Hamel-Smith FORUM
ATTORNEYS-AT-LAW, TRADEMARK & PATENT AGENTS

VOLUME 9 ISSUE 3 | The Lawyers Newsletter for Business Professionals | NOVEMBER 2015

TOO MUCH INFORMATION? THE RISKS OF USING SOCIAL MEDIA TO SCREEN RECRUITS

Catherine Ramnarine

It is trite, but true, to say that technology has transformed the way we live. Unfortunately, developments in the law have not always kept pace with technology, often resulting in legal grey areas that can be difficult to navigate. One such grey area is the use of social media in the recruitment process. There is a growing practice (among employers) of screening social media accounts of prospective employees for any 'red flags' or indications of unsuitability. While currently there are no laws expressly prohibiting this practice, it can, if not managed properly, run afoul of existing laws regarding employment, data protection and privacy. In this Article, we outline some of the risks employers should be aware of when using social media screening in the recruitment process and discuss how these risks can be managed.

Discrimination and the Equal Opportunity Act

The Equal Opportunity Act prohibits employers from discriminating against prospective employees on the grounds of gender, race, ethnicity, geographical origin, religion, marital status or disability.

By screening a prospective employee's social media accounts, an employer runs the risk of viewing information about that person's religious beliefs, marital status or other protected characteristics. It goes without saying that an employer should not refuse employment to a candidate on any of these grounds. However, the risks may not always be so clear cut. A policy or practice of excluding candidates who have posted revealing photos of themselves online, for example, may have a disproportionate impact on female candidates and may therefore be considered discriminatory.

In any case, whether or not an employer actively seeks out or makes a hiring decision based on information about a candidate's protected characteristics, by exposing itself to this information on social media, it is also exposing itself to an allegation that it was influenced by this information and, by extension, that it is guilty of discrimination under the Equal Opportunity Act.

Privacy, Personal Information and the Data Protection Act

The Data Protection Act is intended to protect personal privacy and information. While most of the Act does not yet have legal force, the 'General Privacy Principles' set out in Section 6 have been proclaimed and are in force. These Principles require anyone who stores, handles or processes someone else's personal information to:

- Identify the purpose for which they are collecting the information
- Collect only the information necessary for that purpose
- Obtain a person's consent to the collection, use or disclosure of his personal information
- If requested, allow the person the opportunity to challenge the accuracy and completeness of any personal information collected about him.

These General Privacy Principles apply whether the information in question is collected directly from the person to whom it relates or whether it is collected from other sources. Employers are therefore required to adhere to these Principles when obtaining personal information about a candidate from his social media accounts.

Managing the Risks

Social media screening can be a useful and valuable recruitment tool, once it is managed effectively. Here are some tips for managing the potential risks:

- Develop a formal policy governing the use of social media screening in the recruitment process and ensure that anyone involved in the process clearly understands

(cont'd on page 2)

CONTENTS

BRAND PROTECTION – GUARDING AGAINST ONLINE INFRINGEMENT

Fanta Punch

The Internet has been a cost effective tool in the exploitation and commercialisation of brands. Yet, the same technology that can give a brand global reach, can also facilitate infringement or misuse which can be detrimental to a business.

A brand is open to online threats in a number of ways, for example:

- Inappropriate use of domain names or cybersquatting;
- The sale of counterfeit goods at online auction sites; and
- Negative brand exposure through commonly used social media sites, such as Facebook, Twitter, YouTube and LinkedIn.

Adopting a multi-faceted approach to strengthening your brand's position is recommended when seeking to protect a brand against online abuse. Below are some ways a brand owner can strengthen a brand's positioning.

Registering Brands

Ensuring that appropriate trade mark and domain registrations are sought and maintained in as many jurisdictions as possible can be a powerful deterrent. This makes it easier to commence action against infringement based on registration rather than common law actions, such as passing off. It may also be worth seeking registration in countries where the brand does not have an actual presence but where possible threats of infringement may occur. However this ought to be balanced against the threat of revocation actions for vulnerable trade marks which have not been used over time.

Building Customer Loyalty

Where brand owners have a strong online presence and customers identify with their genuine products, this too can be of significant value. Development of a strong and loyal customer base can go a long way in the promotion and protection of a brand. Establishing regular communication

(cont'd on page 3)

Too Much Information? The Risks of Using Social Media to Screen Recruits *(cont'd)*

(cont'd from page 1)

the legal risks and requirements.

- Ensure that your use of social media screening is reasonable and proportionate. It is important to consider the nature and requirements of the position that you are seeking to fill as some may justify a higher level of scrutiny than others. For some positions, it may only be appropriate to screen a candidate's 'professional' social media accounts, like LinkedIn. For others, such as positions which require a high degree of sensitivity, trust or public confidence, an employer may be justified in screening a candidate's 'personal' social media accounts, like Facebook, Twitter or Instagram, for discriminatory or controversial posts.

- It is also important to consider the stage at which social media screening is carried out. Is it really necessary to screen all applicants for the position? It may be more sensible to screen only those who have been shortlisted, or to screen only the selected candidate prior to making a formal offer of employment.

- Let the candidates know that you will be carrying out social media screening and obtain their informed consent. Ideally, this should be done as early as possible during the recruitment process, even though the actual screening may take place at a more advanced stage.

- Give candidates an opportunity to review and comment on the accuracy and completeness of your findings. Some of the information you find may be outdated or inaccurate. Also, it is possible that your searches may have yielded information about someone else with the same name as your candidate.

- Do not attempt to obtain access to a candidate's social media accounts by deception (making a 'friend' request under a false name) or coercion (requiring candidates to turn over their passwords as a condition of employment). Not only is this likely to be viewed as a breach of the General Privacy Principles under the Data Protection Act, it is hardly likely to endear you to the candidate or create a positive working environment.

Social media screening can be a valuable part of the recruitment process, but must be managed effectively. Apart from the legal risks outlined above, employers who adopt an ad hoc or overzealous approach to social media screening run the risk of turning off capable and talented prospective employees who view it as an invasion of their privacy. By adopting a thoughtful, measured and proportionate approach you can mitigate the risks and maximise the potential benefits of using social media screening in recruitment.

Catherine Ramnarine is a Partner in the firm's Dispute and Risk Management Department.

For more information about the Equal Opportunity Act and Data Protection Act, see past issues of the Forum at:
http://www.trinidadlaw.com/

Brand Protection—Guarding Against Online Infringement (cont'd)

(cont'd from page 2)

with customers and being responsive to their needs can help build customer loyalty, not to mention the obvious benefit of receiving their invaluable feedback.

Being Decisive

An important aspect of strengthening a brand also involves continual monitoring of online auction sites (such as Google, Amazon, eBay) for unauthorised trade mark use, either by carrying out regular product checks or retaining specialist companies to conduct searches for unauthorised use. This is especially relevant where online infringers have short turn-around times for online sales as a way to avoid detection. A proactive brand owner ought to keep abreast of any trends in infringing activity as they relate to the brand's relevant product market.

Being well positioned to take decisive and prompt action to dissuade potential infringers goes some way to protecting the online presence of a brand. In the UK case of Cosmetic Warriors Ltd and another v Amazon.co.uk Ltd and another [2014] EWHC 1316 *(Ch)*, the owner of the registered LUSH trademark (in respect of its special soaps and bath products) successfully brought trademark infringement proceedings against Amazon, an online retail site. It was held that Amazon infringed LUSH's trademark through use of the word "Lush" on its website. When customers searched Amazon's website for the word "Lush", it appeared in various online search results. Customers were then directed to other similar or related products but were never told that Lush's products were unavailable on the Amazon site. The court found that the average customer could not easily determine that Lush's products were not available on the website.

Understanding the Environment

Social media sites provide an excellent marketing opportunity for a brand to reach a very wide audience through a dynamic virtual space. However, it also presents risks for brand owners in equal measure, especially where the brand owner has no control over user-generated content published on these sites.

Social media can at times be used to complain about poor service, criticize a brand or engage in negative campaigning. The potential threat from social media was highlighted earlier this year in the rumoured report about a possible food poisoning death from the purchase of fast food from a local Pricesmart outlet. In this informal and fast paced environment, comments can be spread very quickly which can damage a brand's reputation, so an important component of any online strategy should include monitoring of social media sites or online customer complaints sites.

Online advertising for example keyword advertising, through sites like 'Google AdWords', can also facilitate online infringement. Advertisers can purchase or bid on trade marks or brand names which are used as sponsored names online or as metatags.

When users search for the particular trademark, they are directed to a sponsored link, even if the advertiser does not own the trademark, so generating traffic directly to the advertiser's site. If it is possible to prove that such activity infers or suggests a connection between the advertiser's products and those of the registered trademark, it may be a possible infringement. This is another area which requires vigilance by the brand owner in protecting its online presence.

Developing a Suitable Enforcement Strategy

Having a suitable enforcement strategy is necessary to deal effectively with infringing activity. For the proactive brand owner, being vocal about enforcement policies or taking a very aggressive approach by initiating infringement proceedings against *any* unauthorised use, on a global basis, regardless of the value of the claim, are strategies that could deter infringers.

In considering a suitable approach, the issue of jurisdiction in determining infringement is relevant. The UK- based case, *1-800 Flowers Inc v Phonenames Ltd (UK) [2001] EWCA Civ 721* dealt in part with a challenge to the use of website space in trademark opposition proceedings. For the purposes of trademark law, the Court held that website use could not be regarded as use everywhere in the world, but only based on accessibility. In that case, the website was targeted to a particular community and so limits on jurisdiction could be applied.

Summary

Online protection of a brand can be a time consuming and expensive exercise and it may be difficult to justify the resources for it. Where investment in marketing a brand online is part of a business strategy, then protecting the brand against online abuse ought to be worthwhile to the brand owner who is willing to:

- Effectively manage a brand by having a thorough understanding of its intellectual property assets and the ways in which a brand can be attacked or undermined;
- Be prepared through awareness of the actions of its competitors and to monitor use of the brand in order to successfully compete in the market.
- Develop knowledge of the market and the key players where the brand operates to identify trends; and
- Adopt a strategic approach in response to infringement and the ever changing pace at which it occurs.

Fanta Punch is a Partner in Hamel-Smith's Intellectual Property practice area. Her email address is fanta@trinidadlaw.com.

VIRTUAL PIRACY – HOW TO PROTECT YOUR DOMAIN NAME

David Hamel-Smith

As our businesses (and lives) move from the physical to the virtual, we can find ourselves in an internet universe where online real-estate (domains) risks being captured and ransomed by opportunists who can loot and plunder the goodwill associated with our brands.

Recently, Mr. Sanmay Ved was browsing Google Domains (a domain-name brokerage owned by Google) when he noticed that the Google.com domain name was up for sale. He quickly purchased the domain name for a mere $12. Google immediately realized what had happened and they cancelled the sale and offered Mr. Ved a reward of "more than $10,000" for realizing their mistake. Impressively, Mr. Ved asked that Google please donate the award to a charity, The Art of Living India, and Google, presumably "feeling lucky" to have their multi-billion dollar domain name back in their hands, happily doubled the donation.

What can you do if you find out that your trademark is registered as a domain name by someone who is not as charitable as Mr. Ved? What recourse do you have if you contact that person (or they contact you) and you are told that you must pay them an exorbitant fee for the domain name? While the answer is slightly more complicated than simply offering a donation, you may have some recourse against domain name pirates.

In the early days of the Internet, prior to Google, Facebook and Wikipedia, one would have had to prove that the registered owner of a domain name was engaging in the tort of passing off. This is what was done in the much-cited case of *British Telecommunications plc & Ors v. One in a Million Ltd & Ors* [1998] EWCA Civ. 1272.

In that case, the Defendants registered dozens of domain names associated with popular brands and then ransomed the names to the brands at premium prices. Several of the major brands then sued the Defendants in an attempt to get possession of the domain names without coughing up the requested fees. The major brands succeeded at trial, but One in a Million Ltd appealed. In summarizing the facts of the dispute the Court of Appeal stated the following:

> *"[One in a Million Ltd] have made a specialty of registering domain names for use on the Internet comprising well-known names and trademarks without the consent of the person or company owning the goodwill in the name or trademark. Examples are the registration and subsequent offer for sale to Burger King by the second defendant of the domain name burgerking.co.uk for £25,000 plus VAT and of bt.org to British Telecommunications for £4,700 plus VAT."*

The Court of Appeal managed to massage the claim into the existing tort of "passing off" by finding that, although the registered domain names were not actively operating, the mere registering of the name created a (misleading) association between One in a Million Ltd and the goodwill associated with the brands. For example, the Defendants registered the domain name "marksandspencer.co.uk" and the Court stated the following:

> *"It is accepted that the name Marks & Spencer denotes Marks & Spencer plc and nobody else. Thus anybody seeing or hearing the name realises that what is being referred to is the business of Marks & Spencer plc. It follows that registration by the appellants of a domain name including the name Marks & Spencer makes a false representation that they are associated or connected with Marks & Spencer plc. This can be demonstrated by considering the reaction of a person who taps into his computer the domain name marksandspencer.co.uk and presses a button to execute a 'whois' search. He will be told that the registrant is One In A Million Limited. A substantial number of persons will conclude that One In A Million Limited must be connected or associated with Marks & Spencer plc. That amounts to a false representation which constitutes passing-off."*

Accordingly, the Court of Appeal upheld the trial judge's decision in favour of the major brands.

ICANN Uniform Domain Name Dispute Resolution Policy

Since the *British Telecommunications* decision, we have seen the establishment of the Internet Corporation for Assigned Names and Numbers ("ICANN"). ICANN is an internationally organized non-profit organization responsible for the registering and selling of Generic Top Level Domains ("gTLDs"). Importantly, ICANN has implemented a Uniform Domain Name Dispute Resolution Policy (the "dispute resolution policy") which governs domain name disputes.

Under section 4(a) of the dispute resolution policy, registrants of domain names are required to submit to administrative proceedings under the policy if there is a complaint that:

- the domain name is identical or confusingly similar to a trademark;
- the registrant has no rights or legitimate interests in the domain name; and
- the domain name was registered and is being used in bad faith:

The dispute resolution policy also notes that: "In the administrative proceeding, the complainant must prove that each of these three elements are present."

The ICANN dispute resolution policy relieves claimants from the burden of having to prove that they suffered the tort of passing-off, but still requires them to meet the fairly onerous requirements set out at section 4(a).

One frequently cited decision under the ICANN policy comes from a dispute between Madonna, the well-known

(cont'd on page)

Virtual Piracy – How to Protect your Domain Name *(cont'd)*

(cont'd from page 4)

entertainer, and Dan Parisi over the domain name "Madonna.com", ***Madonna Ciccone v. Dan Parisi*** (No. D2000-0947). In the arbitral proceedings, the respondent did not dispute that the domain name was identical or confusingly similar to Madonna's trademark, rather he argued that he had a bona fide business interest in the use of the name and that there was no evidence that his primary motivation was to sell the disputed domain name or any other demonstration of it being used in bad faith. In coming to its decision to award Madonna the domain name, the arbitral panel found that the respondent had engaged in a pattern of conduct whereby he registered other names and marks of brands and celebrities to sell at an inflated price. From this, the panel determined that Mr. Parisi had no legitimate interests in the domain name and that it was registered in bad faith.

There have also been several court decisions flowing from the ICANN arbitral decisions, including the Ontario decision of ***Black v. Molson Canadian*** [2002] CanLII 49493 (ONSC) where the Ontario Supreme Court reversed an arbitral decision which awarded the domain name "Canadian.biz" to Molson Canadian. The Ontario Court applied the ICANN policy to the facts of the case and determined that:

- *Simply because a domain name is identical or similar to a trademark should not result in the transfer of the domain name to the trademark owner. A domain name should not be transferred unless there is some evidence that the use of the domain name infringes the trademark. Since Molson's Canadian trademark is registered for use with beer only and does not give Molson the exclusive use of the word "Canadian", any person should be able to own the <canadian.biz> domain name. The public would not confuse the <canadian.biz> domain name with other domain names used by Molson.*

- *Black's assertion that he intended to use the domain name for a "profit-seeking venture", was sufficient to establish that Black has legitimate rights or interests in the domain name.*

- *Simply because Black was aware of Molson's Canadian trademark was not a sufficient basis for finding that Black registered the domain name in bad faith.*

The ICANN policy, and the Courts' interpretation of it, highlight the balance that needs to be struck between the desire to allow users the ability to register legitimate domain names for their own use, and the interest of companies in protecting their intellectual property from bad faith infringements.

In conclusion, what recourse do you have if you find out that your brand name is already registered as a domain name by someone else?

Well, if it can be established that:

- the domain name is confusingly similar (or identical) to your trademark; and
- the owner of the domain name has no legitimate interest in it; and
- the domain name is being used in bad faith –

then you would be well advised to commence arbitral proceedings under the ICANN dispute resolution policy which could potentially lead to your being awarded ownership of the domain name.

If those three criteria cannot be satisfied, it may be that the registered owner of your domain name is actually a legitimate owner and your only recourse might be to engage in a negotiation to purchase the domain name.

David Hamel-Smith is an Associate in Hamel-Smith's Dispute and Risk Management Department.

The Lawyers Newsletter for Business Professionals

Published by M. Hamel-Smith & Co.
Eleven Albion, Cor. Dere & Albion Streets
Port of Spain, Trinidad & Tobago
Tel: 1(868) 821-5500 / Fax: 1(868) 821-5501
E-mail: mhs@trinidadlaw.com / Web: www.trinidadlaw.com

Member
Lex Mundi
World Ready