima facie void (for reasons of public policy) unless they are reasonably necessary to protect the legitimate business interests of the employer. To be held valid, a post-employment restraint of trade needs to provide no more than adequate protection for the employer.[16] Employers may therefore opt to explicitly state that social media connections made by employees in the performance of their duties are indeed legitimate business interests that can be protected by a restraint clause.

Employment agreements should be regularly reviewed and updated — particularly when employees are promoted. While these proactive drafting strategies may clarify social media connection ownership at the employment agreement level, should any dispute proceed to litigation, it still remains to be seen whether a court would be willing to definitively label social media connections or accounts as the "confidential information" of employers.

Control social media accounts

Given that LinkedIn's User Agreement stipulates that all accounts belong exclusively to account holders, employers may want to consider encouraging their employees to make use of social media accounts expressly owned and controlled by them.

Provide training and recognition

Finally, it may be worthwhile providing employees with training around social media use and explain why certain social media connections are valuable to a business. Having social media policies and tightly drafted employment agreements are useful, however encouraging employees to promote the business may lead to less internal resistance.

For example, employers may consider offering incentives (financial or otherwise) to employees who establish new social media connections that benefit the business.

Through fostering a culture of transparency and collaboration, employees may be less willing to undercut their employer should they decide to later resign. Of course, employers can make clear that disciplinary action may be taken against employees if and when necessary. However this is a developing area in the law and employers may want to consider exercising restraint, lest it be later shown that they do not have general ownership rights over employee social media connections.

Conclusion

The strategies suggested in this article, if implemented, may strengthen claim of "ownership" over an employee's social media connections made during the course of their employment. However given that rights over social media connections is an issue that remains to

be determined by a court in Australia, the true value of these connections needs to be fully explored by employers prior to applying measures which may potentially be costly, over-reaching or damaging to the employment relationship.

Stephanie McHugh
Lawyer
Russell Kennedy Lawyers
smchugh@rk.com.au
www.russellkennedy.com.au

Footnotes

1. *Wright v Gasweld Pty Ltd* (1991) 22 NSWLR 317 at 334; 20 IPR 481 per Kirby P.
2. See eg *Faccenda Chicken v Fowler* [1987] Ch 117; (1985) 6 IPR 155; *NP Generations Pty Ltd v Feneley* (2001) 80 SASR 151; 52 IPR 563; [2001] SASC 185; BC200102992 (*NP Generations*).
3. *Forkserve Pty Ltd v Jack* (2001) 19 ACLC 299; [2000] NSWSC 1064; BC200007218.
4. Above n 3, (2001) 19 ACLC 299 at 323.
5. *NP Generations,* above n 2.
6. *Eagle v Morgan* (ED Pa, No 11-4303, 12 March 2013).
7. *Christou v Beatport LLC,* 849 F Supp 2d 1055 (D Colo, 2012).
8. *Sasqua Group Inc v Courtney* (ED NY, No 10-528, 2 August 2010).
9. *Hays Specialist Recruitment (Holdings) Ltd v Ions* [2008] All ER (D) 216 (Apr); [2008] IRLR 904.
10. Above n 9, [2008] IRLR 904 at 907, [19].
11. *Whitmar Publications Ltd v Gamage* [2013] EWHC 1881 (Ch).
12. *Naiman Clarke Pty Ltd atf Naiman Clarke Trust v Tuccia* [2012] NSWSC 314; BC201203367.
13. *Sprout Network Pty Ltd v Roth* [2017] NSWSC 1717; BC201710735, at [17].
14. Available at LinkedIn, User Agreement, www.linkedin.com/legal/user-agreement, accessed 25 November 2019.
15. *Little v Credit Corp Group Ltd* [2013] FWC 9642 at [67].
16. *Amoco Australia Pty Ltd v Rocca Bros Motor Engineering Co Pty Ltd* (1973) 133 CLR 288; 1 ALR 385; BC7300033.