Secrets, Strategies and Proposals for Reform in the United Kingdom

by

Jon Lang

COMPUTER AND TELECOMMUNICATIONS
LAW REVIEW

VOLUME 8, ISSUE 8
NOVEMBER 2002

THOMSON
SWEET & MAXWELL

Sweet & Maxwell Limited
100 Avenue Road,
London NW3 3PF
Law Publishers

Secrets, Strategies and Proposals for Reform in the United Kingdom

We all know that prevention is better than cure. Indeed, in many cases, like misreporting expenses as items of capital expenditure or allowing the disclosure of secret commercial information, prevention is the only sensible option. Yet so often, it is not until competing and very similar products appear on the market in unseemly haste or in otherwise questionable circumstances, perhaps eroding any first mover advantage a company may have been banking on to recoup its R & D overspend, will suspicions be aroused and thought given to the protection of commercial know-how. Because it is then that commercial directors will start asking their technical directors some difficult questions. And the technical directors will be tetchy—sometimes because of begrudging admiration for the competition but sometimes because they suspect foul play—the use of their own secret know-how by a competitor who most definitely should not have had access to it.

It is then that lawyers are called in and will start asking questions about know-how protection strategies, designation of documents, if access to information was restricted in any way, how could this happen, etc., etc. Whilst these questions might conjure up images of barn doors and bolting horses, the body of law that governs this area, often referred to as the law of breach of confidence, makes these sorts of questions necessary. Since the eighteenth century there has been much case law developed around actions brought to restrain, or recover compensation for, breaches of confidence. Whilst these cases often involved famous people and their private lives (and still do of course), many have also involved the misuse of commercial information of one company by another. What must be shown before relief is granted by the courts in an industrial espionage type case is that the information suspected to have been wrongly acquired was confidential in the first place. This often involves an analysis of how it was treated internally by the company seeking relief. Next, it must be shown that the circumstances under which the information was obtained gave rise to an obligation of confidence. Thus, some form of relationship is usually demonstrated between the owner of the information and the person alleged to have committed the misappropriation. This is not always easy in blatant industrial espionage cases if dealing with a complete stranger as opposed to, for instance, a disaffected member of staff passing secret information to a competitor. However, it is fairly clear now that the reprehensible means by which a person obtains information is relevant and the absence of a relationship in the true sense will not be prohibitive in an otherwise deserving case. And finally, an unauthorised use of the information (and detriment) must also be shown which again is not too difficult in cases of blatant misappropriation. Hence the questions! But out of the questions and a full analysis of what has happened usually comes not just a sustainable case (hopefully) but better protection for trade secrets within the organisation concerned. Once bitten, twice shy!

But a question that is often asked is why the law does not provide any real deterrent for this kind of unacceptable commercial activity. The commercial director will still be angry even after promises from his lawyers that any case mounted will succeed, not least because when dealing with trade secrets misappropriation, it is usually very difficult, if not impossible, to restore the secrecy of information that has been misappropriated. Moreover, the company's whole marketing strategy (and of course level of sales) may be adversely affected by competing goods (suspected to have been developed with filched know-how) being put on the market at the same time or even before the innocent company's own goods. Distributors may be confused, embarrassing questions will be asked over coffee at trade shows; perhaps even enraged sales directors will try and gather up the suspect products at the competitor's own trade show stand escalating yet further what might already be a very embarrassing situation. It has been known to happen! Thus, even complete victory in court rarely leaves a wronged party totally satisfied. They will still want retribution! And, in the same way as in many asset recovery type actions, discussion will take place about police involvement. If there has been a break-in and files stolen, there will be obvious criminality. But with trade secrets misappropriation, the industrial spy (for want of a better expression), be it an employee, consultant or cleaner, will not need to deprive the owner of possession of the trade secret (and indeed will usually not want to for fear of

arousing suspicion) to gain the advantage that they or others on whose behalf they act, seek. Because information (not the paper, CD-ROM or other medium on which it is contained), is not like property in the conventional sense. When a car is stolen, the owner no longer has possession of it. It is not there when he arrives at the station car park. There is nothing ambiguous about it. It has gone! But, in the case of information, the bad guy who commits to memory secret chemical formulae, business plans or technical information is depriving the owner not of the information itself but of the monopoly he enjoys over that information. Thus, the owner is still able to exploit the know-how, only without the advantage of exclusivity. The fact that the industrial spy does not "permanently deprive" the owner of the information in the same way as the thief permanently deprives an owner of a car, leaves a charge of theft inappropriate.

However, there is a far more fundamental reason why a charge of theft cannot be founded. It is trite law that information is not property for the purposes of the Theft Act. Thus, in 1979, a cheeky student who "borrowed" an exam paper (before the exam) but then put it back again, was acquitted of theft; he did not steal the piece of paper but merely appropriated the information on it and information, not being property, destroyed the prosecution case.

So, whilst the criminal law does not assist the victim in the case of pure theft of information (at least not yet!), practitioners in this area generally do not have too much difficulty in building civil cases based on the law of breach of confidence. But a discrete civil law in this area, as exists for instance in the U.S. in the Uniform Trade Secrets Act, which has been adopted in several states, might be helpful, not least because it would do away with some of the difficulties and uncertainties that arise when applying judge made law developed in piecemeal fashion over the last few hundred years. And if "theft" of a trade secret were criminalised (as it has been in the U.S. with The Economic Espionage Act, and in many other European jurisdictions) it might be even more helpful, particularly to lawyers trying to placate the once bitten client who might well be wondering whether all the R & D effort is worth it for the next product in design phase. It might also act as a deterrent! Whilst we have in the United Kingdom, criminal liability arising in certain circumstances where other types of intellectual property is concerned (under the Copyright, Designs and Patents Act and the Trade Marks Act), and also an offence of hacking under the Computer Misuse Act, as yet we have nothing which criminalises the misappropriation of pure information. That is not to say, however, that we have been short of debate on the subject!

Many practitioners in this area will be familiar with the often quoted passage from a speech by Sir Edward Boyle in the House of Commons on December 13, 1968 when, during the second reading of the Industrial Information Bill (a Bill designed to tackle industrial espionage) he said, after quoting a passage from a letter written by Mr Alan Campbell Q.C. to *The Times* a year before:

> "I am asking whether the law is adequate, whether the time has not come when we should add to the provisions in the law against civil wrongs and whether we do not now also need provisions against the criminal offence of industrial theft. It is not too much to say that we live in a country where, in Mr Campbell's words, the theft of the boardroom table is punished far more severely than the theft of the boardroom secrets".

The position is not really any different today. The Law Commission, in their *Report on Breach of Confidence*, published in 1981, considered whether the civil law in this area should be left to be moulded by the courts or whether it was desirable, given its then present state, for there to be at least some statutory framework setting out the main principles. The Law Commission concluded, in the light of what they saw to be the uncertainties and inadequacies of the present law, that it would be unsatisfactory to leave the problem areas to be resolved by piecemeal litigation and that the law on breach of confidence should be replaced with a new statutory action. The problem areas identified were various but included the protection available for improperly obtained information regardless of any relationship between the wrongful acquirer of a trade secret and its rightful owner.

Whilst the Government accepted the Law Commission's recommendations, nothing has been done. We are still left with courts working out the law in this area on a case-by-case basis although by doing so some of the problem areas identified by the Law Commission do seem to have been overcome.

The Law Commission later picked up the theme of Sir Edward Boyle's proposed Industrial Information Bill more squarely when they examined the effectiveness of the law in deterring breaches of confidence and their Consultation Paper, published

in November 1997, specifically sought views on the criminalisation of the deliberate misuse of trade secrets.

The Law Commission's view at this time was that there were arguments in favour of criminalisation, provided a defence to a charge could be drafted in precise terms. This view was based on the fact that theft of a trade secret is analogous to theft of property and should be treated in a similar way, and the very real economic importance, both from a private and public interest stand point, of protecting investment in know-how. Moreover, given the lack of authority for the award of exemplary damages in breach of confidence cases, doubts over whether the award of exemplary damages, even if available, would itself be enough of a deterrent, the limited value of an injunction once the misuse has taken place and the costs and delay in civil law claims for breaches of confidence, they provisionally concluded that the imposition of criminal liability would be a more effective way of regulating trade secrets misuse than civil liability alone.

Comments were to be submitted in response to the Law Commission's consultation paper by March 1998. Whilst many respondents are known to have been generally in favour of the Law Commission's provisional conclusions and proposals for criminalisation, many having earlier expressed their views pursuant to a previous consultation process, the Law Commission has not yet published a report and made known their final recommendations. This is probably because they will first await the response to their report entitled "Fraud", published at the end of July 2002, following a subsequent consultation process commenced in April 1999 by their paper entitled, *Legislating the Criminal Code—Fraud and Deception*. This consultation paper was published in response to a request by the Home Secretary to the Law Commission in April 1998 to examine the law on fraud and to examine, for instance, whether it meets the needs of developing technology, and to consider whether a general offence of fraud would improve the criminal law. Because it is possible that any general offence of fraud would be wide enough to include criminal liability for misappropriation of trade secrets, full consideration of a discrete law in this area is likely to be placed on the back burner, at least for the moment.

So, at present, lawyers make do with what they have when advising clients—the civil law of breach of confidence, judge made piece-meal case law. It may not be much of a deterrent in the sense that the bad guys know they will get slammed in the clink if they get caught stealing the boardroom secrets, but it is flexible and there are few cases where redress has not been available in deserving cases. But claimants that have helped themselves and have gone to lengths to keep secret and secure information that should be kept secret, which includes having in place strategies and policies that are adhered to throughout their organisation, will not only reduce the risk of trade secret misappropriation in the first place, but stand in a much better position, when seeking relief from the civil courts, of persuading a judge that the information in question was truly secret and worthy of protection. So it pays to know what's secret and to do everything possible to keep it that way!

JON LANG
Litigation Partner
White & Case,
London