Blackstone
CHAMBERS

Presented by IRS in association with Blackstone Chambers

"Employment Law in the High Court"

Friday 25th February 2005

CONFIDENTIAL INFORMATION AND DATABASE PROTECTION

ROBERT HOWE

Blackstone Chambers, Blackstone House, Temple, London EC4Y 9BW

Tel: +44(0)20-7583 1770 Fax: +44(0)20-7822 7350 Email: clerks@blackstonechambers.com

www.blackstonechambers.com

Contents

CONFIDENTIAL INFORMATION AND DATABASE PROTECTION

A. INTRODUCTION

1. A frequent feature of many High Court employment disputes is the protection of confidential information. In fact, an employer's fear that his employees (or ex employees) might have "stolen" his "confidential" information is often the main motive for starting proceedings in the first place.

2. Most employment lawyers will therefore be familiar with the arguments about what does and does not amount to "confidential information", about whether employees can contact customers who they can find in the telephone directory without reference to any other information, and so forth.

3. The purpose of this short talk is not consider the (somewhat confused) caselaw on confidential information in great detail, but instead to focus on the advantages which can sometimes be gained from relying on breach of database rights. Database infringement can sometimes provide certainty when common law concepts of "confidential information" fail.

B. CONFIDENTIAL INFORMATION

1) General Principles

4. Following the Court of Appeal's decision in *Faccenda Chicken v Fowler*[1986] IRLR 69, as subsequently interpreted in cases such as *Lansing Linde v Kerr* [1991] IRLR 80, CA and *PSM International v Whitehouse* [1992] IRLR 279 (CA), the outline principles regarding confidential information (so far as relevant to the typical High Court employment case) are fairly easy to summarise. They are just rather difficult to apply in practice.

5. Firstly, *Faccenda* established the idea of three classes of information, to which different considerations apply:

5.1. Class 1: trivial or public information which is not confidential at all, and which an employee is free to disclose or use.

5.2. Class 2: information which the employee must treat as confidential (either because he is expressly told that it is confidential or because from its character it obviously is so) but which once learned necessarily remains in the servant's head and becomes part of his own skill and knowledge applied in the course of his master's business. It might well be a breach of the employee's duties if he were to disclose this information whilst employed, but there is generally no restriction on him using or disclosing such information after termination of the employment.

5.3. Class 3: specific trade secrets so confidential that, even though they may necessarily have been learned by heart and even though the employee may have left the service, they cannot lawfully be used for anyone's benefit but the master's.

6. Secondly, the classes of information are vague and present considerable problems of definition. In *Faccenda* itself, the Court of Appeal suggested that in order to determine whether any particular item of information comes within Class 3 it is necessary to consider all the circumstances of the case including, but not limited to, the nature of the employment, the nature of the information, whether the employer impressed on the employee the confidentiality of the information and whether such information may be easily isolated from other information which the employee is free to use or disclose.

7. Subsequent to *Faccenda*, it has been said that the correct test is to distinguish between "objective" and "subjective" knowledge (see *SBJ Stephenson Ltd v Mandy* [2000] IRLR 233, per Bell J). This distinction derives from a passage in Lord Shaw in *Herbert Morris Ltd v Saxelby* [1916] 1 AC 688 at p.714:

> *'Trade secrets, the names of customers, all such things which in sound philosophical language are denominated objective knowledge – these may not be given away by a servant; they are his master's property, and there is no rule of public interest which*

prevents a transfer of them against the master's will being restrained. On the other hand, a man's aptitudes, his skill, his dexterity, his manual or mental ability – all those things which in sound philosophical language are not objective, but subjective – they may and they ought not to be relinquished by a servant; they are not his master's property; they are his own property; they are himself. There is no public interest which compels the rendering of those things dormant or sterile or unavailing; on the contrary, the right to use and expand his powers is advantageous to every citizen, and maybe highly so for the country at large."

8. Another test which has been proposed for the purposes of distinguishing between "Class 2" and "Class 3" information is what might be called the "honesty test" – see e.g. *FSS Travel v Johnson* [1998] IRLR 382 (CA). This test derives from Cross J in *Printers & Finishers Ltd v Holloway* [1965] 1 WLR 1 at 5 A-C:

> *"If the information in question can fairly be regarded as a separate part of the employee's stock of knowledge which a man of ordinary honesty and intelligence would recognise to be the property of his old employer and not his own to do as he likes with, then the court, if it thinks that there is a danger in the information being used or disclosed by the ex-employee to the detriment of the old employer, will do what it can to prevent that result by granting an injunction."*

(cited with approval in e.g. *FSS Travel* at Paragraph 34)

9. Staughton LJ in *Lansing Linde v Kerr* [1991] IRLR 80 (CA), at 84 put the test yet another way – he proposed a "harm" principle:

> *"It appears to me that the problem is one of definition: what are trade secrets, and how do they differ (if at all) from confidential information? Mr. Poulton suggested that* ***a trade secret is information which, if disclosed to a competitor, would be liable to cause real (or significant) harm to the owner of the secret. I would add first, that it must be information used in a trade or business, and secondly that the owner must limit the dissemination of it or at least not encourage or permit widespread publication.***
>
> ***That is my preferred view of the meaning of trade secret in this context.*** *It can thus include not only secret formulae for the manufacture of products but also, in an*

appropriate case, the names of customers and the goods which they buy. But some may say that not all such information is a trade secret in ordinary parlance. If that view be adopted, the class of information which can justify a restriction is wider, and extends to some confidential information which would not ordinarily be called a trade secret."
(emphasis added)

10. Thirdly, it has often been said that if an employer cannot define with precision the confidential information which he wishes to protect, then that in itself may disentitle him to relief. The Court will not make orders restraining use of "confidential information" in general terms - it will only restrain the use of specified, identifiable information: see eg *Lawrence David v Ashton* [1989] IRLR 22 (NICA)[1]; *FSS Travel v Johnson* [1998] IRLR 382 (CA)[2].

11. This might seem a little unfair, given the difficulties which the Court of Appeal has itself encountered when attempting to define what constitutes protectable "confidential information". The other great practical problem for an employer is often that he does not know precisely what information the employee may have taken. He is therefore driven to seek an order in broad and general terms.

2) Protecting confidential Information – Some practical problems

12. "Confidential information" is therefore an inherently slippery concept. In practice, an employer trying to restrain breach of confidence frequently encounters various obstacles:

---

[1] Per Balcome LJ: *"I have always understood it to be a cardinal rule that an injunction must be capable of being framed with sufficient precision so as to enable a person enjoined to know what it is he is to be prevented from doing. After all, he is at risk of being committed for contempt if he breaks an order of the court. The inability of the plaintiffs to define, with any degree of precision, what they sought to call confidential information or trade secrets militates against an injunction of this nature. That is indeed a long recognised practice."*

[2] Per Mummery LJ: *"Lack of precision in pleading and absence of solid evidence in proof of trade secrets are frequently fatal to enforcement of a restrictive covenant."*

12.1. **Defining what is "confidential":** as pointed out above, this is often difficult.

12.2. **Decay of Confidentiality**: Confidential information may become out of date, and cease to merit protection over time.

12.3. **Damages and Remedies:** Even where actual or threatened breach of confidence is established, the Court has a broad discretion as to remedy. If the Court considers that the information is not that "important", or only marginally important, an injunction may be refused, or nominal or limited damages may ultimately be awarded.

12.4. **Public interest defences:** The employee may also argue that the public interest requires that he should be allowed to use or disclose the information.

C. THE DATABASE RIGHT

13. The Database Right derives from the EC Database Directive[3]. The Database Regulations[4] give the Directive effect in domestic law (both by amending the Copyright Designs and Patents Act 1988 and by the free-standing provisions of the Regulations). This is a technical field which raises considerable complications at its fringes (such as in the application of its transitional provisions, or in the overlap with copyright per se). What follows is a brief tour of the parts which might be useful to an employment lawyer.

14. It will be seen that the Database Right is very broad. It may be exceptionally useful to an employer who is faced with an employee or employees who have taken parts of a computer database (e.g. classically, customer or supplier lists).

---

3 Directive 96/9/EC

4 *Copyright and Rights in Database Regulations 1997*, SI 1997/3032

1) What is a "Database" under the Regulations?

15. For the purposes of the Regulations, a Database is "*a collection of independent works, data or other materials*" which:

    (1) are "*arranged in a systematic or methodical way*", and

    (2) are "*individually accessible by electronic or other means*"[5].

16. This is a broad definition, and is likely to cover most computer systems which contain lists of contacts and the like.

2) When does the Database Right arise?

17. Not every "database" qualifies for the Database Right. A right subsists only if "*there has been substantial investment in obtaining, verifying or presenting the contents of the database*"[6]. However, "*investment*" is also given an expanded meaning. It "*includes any investment, whether of financial, human or technical resources*". Again, this is likely to enable most employer's databases to quality for the right, provided that some significant effort has been devoted to compiling and maintaining it.

3) Who Owns the Right?

18. The "maker" of the database is the first owner of the right[7]. The "*maker*" is usually[8] "*the person who takes the initiative in obtaining, verifying or presenting the contents of a*

---

5 Reg 12(1)

6 Reg 13(1).

7 Reg 15.

8 There are some exceptions concerning Crown databases – Reg 14(3) – (5).

database and assumes the risk of investing in that obtaining, verification or presentation shall be regarded as the maker of, and as having made, the database"[9].

19. In a typical employer/employee relationship, this person would nearly always be the employer. However, the point is put beyond doubt by Reg 14(2), which provides that where a database is made by an employee is the course of his employment, "*his employer shall be regarded as the maker of the database*", unless there is an agreement to the contrary.

4) How is the Database Right infringed?

20. When it comes to infringement, the Regulation is again very broadly framed. A person infringes the right if, without the consent of the owner, he "*extracts or re-utilises all or a substantial part of the contents of a database*"[10].

21. The definitions[11] give fairly generous meanings to these expressions:

    21.1. "*Extraction*" means "*the permanent or temporary transfer of*" any of the contents of a database "*to another medium by any means or in any form*". This would very probably cover most means by which an employee might take parts of a database: downloading it, copying it to disc, sending it by email, or printing it out.

    21.2. "*Re-utilisation*" means making the contents of a database "*available to the public by any means*". This is unlikely to be relevant to the type of case where a former employee wants to use the information for a new employer or a competing business of his own, but may be important where the employee is threatening to disclose the information to others.

---

9 Reg 14(1).

10 Reg 16(1).

21.3. "*substantial*", in relation to any investment, extraction or re-utilisation, means "*substantial in terms of quantity or quality or a combination of both*". This is a concept derived from copyright, and likely to be interpreted in a similar way. It is well established that the question of whether there has been "substantial" copying is not determined simply by mechanically comparing the proportion of the work copied to the total of the work – the question is whether, having regard to both the nature and quantity of the copying, an important or significant part of the work has been used. For example, even a few bars of music may be substantial part of a musical work if they are a recognizable reproduction of the essential part of the melody. It is also often said that "*what is worth copying is prima facie worth protecting*"[12].

21.4. In addition, even where the individual extraction is insubstantial, the Regulations also provide that repeated and systematic extraction or re-utilisation of insubstantial parts of the contents of a database may amount to the extraction or re-utilisation of a substantial part of those contents[13].

22. The combined effect of these provisions is that in many employment cases, such as where an employee has downloaded a customer list, or details of pricing or tendering information, from his employer's computer system, the employer may well be entitled to sue for infringement of his database right. The database is broadly defined; the threshold for creation of the right is low; and the infringement provisions are broad.

---

11 Reg 12(1)

12 Per Petersen J in *University of London Press Ltd v University Tutorial Press Limited* [1916] 2 Ch 601 at 610, approved by both Lord Reid and Lord Pearce in *Ladbroke (Football) Ltd v William Hill (Football) Ltd* [1964] 1 WLR 273 at pp.279 and 293

13 Reg 16(2).

5) Advantages over common law "confidential information" claims

23. Whilst not a panacea for all problems, the great strength of the *sui generis* database right is that its key purpose is to protect business investment in data against *unfair use*. It does so:

(1) irrespective of considerations of confidentiality and duration of confidence;

(2) irrespective of considerations of originality;

(3) because it focuses on the existence or not of "a substantial investment in obtaining, verifying or presenting the contents of the database";

(4) because infringement in this context is demonstrated by extraction or re-utilisation or all or a substantial part thereof – naughty employees generally take the lot and decide what they need later;

(5) with the result that with appropriate steps in advance (contents of T&Cs, design of database protocols, record keeping re. data entry, amendment and investment) proof of the existence of such a right should be comparatively easy;

(6) so as to create a "mixed IP right", almost halfway between copyright and confidence; but

(7) with the potential for the remedial flexibility of both (i.e. final remedies including damages, accounts etc, interim remedies including delivery up and springboard injunctions).

24. Put together these factors go some considerable way to mitigating the drawbacks of the standard springboard template in information theft cases as:

(1) with good record-keeping, coupled with well drafted T&Cs should make proof of the relevant IP right comparatively simple; infringement in the form of copying will be as easy/difficult to prove as ever – the same case made on the same inferences will probably be made;

(2) arguments about confidentiality, duration of confidence and the employee's ordinary knowledge and skill should also be side-stepped, saving cost in preparation and argument of the case, and enabling speedier preparation for Court;

(3) defences will be reigned back to narrower IP type defences;

(4) remedies for the employer are broader. The rights and remedies of a copyright owner under ss 96 to 98 of the CDPA apply to the owner of a database right; and in copyright cases there is a prima facie right to a permanent injunction to restrain infringement[14]. Infringement of the database right may also entitle the owner to claim "additional" (or flagrancy) damages under Section 97 of the CDPA[15].

25. Where the client is prepared to go the whole distance, there is no reason in principle why a database claim should not be combined with a confidentiality case and/or a copyright claim[16]. But because of the advantages set out above:

---

14 See e.g. *PPL v Maitra* [1999] 1 WLR 870 (CA)

15 Reg 23.

16 Although it is important to note that there is an additional requirement in order for *copyright* to subsist in a database: that by reason of the selection or arrangement of the contents, the database constitutes the author's own intellectual creation (CDPA, Section 3A(2)). It is therefore unlikely that a claim for infringement of copyright in a database (as opposed to other materials) will add much to a claim for infringement of the database right.

(1) it should also be a candidate for stand alone relief in appropriate cases; and as such

(2) should merit careful consideration when drafting standard T&Cs, company procedures, computer manuals and protocols and when designing computer use recording keeping procedures.

ROBERT HOWE

Blackstone Chambers

February 2005