



# Whose timeline is it anyway?

January 2012

As the use of social media as a business tool becomes more widespread, the lines between personal and professional are becoming increasingly blurred. While more and more employers are recognising the benefit of encouraging their employees to use social media tools such as LinkedIn and Twitter to promote their business and network online, the question of ownership of the social media accounts and the corresponding contacts is often overlooked. In particular, what respective rights do the employer and employee have when the employment relationship comes to an end?

### Twitter

The issue has recently been highlighted by a claim brought by PhoneDog, a US website that publishes “mobile news and reviews”, against an ex-employee, Noah Kravitz. According to PhoneDog, in the course of employment its employees are given Twitter accounts to promote the company’s services and disseminate information. Kravitz’s Twitter name as an employee was @PhoneDog\_Noah, and the account generated some 17,000 followers. When Kravitz left PhoneDog, he took the Twitter account (and followers) with him, but changed the name to @noahkravitz. PhoneDog claims that the Twitter account and password constitute proprietary, confidential information, that Kravitz’s actions amount to misappropriation of trade secrets, and that it is entitled to at least \$340,000 in damages (on the basis that each Twitter follower is worth \$2.50 multiplied by the number of months that Kravitz has retained the account).

At present, the substantive merits of this case have yet to receive judicial consideration. However, a California District Court has considered, but denied, those parts of a Motion to Dismiss filed by Kravitz which amounted to an attempt to strike out the claim for misappropriation of trade secrets.<sup>1</sup> While the Court did dismiss subsidiary claims based on economic torts, it held that the question of whether PhoneDog had any property interest in the Twitter account, the valuation of that interest and the issue of whether the account followers and password were trade secrets, required consideration of evidence at a later stage of the proceedings.

While the case does not as yet therefore provide any legal precedent on the matter, at the very least it shows that such claims are not merely speculative, and that on these facts a claim for misappropriation of trade secrets was “plausible on its face”.

The PhoneDog case has parallels with events in the UK when the BBC’s political correspondent, Laura Kuenssberg, who had tweeted as @BBCLauraK, moved to ITV on 1 September 2011, keeping her Twitter account (and its following of some 60,000) and changing the name to @ITVLauraK. However, while the

move led to considerable debate in the media about who owned the Twitter followers, according to Kuenssberg<sup>2</sup>, and unlike the PhoneDog case, she had an amicable agreement with the BBC which permitted her to keep the account.

Kuenssberg points out that followers are free to unfollow her Twitter account: this does not mean, however, that there are no legal rights in information relating to a Twitter following that are capable of protection.

### LinkedIn

Similar issues are raised when considering ownership of LinkedIn accounts and associated contacts, issues which were considered by the English High Court in 2008 in the case of *Hays Specialist Recruitment v Ions*<sup>3</sup>.

Hays, a recruitment agency, applied for an order for pre-action disclosure against a former employee, Mark Ions. It was alleged that, while an employee, Ions migrated confidential client and candidate details from Hays’ confidential database to his own personal LinkedIn page, and retained and used those details prior to and post-termination in order to set up business in direct competition with his former employer, in breach of contractual obligations of confidence and restrictive covenants.

As far as the breach of confidence claim was concerned, Ions argued that while an employee he had been a member of LinkedIn for over a year, with the encouragement of Hays, and that the uploading of contacts from the database to LinkedIn was done with Hays’ consent. Ions also argued that once the contacts were uploaded and corresponding invitations to join his LinkedIn network were accepted, the client details entered the public domain and ceased to be confidential. Hays denied this.

The Court found that on the facts Hays had “reasonable grounds” for considering that it might have a claim against Ions as regards the transfer of information concerning clients and applicants by uploading it to his LinkedIn network. If the information was confidential, then arguably the act of uploading client contact details to LinkedIn amounted to a breach of the obligations of confidence owed to the employer, whether or not the client contacts subsequently became public information on LinkedIn, where it appeared Ions had done this for the benefit of his post-termination business and not for the benefit of Hays.

However, it is important to note that as this was a pre-action application the Court made no finding as to who owned the LinkedIn account, as to whether Hays was entitled to an order for delivery-up of the account and damages, and/or whether Hays was entitled to restrain Ions from making further use of his LinkedIn contacts.

<sup>1</sup> US District Court, Northern District of California, Case No. C11-03474-MEJ, 8 November 2011

<sup>2</sup> <http://blog.itv.com/news/laurakuenssberg/2011/09/day-1-welcome-to-itvlaurak/>

<sup>3</sup> *Hays Specialist Recruitment (Holdings) Ltd, Hays Specialist Recruitment Ltd v Mark Ions, Exclusive Human Resources Ltd* [2008] EWHC 745 (Ch)

It is also important to distinguish this case, where Hays argued Ions had accessed large amounts of confidential customer details from the company database in a short period of time to create LinkedIn contacts, from the more common scenario where an employee independently creates his own LinkedIn contacts in the course of his employment by sending invitations to contacts whom he already knows or would like to know, and accepts invitations from others.

In this latter scenario, the case of *Pennwell Publishing v Ornstien*<sup>4</sup>, by analogy, provides a better indication of how English law might apply. Pennwell is a US company which provides business publications, conferences and exhibitions. One of the Defendants, Junior Isles, had been employed by Pennwell as a publisher and conference chairman. Upon joining Pennwell, Isles uploaded a list of personal pre-existing journalistic contacts to the Outlook email system maintained by Pennwell. During the course of his employment, Isles maintained those contacts, alongside contacts made by him for the purposes of Pennwell's business, in a single list on that Outlook account. When Isles left Pennwells, he downloaded the entire Outlook address list and took it with him.

The Court decided that on these facts the entire Outlook address list was the property of Pennwell, and could not be copied or removed in its entirety by Isles for use outside his employment or after his employment came to an end. However, Isles was entitled to take copies of his own personal information.

Just as with the address list maintained by Mr Isles, many LinkedIn accounts will contain a mix of contacts that existed prior to the commencement of an employment relationship, and those developed during that relationship. Of course, a LinkedIn account is different to an Outlook email system, in that the server is maintained by LinkedIn rather than the employer. However, the LinkedIn account may still be predominantly accessed via the employer's computers or mobile devices, and/or via the employer's

internet connection. It may also be arguable that unlike an email address list, LinkedIn connections (or Twitter followers) cannot be protected as confidential information, but this will depend on the existence and extent of any settings that restrict who can view the connections. It is certainly conceivable that, depending on the facts, the Court would be prepared to extend the reasoning behind the Pennwell decision to cover LinkedIn. While an employee might not be required to delete a LinkedIn account completely, he or she might therefore be ordered to deliver-up details of connections made in the course of the employment relationship and remove them from the account.

## Social media policy

The common theme running throughout the cases cited above is that there were no specific contractual terms governing the ownership of contacts made in the course of the employment relationship.

Clear wording in a social media and/or email policy incorporated into the employment contract will help to clarify, as well as appropriate usage, the ownership of contacts that are added to email address lists and social media accounts, what steps an employee is required to take, and/or is prohibited from taking, in relation to those contacts when the employment relationship comes to an end, and whether the employee is permitted to continue to operate the social media account in question after termination, and if so in what form.

Contractual provisions of this nature are likely give an employer the best protection in relation to social media accounts and email lists maintained by employees, and may remove altogether the need to establish that LinkedIn connections and Twitter followers are confidential information.

*This article was first published in E-Commerce Law Reports volume 11, issue 6.*

<sup>4</sup> *Pennwell Publishing (UK) Limited v Nicholas Patrick Ornstien, Daniel Stanley Noyau, Junior Isles, The Energy Business Group Limited* [2007] EWHC 1570 (QB)

## Contact

For further information please contact:



**Andrew Tibber**  
Senior Associate

+44(0)117 902 7758  
andrew.tibber@burges-salmon.com



**Roger Bull**  
Partner

+44(0)117 902 2701  
roger.bull@burges-salmon.com

Burges Salmon LLP, One Glass Wharf, Bristol BS2 0ZX Tel: +44 (0) 117 939 2000 Fax: +44 (0) 117 902 4400  
Chancery Exchange, 10 Furnall Street, London EC4A 1AB Tel: +44 (0) 20 7685 1200 Fax: +44 (0) 20 7685 1266

[www.burges-salmon.com](http://www.burges-salmon.com)

Burges Salmon LLP is a Limited Liability Partnership registered in England and Wales (LLP number OC307212) and is authorised and regulated by the Solicitors Regulation Authority. A list of members, all of whom are solicitors, may be inspected at our registered office: One Glass Wharf, Bristol BS2 0ZX.

© Burges Salmon LLP 2012. All rights reserved. Extracts may be reproduced with our prior consent, provided that the source is acknowledged. Disclaimer: This briefing gives general information only and is not intended to be an exhaustive statement of the law. Although we have taken care over the information, you should not rely on it as legal advice. We do not accept any liability to anyone who does rely on its content.

Data Protection: Your details are processed and kept securely in accordance with the Data Protection Act 1998. We may use your personal information to send information to you about our products and services, newsletters and legal updates; to invite you to our training seminars and other events; and for analysis including generation of marketing reports. To help us keep our database up to date, please let us know if your contact details change or if you do not want to receive any further marketing material by contacting [marketing@burges-salmon.com](mailto:marketing@burges-salmon.com).