Think before you post... Your future employer may be watching

Elliott Payne

Law Department, UCC

Figure 1: Shopping with iphone. Commons licensed image from Jason Howie available at http://www.flickr.com/photos/jasonahowie/8585049088/in/photostream/

Introduction

The explosion of social networking sites in recent years has given many Kim Kardashian wannabes an opportunity to display and glamorise their supposed activities and achievements. However, it has also unwittingly given employers an opportunity to pry into the personal (and at times very personal) affairs of their prospective employees through the practice of cyber-vetting. Social media users should take note. They should think very carefully before they post, tweet or upload a photograph as their future employer may be watching and to paraphrase US Chief Judge Alex Kozinski, removing something from the Internet is about as easy as removing urine from a swimming pool!

https://doi.org/10.33178/boolean.2014.30

What is cyber vetting?

Dr Brenda Berkelaar of Purdue University, who completed a PhD on cyber-vetting, described the practice as: "when organizations use information from search engines or social networking communities to evaluate job candidates." In its simplest form, cyber-vetting is the examination by employers of the digital footprint left behind by a prospective employee.

At a basic level, cyber-vetting can involve a candidate being "googled". It can also consist of a more targeted examination of the social networking site(s) such as Facebook and LinkedIn belonging to the person in question. The third and perhaps most alarming stage of cyber-vetting, which for now appears to be limited to the United States, is a request that the prospective employee "volunteers" relevant passwords or enables the employer to "shoulder surf" so that the employer can have unfettered access to the full extent of the candidate's social networking profile(s), warts and all, without being frustrated by any privacy settings.

Why is cyber-vetting carried out?

Employers cyber-vet because they are trying to protect their legitimate business interests and long term reputation by researching what type of person they are hiring to ensure that they are a good fit for their organisation. This vetting provides a cheap, albeit crude, form of human filtration to enable the more promising employment candidates to progress to the next stage of selection, while the "undesirables" will have been eliminated without even realising it. It is also arguable that cyber-vetting could reveal more about the suitability of a candidate than a carefully crafted *curriculum vitae* or, at the very least, verify the information contained therein.

How extensive is cyber-vetting?

Unsurprisingly, given its government's approach to the surveillance of others, the home of cyber-vetting is the United States. A comparison was undertaken in 2010 by Microsoft of human resources professionals in the US, UK, Germany and France. When these professionals were asked whether:

- □ they reviewed on-line reputational information about a prospective candidate?
- □ 79% of Americans admitted that they reviewed such information all/most of the time compared with 47% (UK), 59% (Germany) and 23% (France);
- □ on-line screening was part of a formal hiring process?

□ 75% of Americans said yes, compared to 48% (UK), 21% (Germany) and 21% (France);

□ they had rejected a candidate as a result of on-line screening?

□ 70% of Americans said yes, compared to 41% (UK), 16% (Germany) and 14% (France).

According to this study, nearly 80% of those involved in human resources management in the US admitted to engaging in cyber-vetting and 70% had rejected candidates based on what they had found. However, whilst the Microsoft findings are clear, they are not conclusive. In the US, the Society for Human Resources Management (SHRM) carried out a variety of studies in 2008, 2011 and 2013 on the attitudes of human resources professionals towards social media. Arguably their most important finding was in 2013, when 57% of those surveyed did not have a formal or informal policy towards the screening of social network websites, compared with 56% in 2011 and 72% in 2008.

On first impression the Microsoft findings differ from the SHRM results. The variation in results could partly be attributed to those involved in human resources management adopting a more "professional" approach when being surveyed by their own umbrella organisation when compared to Microsoft. Furthermore, the question asked in the Microsoft study is broader in that it talks about "on-line reputational information", whereas the SHRM survey is far more precise in its questions and talks specifically about social network websites, thus it is inevitable that there will be a difference between the two sets of results. Given its secretive nature, whilst the true extent of cyber-vetting may never be definitively known, it is apparent that it does take place, and employers and employees should be aware of the risks associated with this practice.

Concerns surrounding cyber-vetting

Probably the biggest risk facing employers who cyber-vet is that it may breach the privacy rights of prospective employees. As displayed in the Microsoft study, the country with the lowest incidence of cyber-vetting was France, which has some of the strictest privacy laws on the planet. In addition, if an employer views the social profile(s) of a candidate, they may inadvertently discover so-called "protected characteristics" such as: gender, ethnicity, disability, family/marital information which would not have been apparent from a *curriculum vitae* or application form. It is also possible that negative inferences could be drawn by employers from content indicating addictive tendencies or at the very least a fondness for alcohol, cigarettes or gaming/gambling. Consequently, if the candidate is unsuccessful in their application and can prove that their profile was viewed by an employer who engages in cyber-vetting, then the employer could be facing a very expensive equality and/or privacy claim and the accompanying toxic publicity that surrounds such litigation.

Attempts to curb cyber-vetting

It is perhaps not a surprise to discover that in the land of the free and the home of the brave, attempts have been made to curb cyber-vetting. Whilst nothing can be done to prevent employers reviewing publicly available information on search engines, over 30 States have introduced or have legislation pending that expressly prohibits: the practice of asking for passwords; requesting that privacy settings be changed so access can be obtained; requesting that employers be categorised as "friends"; or shoulder surfing — even during an actual interview. Any adverse treatment as a result of non-compliance is strictly forbidden.

Whilst this legislation aims to prevent employers accessing content that could embarrass and/or humiliate a prospective employee, the State of California has gone a step further and has introduced legislation colloquially known as the "Eraser law" that will enable teenagers to put incriminating photographs beyond the reach of future cyber-vetters in the first place.

Eraser law

In September 2013, the Californian Governor signed a Bill, which will come into legal effect on 1 January 2015, which requires all Internet website operators, online services, online and/or mobile applications to remove, at a minor's request, specific comments and photographs posted by that minor. In essence, it aims to protect teenagers from online baggage they have posted which they may later regret or could affect their ability to gain college admission, employment or both.

This legislation has been hailed as an extension of a minor's privacy rights and has received widespread support from family and community organisations who highlight the impetuosity of teenagers and the permanency of what they publish online. However, others have been less than generous with their support and see this as no more than a populist trick to secure potential votes. Most of the reservations centre on how this Eraser law will practically work, from:

□ its complete ineffectiveness if the information has already been shared/uploaded by others;

□ its non-applicability to content posted by a third party about a minor;

□ how the under-eighteen age requirement will be enforced when many users lie about their age when they register on social networks in the first place;

□ the jurisdictional applicability of this law, in that it is unclear whether it applies to organisations with physical operations in California or whether operators around

> the United States will have to comply in case some of their teenage customers reside in California?

The efficacy (or not) of this Eraser law is obviously too soon to tell. It should be emphasised that it will only apply to those who are under the age of eighteen, so for many it is too late and of no use.

Why cyber-vetting does not work

Despite its use, cyber-vetting is a crude, unsophisticated and ineffective tool used by employers in the mistaken belief that it will assist them to protect their interests. The reality is that it may harm those interests by discarding candidates who may be a real asset to their organisation.

Cyber-vetting often relies upon imprecise, incomplete and downright incorrect data and as a result imprecise, incomplete and incorrect conclusions will inevitably be drawn. Even if the information is factually correct, a snippet of information viewed in isolation many months, if not years, after the event cannot accurately reflect the true sentiments of the correspondent at the time the statement was made, particularly if the full exchange of emails/tweets/blogs is not available.

When communicating online, particularly if exchanges are confined to a small pool of friends, correspondents may adopt an alter ego — a more extreme and laughable version of themselves and will deliberately propose controversial ideas. This information may be extracted and isolated by cyber-vetting but the context will not be accurately reflected. Furthermore, people in a formal employment setting do not behave in the same way that they do online with friends, so the reliance by employers on cyber-vetting to provide corporate compatibility is destined to produce inaccurate results.

There is a huge variation in the type and amount of information available online and some prospective employees will have larger digital footprints than others. If cyber-vetting is used by employers as a tool of predicting future behaviour then it is fundamentally flawed as by its very nature it does not provide a completely standardised collection of information across all prospective candidates. In addition, for those employees who regularly self-monitor, artificially enhance and/or massage their online reputation, the results of a trawl of social media information may be distorted, and this consequently may negate any assumptions that can be drawn about their character and personality.

Given the doubts about the veracity of information obtained, combined with a non-standardised treatment of candidates, it is more than arguable that, by its very nature, cyber-vetting is both unfair and ineffective. These inaccurate conclusions are all the more worrying when the individuals concerned are unable to have the opportunity to challenge and/or correct such presumptions.

Whilst cyber-vetting is a cheap and quick method of assessing employees it is by its very nature fundamentally flawed and, for that reason, this practice should be consigned to the trash folder and deleted forever. This research into cyber-vetting forms part of a thesis entitled “Employment law for the digital age: How social media has affected the contract of employment” which examines how the traditional employment relationship has been and continues to be shaped by a variety of legal issues associated with the use of social media.

Elliott Payne is a first year doctoral candidate who would like to acknowledge the support provided by his supervisor Dr Darius Whelan and his colleagues in the UCC Law Department.