Unauthorised Email Access

Introduction

It is unfortunately, not uncommon for a former employee ("A"), leaving the employment of a person ("B"), and taking with them intellectual property developed by B and either going to work for a competitor ("C") or commencing business in competition with B. The usual cases involve alleged copyright infringement and alleged breaches of contractual and non-contractual obligations of confidence.

Imagine however, a competitive industry where A hacked into B's emails and began accessing for the benefit of C, new job opportunities made available to B. What rights are infringed and how can they be enforced? This article considers that situation and suggests some practical solutions.

The legal issues

If we take a case, where the industry in which B and C are competitors, is a specialist field and it is not uncommon for the employees of one to be "poached" from the employment of the competitor. In such a case B has now employed one of C's former employees ("D"), who has given a statement to B's solicitors, that his work mobile with C was armed with the passwords and ability to receive all B's emails and that he personally was able to get into B's email server and identify and pursue job opportunities for C which had been directed to B by potential customers!

As to the claims one might make for B, the first thoughts could go to:

(a) The *Competition and Consumer Act* 2010 ("ACL") (ss 21 (Unconscionable conduct in connection with goods or services) and possibly 18 (misleading and deceptive conduct);

(b) Breach of obligations of confidence; or

(c) The equitable claim for unjust enrichment.

Generally, the *Telecommunications (Interception and Access) Act* 1979 was introduced to establish a series of offences and civil remedies for communications which were passing through a telecommunications system and intercepted. However, emails were not part of the business culture in 1979. At first blush the following was appealing:

Under the heading "*Telecommunications not to be intercepted*", the legislation states:

A person shall not:

(a) intercept;

(b) authorize, suffer or permit another person to intercept; or

(c) do any act or thing that will enable him or her or another person to intercept;

a communication **passing over** a telecommunications system." [1]

(My emphasis)

However the definition of "passing over", created an unexpected problem. For the purposes of this Act, a communication:

> (a) was taken to start passing over a telecommunications system when it is sent or transmitted by the person sending the communication; **and**
>
> (b) was taken to continue to pass over the system until it becomes accessible to the intended recipient of the communication. "

(my emphasis)

Reluctantly, I accepted that an email had already passed over a telecommunication system and this provision would not assist. At a point where I began to consider the option referred to above more seriously, I found an amendment had been made to the 1979 legislation in 2006.[2]

The 2006 Act inserted into the *Telecommunications (Interception and Access) Act* (or *Telecommunications (Interception) Act* 1979 as it was originally called), a system addressing unauthorised access to stored communications. An email is held in three locations: the sender's server, the recipient's server and the computer of the recipient when it is downloaded.

The EM to the 2006 Act relevantly states:

> Item 1 inserts a definition of *stored communication* into subsection 5(1) of the Act. A stored communications is defined to mean a communication with four specific elements:
>
> First, the communication must have passed over a telecommunications system...to avoid things such as drafted emails...
>
> Second, the communication must not be passing over that or any other telecommunications system...
>
> Third, the communication must be held on equipment operated by the carrier at its premises...
>
> Fourthly, the communication must be accessible to the intended recipient of the communication.

The result being, that emails were now addressed after 2006, in relation to unauthorised access. The Federal Court of Australia or a court of a State or Territory may, on the application of an aggrieved person, grant the aggrieved person remedial relief in respect of the access by making such orders against the defendant as the court considers appropriate. [3]

---

[1] *Telecommunications (Interception and Access) Act* s 7(1).
[2] The *Telecommunications (Interception) Amendment Act* 2006 (the "2006 Act"); Available at: http://www.comlaw.gov.au/Details/C2006B00009/Explanatory%20Memorandum/Text
[3] Section 165(3) of the *Telecommunications (Interception and Access) Act*.

The practical problem

Lack of evidence is an issue. But for the statement of D, B would not have had confirmation of the system's compromise. An examination by a forensic expert of B's systems, reveals that during the examination, it was noted that the hosting service appeared to have been compromised (hacked), the service was a type where multiple tenants occupied the same service, so attributing the source of the compromise was problematic. The solution offered by the expert was to obtain access to C's staff mobile phones.

We were now in the area of an Anton Piller type application. B was armed with a respected expert who could not categorically identify C with the hacking activities or at all and a former employee of C who said that C was able to access B's emails, but who may have their own agenda against C.

The grant of a search order is a serious interference with the rights of an individual. Accordingly, there must be a strong prima facie case.[4]

Suggested solutions

The evidence given by D might be more powerful. There may be several former employees of C who might give evidence of the practice.

It seems an appropriate case for an application for preliminary discovery to be made, where B is a person who '*reasonably believes that he or she may have the right to obtain relief in the Court from a prospective respondent whose description has been ascertained'*.[5]

The application would be supported by the evidence of an expert who has reached the conclusion that there is evidence of hacking but that the responsible party cannot be identified with accuracy. In addition, there is a signed statement of D, a former employee of C, whose evidence is that he accessed B's emails whilst employed by C.

Critical to the application being made *ex parte*, is the expert's opinion as to whether the evidence on C's staff mobiles may be easily removed or whether the traces of such activity will leave an indelible footprint. In addition, there must clearly be an effort to make reasonable inquiries.[6] The 'dead end' the expert has reached will assist in this regard. The evidence of D in the case is the basis for the requirement that B reasonably believes that C has or is likely to have or has had or is likely to have had in its control, documents directly relevant to the question whether B has a right to obtain the relief and inspection of the documents by B would assist in making the decision.[7]

Of further support for the orders on an ex parte basis, is the expert's evidence that he or she will only need the mobile phones of the staff members for several hours, whilst they are copied. There

---

[4] *Television Broadcasts Limited v Nguyen* 15 IPR 97 at 102 per Lee J.
[5] Rule 7.23 of the Federal Court Rules 2011.
[6] Rule 7.23(1)(b) of the FCR.
[7] Rule 7.23(1)(c) of the FCR.

will no doubt be confidentiality issues which coiled be addressed by limited access to the information to the expert and legal advisers of B.

The important thing is to determine and have the expert opine, as to the ease or otherwise of extinguishing the evidence of the mobile phones of the staff of C.

Dimitrios Eliades
Barrister, Brisbane
19 October 2012