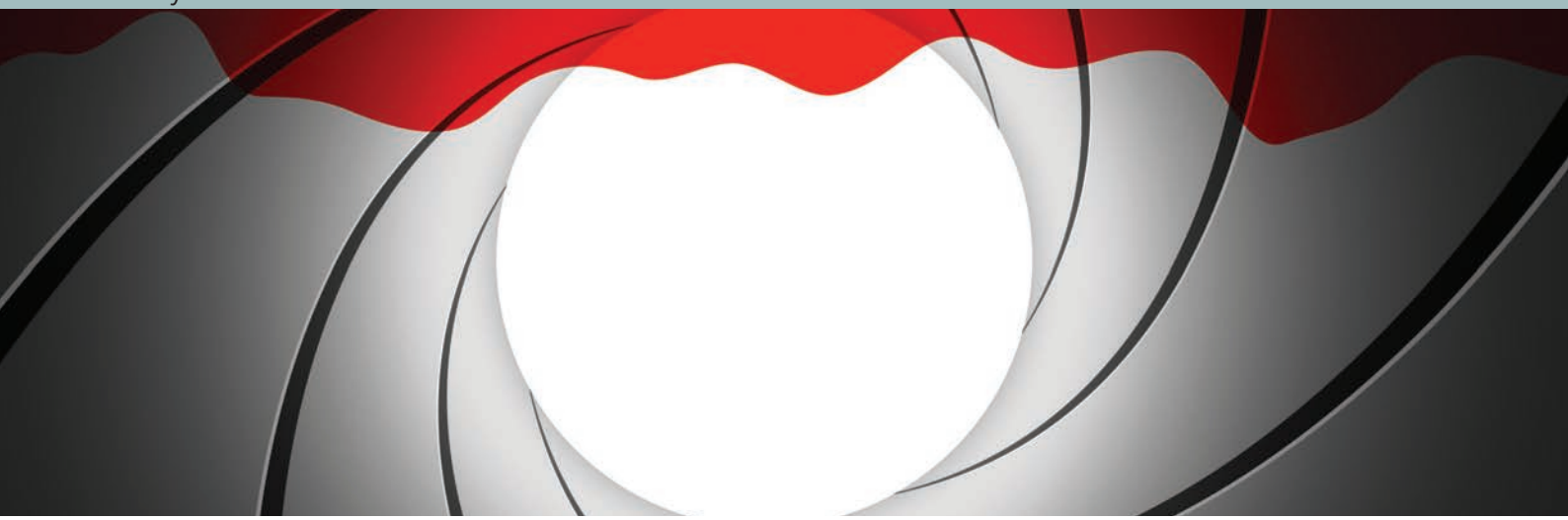
hunt & hunt lawyers

Employment law update

January 2016



Shaken, not stirred?

Protecting your business against employee espionage

"BlueScope Steel stung by alleged corporate espionage" read the headline on the front page of the "The Age" newspaper last Saturday. The article that follows describes the alleged "*international espionage*" by former employee of BlueScope Steel, Chinnari Sridevi Somanchi and the legal action taken by BlueScope Steel in the Federal Court of Australia and Singapore to stop her [1].

The article reports that Ms Somanchi's position with BlueScope Steel (BlueScope) was made redundant in June 2015 and she later took up a position as Innovation Manager with NS BlueScope, a joint venture between Nippon Steel & Sumitomo Metal and BlueScope Steel in Singapore in late 2015. Ms Somanchi, described as a "disgruntled former employee" by BlueScope, is alleged to have taken highly valuable information including internal emails, 13 software packages, and source code for eight software programs. BlueScope alleges that that Ms Somanchi, who was involved in the development of BlueScope intellectual property, downloaded about 40 gigabytes of company documents including codes which she downloaded just before she was made redundant as well as when visiting former colleagues after signing a contract with NS BlueScope.

BlueScope made an application for urgent and interim relief in the Federal Court of Australia on New Year's Eve. Justice Bromberg was satisfied that there was strong prima facie case that Ms Somanchi had breached her contract of employment and that there was also a basis for concluding that BlueScope may have an arguable case based upon infringement of its copyright and breach of confidence.

1 *"BlueScope Steel stung by alleged corporate espionage",* Lucy Battersby and Sarah Dankert, The Age, 9 January 2016.

Accordingly, his Honour considered it appropriate to make orders including preventing Ms Somanchi from making use of certain documents, source codes, software packages and storage devices in her possession, destroying or in any way altering that material and requiring her to disclose and deliver it up to an independent lawyer and do all things necessary to enable independent computer experts KordaMentha to access it. The matter is listed for further hearing in February 2016[2].

Although the legal proceedings are ongoing and final judgement has not been made, the matter serves as a warning for all employers that loyalty cannot be assumed and vigilance is paramount.

Below are four key steps to protecting your business:

1. EMPLOYMENT CONTRACTS AND POLICIES

Employers need to review written employment contracts and company policies and procedures to ensure that they provide adequate protection of their intellectual property and confidential and commercially valuable information, and to ensure that the ongoing obligations owed by their employees are clearly and unmistakably communicated to them. Ms Somanchi's contract of employment required her to treat BlueScope's confidential information as confidential and return it to BlueScope upon the cessation of her employment together with any other BlueScope property held by her. In the absence of express written contractual terms, employers will need to rely on common law and statutory obligations, which may be more limited in scope and in the remedies for breach. Employers should also ensure that employees are covered by a written employment contract applying to their current position, particularly senior employees who may have been with the business for many years. Digging out old employment contracts at the time of change or dispute is usually too little too late.

However, even the most carefully crafted employment contracts and policies will not stop aberrant behaviour and prevent consequent damage and loss. Justice Bromberg accepted on the evidence before him that the intellectual property allegedly obtained by Ms Somanchi had "very substantial commercial value" to BlueScope and BlueScope may face a "real risk of significant loss or damage" if it came into the hands its competitors. A senior manager at BlueScope is also reported as stating in material filed with the Court that losing its customised software to a rival would so badly damage BlueScope that it was not seeking penalties because "it is difficult to see how damages could adequately compensate BlueScope for the loss". Therefore, employers need to think about additional protective measures, such as those outlined below.

2. INTERNAL SAFEGUARDS AND CONTROL MEASURES

Internal safeguards and control measures should be implemented, in consultation with the people who understand any applicable technology. In another high profile case in 2009, former computer programmer for Goldman Sachs in the USA, Serge Aleynikov was accused of taking the firm's high frequency trading computer code when he left for another job. The events that ensued including two criminal trials sparked debate in Wall Street and afar about the fairness of the action against Mr Aleynikov. However, a lesson for employers is that Mr Aleynikov is said to have had "super-user status" which meant that he could log in as an administrator to the system and he says that from the day he arrived at Goldman Sachs he was able to send the firm's source code to himself weekly without anyone saying a word to him about it [3].

3. SPECIFIC STRATEGIES WHEN THE EMPLOYMENT RELATIONSHIP IS STRAINED

Specific strategies may also need to be adopted during times when the employment relationship is strained or is coming to an end. It is at these very times that aggrieved employees may believe their wrongful actions are justified. For example, Ms Somanchi is alleged to have downloaded company secrets on the day that she was to made redundant and presumably after she was advised of the redundancy meeting. Similarly, Mr Aleynikov is alleged to have sent 8 megabytes of source code four times to himself during the six week handover period following his resignation.

2 *BlueScope Steel Limited v Somanchi [2016]* FCA 4, 4 January 2016

3 *"Did Goldman Sachs Overstep in Criminally Charging its Ex-programmer",* Michael Lewis, Vanity Fair , 31 August 2013

4. CONTRACTORS AND CONSULTANTS

It is equally important for businesses to consider these issues when dealing with contractors and consultants, many of whom may have access to company IT systems and confidential information and may also be involved in the creation or development of intellectual property.

Corporate espionage may make for an interesting plot for 007 movies but employers should ensure their business is protected, not shaken or stirred…

Hunt & Hunt can review your employment and contractor agreements and company policies and procedures as well as provide you with specific strategies to protect your business when disciplining or exiting employees.

Authors
Gisella D'Costa and David Thompson

NSW
Shawn Skyring
Martin Dunne

VIC
David Thompson
Gisella D'Costa

SA
Emily Slaytor

WA
Darren Miller

TAS
Antony Logan
Sarah Sealy (mat leave)
Stephanie Manning

NT
Chris Osborne