BILETA

14th BILETA Conference: "CYBERSPACE 1999: Crime, Criminal Justice and the Internet".

Monday, March 29th & Tuesday, March 30th, 1999.
College of Ripon & York St. John, York, England.

The Extension of the Criminal Law to Protecting Confidential Commercial Information: Comments on the Issues and the Cyber-Context

CD Freedman[*]
Herchel Smith Research Fellow in Intellectual Property Law
Emmanuel College, Cambridge

Introduction

Constructing civil remedies and criminal laws to deal with the misappropriation of confidential information has always presented conceptual and practical difficulties for the law. Much has been done in recent years with respect to protecting personal data against interference, but much remains to be done in the area of confidential commercial information. It is clear that whilst the economic value of such information may justify its legal protection, its very nature makes the application of legal principles to it problematic. The approach to civil liability for misappropriation in English law has sought to avoid these complications by adopting an indirect approach to protection, focusing on the enforcement of obligations of confidence arising in law or equity in relation to such information rather than the information itself. The criminal law has been applied in an even more hesitating fashion. Criminal liability is contingent on the misappropriative act itself being incidentally proscribed by law, and there are significant gaps in the present scope of criminal law coverage. The release in late 1997 of a consultation paper by the Law Commission with its provisional recommendations for a new criminal offence of misuse of trade secrets,[1] is but the latest development highlighting the inadequate status of the criminal law in this area.

In this paper, I shall review the nature of the problem and some of the relevant legal issues. The best response to the present state of the law on these issues would be a complete revision of civil and criminal liability to offer a comprehensive model of protection. Notwithstanding that such global reform of the law in this area is probably not in the cards, the position advocated here is that the criminal law is indeed a appropriate vehicle through which to deter the misappropriation of confidential commercial information. However, the scope of any new law must be carefully circumscribed - if it is drawn too wide, the law runs the danger of acting outside of the articulated rationale for criminal liability and endangering other legitimate interests (particularly in the cyberspace context). If it is drawn too narrow, any new law may very well be ineffective. I would suggest that there are a number of difficulties, both doctrinal and practical, that must be resolved prior to enacting new legislation in this area and will present a few observations upon the more critical issues for those primarily interested in the implications for cyberspace.

I. The Need for Effective Legal Protection in the Modern Technological Context

1. Confidential Commercial Information: Definitional Problems and Functional Description

The commercial value of *confidential commercial information* [2] has traditionally provided the primary justification for civil remedies and criminal sanctions to deter misappropriative activity in English law and elsewhere.[3] This is reflective of the fact that such information, in the form of trade secrets or "know-how" or otherwise, has always been an important business asset. In the contemporary context, the need to protect such information is made even more acute as innovation has become the central feature of post-industrial developed economies,[4] making knowledge-based assets increasingly critical economic resources in such economies. In this sense it is clear that threats to the security of confidential commercial information fit within the convergence of two technology-related trends: the rise in value of intellectual property and information in post-industrial economies arising from innovations in technology, and the rise in economic crime as a phenomenon in national and international commercial life itself stemming partly from technological innovation.[5] Before turning to the state of the law and how it might be reformed, it is useful to say a brief word respecting the nature and economic function of confidential commercial information in the modern technological context.

If one tries to create a definitive typology of confidential commercial information, the exercise seems doomed to failure.[6] Not only does the intangible and indivisible nature of information make the task difficult,[7] but the myriad forms that confidential information can take in a commercial context - from technical pre-patent schematics to more generalised know-how and operational procedures - renders any attempt at an exhaustive definition practically meaningless.[8] In short, exhaustive classification is an unproductive exercise that is best avoided. One can, however, seek to describe the function and importance of confidential commercial information in economic terms, and draw appropriate conclusions to be used in constructing legal models protective of such information.

Basic economic principles suggest that the law ought to provide a degree of protection to confidential commercial information in order to encourage sufficient investment in the creation of new knowledge-based assets, whilst at the same time avoiding the creation of an artificial scarcity of such resources through over-protection.[9] This balance between the protection of information to encourage investment in development with adequate access to information is a delicate one - economic efficiency in information will not be achieved through over-investment in the creation of informational resources or through duplication of resources to create the same information resources. [10] Moreover, individuals ought be guided by the clear availability of suitable legal remedies in determining the level of private resources, if any, that ought to be dedicated to providing additional protection for such information so that these private expenditures may be optimised.[11] On a global level, then, it is the task of law-makers to achieve this fine balance between protection through legal remedies and self-help and access through appropriately constructed laws.

2. Regulation and the Modern Technological Context

This basic economic paradigm must be viewed in the contemporary context; a context in which the innovation of new knowledge-based products is increasingly important to post-industrial developed economies. The process of innovation is itself often a joint and serial activity; a process in which developers share and exploit resources and build on each other's work in an attempt to create new products and wealth. In this sense, confidential commercial information in its various forms functions within this cycle of innovation as both a commodity (valuable in itself) and as a resource (to be exploited by commercial actors).[12] Central to the success in exploiting such informational resources is the ability to share the information without risk of destroying its value through illicit acquisition, use or disclosure. This need to be able to exploit valuable informational resources in partnership is critical to the ongoing refinement of technologies; the exchange of confidential information in this sense is, to use one judge's phrase, "both necessary and expected."[13]

Having said that confidential business information is increasingly valuable in the modern technological context, one can also add that this context itself has changed the nature of commerce with implications for any attempt at regulation in this area. As the Alberta Law Reform Institute reported when it looked at the protection of trade secrets in Canadian law:[14]

> …technology has changed the nature of modern business in a number of respects. [first] Business has become a race against time. Technology is volatile and short lived. The increasing pace of technological change means that perfectly good ideas and inventions may be obsolete before they can be patented and brought to the market place. This problem is complicated by the fact that different parts of a product may have different development rates…Today the business advantage lies in technology. The business pressures to know what competitors are doing are therefore intense….[second] employee mobility is greater than any time in history…[third] technology has made espionage so much simpler. There is now an array of sophisticated equipment, much of it derived from military developments, which makes espionage within even well run enterprises a real threat.

The modern technological context, then, is a business environment where information is critical in different stages of product development, is quickly out of date, and is susceptible to misuse or unauthorised disclosure by those having had control over it or being able to acquire it illicitly. The presence of a global networking environment highlights these problems and makes the need for effective legal treatment even more critical.[15] In such circumstances, I would suggest, there is a need for effective deterrents against misappropriative acts both to maintain the value of informational assets and to protect the integrity of the innovation cycle.

II. The Present State of the Law

1. Problems in Ascertaining the Precise Nature of the Mischief to be Remedied

To follow correct form in evaluating the merits of criminalising certain acts in relation to confidential information, the discussion ought properly to begin with a detailed analysis of the mischief to be remedied, identify those specific acts which ought to be proscribed, and consider the public policy implications of proscribing such acts. Unfortunately such a traditional approach is made difficult by the lack of sufficiently independent data upon which to base such an analysis, a point that I shall return to later. One should recognise at the outset that considering new regulation without such an independent review of the nature of the mischief to be remedied will undoubtedly run into trouble at some stage.

Notwithstanding the lack of data respecting misappropriative activity, what can be said in general terms is this: confidential commercial information is primarily at risk in two types of scenarios - situations in which information is acquired through illicit means and without the complicity of one rightfully in possession, and, situations in which the information is obtained from one rightfully in possession but in breach of that person's obligations. The first scenario is essentially variations on the theme of industrial espionage; acts which can themselves be characterised as purely private activity (whether local or trans-national) or as state-sponsored acts.[16] The second set of scenarios encompass matters ranging from simple disclosure by ex-employees to new employers to deliberate disclosure by present confidants claimed to be in the public interest.

2. Property in Confidential Information and the Approach to Civil Liability

With some hesitation, it seems necessary to include some recognition of the traditional debate respecting proprietary rights in confidential information within this discussion.

Notwithstanding the fact that, as one scholar put it, "[t]here is a natural and deep-seated tendency… to treat confidential information in proprietary terms,"[17] the inability to exclude others from its use or possession as is required in the normal legal sense of *ownership*[18] would seem to deny it proprietary status as a result. Whilst the issue has not been definitively settled in English law,[19] the great weight of judicial[20] and academic[21] comment is inconsistent with ascribing to such information a property characterisation and as such the normal criminal law of theft is inapplicable.[22] In American law,[23] by comparison, it is clear that specified types of commercial information in the form of trade secrets may be property for both the purposes of certain civil actions[24] and criminal offences.[25] Given that the balance of rights achieved in a ready-made form by property law is seemingly unavailable in this exercise, the challenge for the English criminal law is to identify those matters of private consequence that are in the public interest to protect, and how those interests might be furthered through the availability of criminal sanctions.

In private English law, confidential information is indirectly protected from unauthorised use or disclosure through the enforcement of obligations of confidentiality in relation to such information. Obligations may be expressly or implicitly agreed to, or judicially constructed in appropriate circumstances, as between the parties. It has been said that the protection of confidential information in the form of the equitable action of breach of confidence, the primary vehicle for civil liability outside contract, is *sui generis* in the sense that it has arisen in a multi-jurisdictional fashion, emanating from principles of property, contract, and equity.[26] It seems sufficiently clear now that the action for breach of confidence falls completely outside tort.[27] Others would put the action in none of these jurisdictional pigeonholes in a contemporary context, seeing it as but another manifestation of the law of restitution.[28] Whatever one's view of the evolutionary antecedents or the jurisdictional basis of the action, it is now sufficiently clear that there exists an independent jurisdiction in equity arising on principles of good faith and conscience to restrain unauthorised use or disclosure of confidential information.[29]

Whilst the existence of this independent jurisdiction can now be seen as definitively settled, its scope and extent is still not fully developed. In a general sense, the contours of the action will depend very much on the nature of the information sought to be protected, the parties to the action, and the circumstances claimed to give rise to an enforceable obligation between the parties. Uncertainty respecting the parameters of this developing jurisdiction naturally colours attempts to introduce criminal law provisions into the same area.

3. The First Scenario: Conduct-Based Liability for Illicit Acquisition

The first scenario identified above respecting misappropriation are those situations where one not properly in possession of the information in question seeks to acquire it without the complicity of one properly in possession of the information. Conventional ploys like bribing and suborning employees are essentially variants on breach of confidence relying on receipt-based principles of liability, which I shall turn to below. The issue here is whether liability may follow based directly on the nature or method of acquisition, which is obviously relevant in technological contexts.

There is an obvious need to balance policy interests in this area; whilst business people have a legitimate interest in securing as much information as possible on competitors and their products, it is in no one's interest to have a completely unregulated marketplace. The Younger Commission described this fundamental consideration in these terms:[30]

> The main difficulty in considering the acquisition of industrial and commercial information is deciding where to draw the line between methods which consist of

> painstaking and legitimate gathering of business information and those which the law should treat as illegal. Most people would agree that it is part of the normal function of an efficient business man to be well-informed on his competitor's products, prices, sales promotions, and so forth; and most people would agree that it would be quite wrong for him to steal his rival's test samples or suborn his employees; but there are grey areas.

The lack of property in confidential information has resulted in an approach to liability in both civil and criminal law in this area that is highly unsatisfactory.

Criminal liability does not proceed from a generalised approach based on misappropriation directly; the lack of property takes the misappropriative act outside the law of theft.[31] Liability, then, is conditioned on the act itself being incidentally proscribed under statute (for example, under the *Interception of Communications Act 1985*, the *Copyright, Designs and Patent Act 1988*, the *Computer Misuse Act 1990*, or the *Trade Marks Act 1994*) or common law (primarily the offence of conspiracy to defraud), with each area having its own deficiencies.

Whilst it is beyond the scope of this paper to attempt an exhaustive analysis of the various criminal law proscriptions relevant to the remedy the mischief identified, I would suggest, much as the Law Commission recently advised,[32] that there are significant gaps in this incidental application of the criminal law. For example, "van Eck" reception devices used to capture the radiation from computer screens from public vantage points would not seem to run foul of the Computer Misuse Act 1990, as neither would reading confidential information off the screen directly, provided one has not caused the computer to perform a function within the meaning of that statute.

This is an undesirable state of affairs. One would think that the criminal law ought to be able to relieve the "decent and reputable trader's sense of helplessness"[33] in such circumstances.

What then of civil liability? It would seem natural to look to private law for norms of actionable conduct that might be useful in determining complementary criminal standards. Unfortunately, this is an area in which civil liability is most uncertain.

First, English law traditionally disfavours an approach that speaks to norms of "unfair competition" directly .[34]

Secondly, there are a number of inconsistent authorities as to whether a jurisdiction exists to find liability based on an acquisitive method standing alone, and what the test to find such liability ought to be. Various conduct-based standards have been proposed in the context of the equitable action of breach of confidence - amongst them that the act of acquisition was itself unlawful,[35] surreptitious,[36] reprehensible,[37] unconscionable,[38] wrongful,[39] and on the basis that the act falls under some generalised principle of liability grounded in the flexible nature of the equitable jurisdiction itself.[40] Many respected authorities argue that liability based on any such approach implicitly raises the spectre of liability imposed on highly idiosyncratic judicial views of general or commercial morality.[41] This is a criticism that is not unique to breach of confidence claims but reflects a fundamental tension that has been at the root of the long-standing judicial reluctance to import equitable doctrines into the commercial context.[42] On the other hand, one might argue that this trend seems to have abated somewhat in recent years as equity has undergone a period of revitalisation, especially in commercial contexts. Clearly the point is most uncertain.

4. The Second Scenario: Receipt-Based Liability for Breach of Confidence

With respect to the second set of scenarios, this is an area where private law has developed sophisticated receipt-based principles of civil liability in law and equity. The question for the criminal law in this area is whether criminal laws can be fashioned where civil liability is itself

insufficient - for example, where the defendant is judgement-proof.

The Law Commission's 1997 provisional recommendation supports the creation of a new offence of misuse of trade secrets that is exactly on point and would appear to be an appropriate way forward in this area. The model advocated restricts application of the law to offensive conduct in relation to unauthorised use or disclosure of a functionally defined subset of confidential commercial information, "trade secrets". The orientation of the provisional draft law is to punish an offender who knowingly misappropriates valuable information that is not "generally known." The offence is not overly broad in scope and the Law Commission intends actual prosecutions to be instigated only the worst cases and where the availability of civil remedies is inadequate in the circumstances of individual cases. The most appropriate use of such sanctions would be to punish employees, co-venturers, consultants and others who rightfully acquire information but then knowingly and intentionally misuse it. The scope of the provisional model deliberately does not speak to illicit modes of acquisition or the question of industrial espionage.

The cyberspace interest in this area does not so much lie in the methods by which the proscribed act of misappropriation is accomplished, but with the shape of cyberspace itself. It seems clear that certain types of employees are now increasingly mobile in modern information economies. This is especially true in respect of the services of technical experts and specialised managers who are active in the technology sectors.[43] There is a strong economic interest in making the skills of these experts available in the market-place on demand. However, as these same people work with the kinds of valuable confidential commercial information that is often the primary asset of their employers, there is an economic interest in ensuring that confidential information provided by employers remains confidential especially as against industry rivals. Over-protection of information through broad criminal liability in this area may very well inhibit necessary employee mobility and slow the natural pace of innovation unjustifiably.

III. Some Observations On Criminalisation and The Cyberspace Context

It seems appropriate to open this section of the discussion with some comments on the term "cyberspace." It would appear that the use of the expression (itself from William Gibson's seminal science fiction novel, *Neuromancer*) in both the academic literature and in the media is most popularly associated with the Internet, and perhaps exclusively so. It seems to me that this is an unduly restrictive definition of the term given that we are still in the infancy of the information age and our conceptions of cyberspace are equally in their early stages. I would suggest that given both the continually evolving nature of information technology and the increasingly inter-connectivity of information handling devices, cyberspace is more than merely the virtual space created by a global network of computer networks and I have used the term here in a broader sense. Whitaker has recently described cyberspace in this sense as a new world of "technological fusion" which itself "exists nowhere and everywhere… forever a *tabula rasa* in the sense that it is constantly being constructed and reconstructed, written and rewritten."[44] This seems an apt characterisation in my view.

I suggest that new criminal laws enacted to protect confidential commercial information will impact on cyberspace generally in two respects. Obviously regulation will impact upon the use of information technologies to commit acts that may be proscribed by law. In this sense, it is the definition of the subject-matter to be protected and the breadth of the proscription on activity that is all important. If the scope of regulation is overly broad, new laws may prove detrimental to the optimal exploitation of technologies such as the Internet. Regulation will also have an impact on the development of information technologies themselves, and in this sense it is again of critical importance that the scope of regulation be drawn with care else we risk an over-protection of information and a hindrance on the mobility of the specialised labour force that creates those

technologies that are cyberspace.

Having presented some thoughts on the problem of misappropriation of confidential commercial information and its inadequate legal treatment at present, the following remarks are directed to some of the issues relevant in the process of constructing new laws to protect confidential commercial information in the "information society" and some of the implications for cyberspace.

1. The Need to Develop a General Model Providing Comprehensive and Complementary Liability Rules in Private and Criminal Law

Intellectual property rights are of increasing economic importance in national and global economies. As such, the law must respond to the need for liability rules that provide adequate protection to maintain sufficient investment to encourage continued development without over-protecting these rights. In general terms, traditional rights such as copyright and patent have developed sophisticated structures which I would suggest will be able to respond to society's on-going needs.

The law respecting the protection of confidential information is very much an aspect of intellectual property law that is in need of revision. In the 19th century, a jurisdiction in equity was created to enable such information to be protected based on the enforcement of actual or constructive obligations of confidentiality. Whilst these principles have seen radical development in the United States in the ensuing years in both the fields of intellectual property law (the law respecting trade secrets, in both common law and statutory forms) and constitutional law (the recognition of privacy rights), English law has been content with a conservative process of refinement that may not adequately meet our present and future needs. This is particularly so where liability is sought to be recognised based on conduct of the defendant in acquiring the information as the primary basis of liability, rather than through the traditional relational context.

In approaching the question of a new criminal law presence in this area, I would suggest that it is of the utmost importance that fragmentary and context-specific strategies be abandoned in favour of the development of generalised principles.[45] What is needed is a principled and comprehensive model of protection that offers complementary civil and criminal liability in respect of confidential commercial information. By not adopting a more principled approach both at civil and criminal law, we risk over-regulation and inconsistent application of present models of liability.

For example, whilst there are distinctions now made between government, commercial and personal information within the equitable action of breach of confidence, such a distinction has not been as strongly made in the incidental application of criminal law. The rationale for protecting these various types of information is quite different, as is the proper scope of legal protections. Certainly no reasonable person would suggest that confidential information as it relates to corporations and individuals is the same, yet these distinctions fail to inform the criminal law. If we are to offer protection to confidential commercial information without unduly impinging on other legitimate interests (for example, civil liberties), it would seem prudent to draft new laws to ensure that they are not applied outside the context of their articulated rationale. In this sense, we ought recognise that liability rules in respect of confidential information have the ability to act as methods of private censorship, as was attempted in the *Scientology* cases in the United States.[46] Beyond this, it seems odd to limit protection of that which is considered properly protectable, to acts of use or disclosure but not acquisition. Surely it is the nature of the misappropriative act itself that is culpable, whilst the nature of the information merely demarcates the appropriate breadth of the proscription.

2. Defining an Appropriate Role for Criminal Sanctions

The Law Commission has taken the provisional position that criminal law in this area should be narrowly applied and ought to follow civil liability.[47] As civil liability is essentially receipt-based liability in this area, the implicit position is that the criminal law ought to refrain from introducing

new standards of conduct-based liability. This is to say that the criminal law should restrict itself to breach of confidence situations where the threat of civil liability in the circumstances is insufficient to promote compliance with express or implicit obligations of confidentiality. This approach is reflective of the traditional reluctance in English law to construct models of direct liability for unfair competition.

I have suggested that the law should offer comprehensive protection for confidential commercial information. I would further suggest that the criminal law in this area may fulfil three functions: to set minimum standards of acceptable commercial behaviour, to deter the breach of private obligations of confidence in appropriate circumstances as envisaged by the Law Commission, and to bring domestic treatment in line with emerging international standards respecting the protection of intellectual property through more liberalised unfair competition norms. This is relevant in the cyberspace context as we are presently engaged in setting out the principles that will govern the conduct of commerce in cyberspace (like the standard and method of encryption necessary to allow commercial transactions to be conducted on the Internet). We ought to confront the need to set appropriate standards of commercial behaviour in relation to confidential commercial information in this area as one might reasonably expect misappropriation to be accomplished through the use of emerging technologies.

With respect to the first point, the function of the criminal law in the commercial context is, at a minimum, to define the outer limits of tolerable commercial behaviour.[48] In this sense, the criminal law plays a role that civil remedies cannot: it serves a declaratory and educational function in supporting appropriate standards of commercial behaviour. The difficulty, of course, lies in applying criminal sanctions where civil liability is uncertain,[49] and where it is unclear as to whether the conduct in question is truly worthy of blame.[50] However, it is clear that one legitimate function for new criminal laws in this area is to set a threshold standard for commercial behaviour, below which criminal liability may be incurred.

Secondly, the criminal law is able to provide general deterrence against wrongful acts where civil liability is inadequate; for example, where the defendant is judgement-proof or the plaintiff is without the resources or sophistication to bring an action (or even has been driven into bankruptcy as a result of the acts in question). In such circumstances, the proscribed act still attracts liability and consequences. This is useful in enforcing commercial morality in the sense of deterring certain wilful breaches of obligations of confidence in cyberspace or elsewhere.

Thirdly, national criminal laws can also act internationally in the sense of working towards harmonisation of national laws, and creating a global response to such trans-national problems as money laundering. It may be that such an approach is the best way of protecting intellectual property across borders, and perhaps the solution to the trans-national problem of industrial espionage.[51] I would suggest that on a criminal law level, it would seem reasonable to proceed in part on the basis of enacting legislation aimed at eradicating "dishonest commercial practices" in relation to the misappropriation of valuable commercial information where the nature of the conduct is sufficiently offensive. Such an approach allows one to confront competitors who obtain confidential information illicitly through conventional methods (such as suborning employees) and through the use of technological means to surreptitiously acquire their rival's secrets. I would suggest that such a standard would dovetail nicely with the standards agreed upon in the TRIPs Agreement, itself building on the incorporated provisions of the Paris Convention for the Protection of Industrial Property, Art. 10*bis*,[52] which establishes a regime against unfair competition practices which is now enforceable under TRIPs through the World Trade Organisation.

3. The Need for More and Better Data Respecting Misappropriative Acts

Criminal laws must be sufficiently precise to enable people to know whether they risk criminal liability for a contemplated course of conduct, and avoid inefficient enforcement of the criminal law

through flawed prosecutions. Lawmakers considering the problem of misappropriation are faced with creating new laws without a detailed and independent review of the nature of the problem. Whilst one might be able to develop the main principles of a protective model that speaks to the relevant public policy interests in a more global sense, there is a serious lack of sufficiently reliable data to determine those acts themselves which ought be proscribed in any new law. I would suggest two points in this regard.

First, the present lack of comprehensive civil and criminal sanctions necessarily affects the reporting of misappropriative activity as existing legal remedies do not cover the acts subject of a potential complaint. Moreover, even where there are remedies available at law, trade secret cases traditionally suffer from a reluctance on the part of victims to extend losses and suffer crises of investor confidence by engaging the legal process for redress of their complaints.[53] That there are few complaints should not be taken to mean that misappropriative activity does not occur.

Secondly, such evidence as does exist in the forms of statistics or studies that document the problem of misappropriation tend to grow out of proprietary surveys conducted by industry groups, like the American Society for Industrial Security.[54] The problem in relying on these types of studies is that they are geared towards producing lists of industry losses rather than detailing types of conduct. The loss figures themselves are not actual losses, but estimates and projections based on subjective criteria.[55] Such projected losses may make interesting journalism,[56] but law-makers ought to be wary of legislating based on the expectation of the looming economic disaster these estimates tend to engender. However, even when viewed critically, these figures do point at a serious problem that threatens to become larger if it remains unchecked.

Sadly, there are few academic studies. The most recent is by Professor Burr who looked at misappropriation of trade secrets in the American state of New Mexico and found that misappropriation of trade secrets mainly involved confidants (employees, government inspectors, etc.) but also extended to third party theft. Whilst this study was limited in scope and volume of data, it is one of the very few sources of publicly available and independent data in this area. The sample was taken from a pool of small to medium sized corporations and did not sample large or trans-national corporations, whose orientation seems to be traditional industrial manufacturing rather than economic activities tied to newer technologies and informational products. The study also seems to be directed at the question of civil redress rather than willingness to pursue criminal complaints.[57]

The risk that is run is that in enacting laws that seek to remedy the mischief of misappropriation without a very clear idea of which acts ought be proscribed, one runs the risk of over-regulation. In the context of a global communications environment, such as the Internet, this is not just a matter of national concern. It is clear that in some cases, local regulation of cyberspace can have international implications. Such was the case in the claim by German prosecutors against CompuServe, resulting in the blocking of certain newsgroups to its world-wide subscribers.[58] In this sense, it is important to get the national balance right.

I suggest that governments would be well advised to take the lead in commissioning further research on this point if laws are to achieve their potential in addressing real-world needs. What is required is both an accurate estimate of the nature and scope of misappropriative activities, and, procedural reform to encourage complainants to come forward to engage the legal process whilst maintaining the security of their informational assets during the course of litigation (civil and criminal).

4. Incorporating Technological Solutions into Legal Models

American law has traditionally required protective measures in trade secrets law. Indeed, the public policy encouraging self-help has found its way from trade secrets law into the latest federal copyright statute which proscribes the circumvention of technological protection measures like encryption or copy protection.[59] The present model of civil liability in English law for breach of

confidence does not require that an information owner take reasonable steps to protect his or her information (though such efforts may be relevant in recognising the information in question as that having "the necessary quality of confidence"[60]),[61] a position that the Law Commission provisionally advocates for the criminal law.[62] The popular objection against such a requirement is the analogy to the homeowner who suffers a burglary - ought we make criminal liability of the burglar contingent on the doors and windows of the house being locked?

With respect, it is my submission that this position is quite wrong.

First, intangible information is not the same as household electronics equipment and jewellery. In the area of confidential information, where the subject-matter might itself be no longer protectable by the desire of the owner to place it in the public domain, it would appear that such a requirement is useful in limiting the scope of any legal protection to that which is in fact relatively secret and of commercial value.

Secondly, there is a public interest in encouraging the prudent use of technology in handling informational assets. Those who use information technology to deal with their sensitive information ought to be encouraged to act wisely.

Thirdly, and perhaps most importantly, by not making the law more clearly predictable information owners are placed in a position where they must go beyond taking *reasonable* protective measures and must take maximum protective measures consistent with their perceptions of the value of the information in question. Rational actors will take protective measures on a cost-benefit basis, but the efficiency of such measures in economic terms is not addressed by the state of the law and seemingly a policy of encouraging economic inefficiency is adopted.[63] Is it really better to require traders with valuable information to operate by the law of the jungle rather than merely act as reasonably prudent business people?

I would suggest that the adoption of such a requirement very much reflects the reality of cyberspace. Technologies like software-based encryption of information are useful in both attracting legal protection to certain types of information as well as assisting information owners in the efficient exploitation of the Internet to handle information.

Conclusion

Abraham Lincoln famously remarked upon the utility of the patent concept in words that apply with equal force to all protected forms of intellectual property. He described the benefit of legal protection as promoting innovation by adding "the fuel of interest to the fire of genius."[64] The law has different reasons for protecting differing varieties of such property, each having its proper limits and each seeking to further the innovative process by balancing private and public interests in knowledge-based assets. In our own time, as intellectual property rights are of critical economic importance, there is a greater willingness to employ the blunt instrument of the criminal law to safeguard such rights. It is my suggestion that in the area of confidential commercial information, there is a need to revise present models and offer comprehensive and complementary protection through both receipt-based and conduct-based standards of liability. The complicating feature is the effect such remedies and proscriptions may have on individual and commercial exploitation of information technologies. I would counsel caution in drafting new laws and encourage more extensive study of the mischief to be remedied, especially the creation of suitably independent data on the nature of misappropriative activity, and encourage law-makers to look beyond national borders to the international context and implications of regulation.

Notes

[*] My thanks to Dr Ian Walden, Queen Mary & Westfield College, London for his comments on a previous draft of this paper.

[1] Law Commission for England and Wales, *Legislating the Criminal Code: Misuse of Trade Secrets* (CP 150, 1997), hereinafter *Consultation Paper on Misuse of Trade Secrets*.

[2] I am using the phrase *confidential commercial information* in this paper in a generic sense, purposely avoiding other descriptions which often have specialised or inconsistent meanings both within English law and in other legal systems - for example, "know-how"; compare *Income and Corporations Tax Act 1988*, s.533(7), *EC Technology Transfer Regulation*, Art. 10(1), and *Poly Linn Ltd v. Finch* [1995] FSR 751. An alternative description might be that used in the *Agreement on Trade-Related Aspects of Intellectual Property Rights*, Art. 39, *undisclosed information*; with respect to this formulation, see R Krasser, "The Protection of Trade Secrets in the TRIPs Agreement" in F-K Beier and G Schricker (Eds), *From GATT to TRIPs - The Agreement on Trade-Related Aspects of Intellectual Property Rights (IIC Studies in Industrial and Copyright Law, Vol. 18)* (Munich: Max Planck Institute, 1996); F Dessemontet, "Protection of Trade Secrets and Confidential Information" in CA Correa and AA Yusuf, *Intellectual Property and International Trade: The TRIPs Agreement* (Kluwer Law International, 1998), 237 and authorities cited therein at fn. 2.

[3] *Consultation Paper on Misuse of Trade Secrets*, para. 3.1; F Gurry, *Breach of Confidence* (Oxford: Clarendon Press, 1984), 7-8; J Hull, *Commercial Secrecy: Law and Practice* (London: Sweet & Maxwell, 1998), 3-4; R Dean, *Law of Trade Secrets* (North Ryde, NSW: LBC, 1990), 8-10; J Pooley, *Trade Secrets* (NY: Law Journal Seminars Press, 1997), §1.03[3]; MF Jager, *Trade Secrets Law* (West Group), §1.04.

[4] C Arup, *Innovation, Policy and Law* (Cambridge: Cambridge University Press, 1993), 123.

[5] See RB Davies and G Saltmarsh, "An International Overview of the Incidence of Economic Crime" in J Reuvid (Ed.), *The Regulation and Prevention of Economic Crime Internationally* (London: Kogan Page, 1995), 91-112.

[6] See generally on the problem of definition: JA Thorburn, "Defining Confidential Business Information" (1996), 9 SPG Intl L Practicum 5, 6-8; KG Fairbairn and JA Thorburn, *Law of Confidential Business Information* (Aurora: Canada Law Book, 1998), ch. 3.

[7] Primarily by denying information a true proprietary characterisation; see below.

[8] *Faccenda Chicken Ltd. v. Fowler* [1986] 1 All ER 617, 627; BS DuVal, "The Occasions of Secrecy" (1986), 47 U Pitt LR 579, 588.

[9] Arup, 126.

[10] See W Landes, R Posner & D Friedman, "Some Economics of Trade Secret Law" (1991), 5 J Econ Persp 61.

[11] "Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy" (1992), 106 Harv LR 461.

[12] Arup, 125-130.

[13] *Lac Minerals Ltd. v. International Corona Resources Ltd.* (1989), 61 DLR (4th) 14, 47 (SCC) per LaForest J.

[14] Institute of Law Research and Reform and a Federal Provincial Working Party, *Trade Secrets*

(Report No. 46, 1986), para. 2.10-2.12.

[15] B Atkins, "Trading Secrets in the Information Age: Can Trade Secret Law Survive the Internet?" (1996), 4 Ill LR 1151, 1152-1154; VA Cundiff, "Trade Secrets and the Internet: A Practical Perspective" (1997), 14 Comp L 6, 7.

[16] These latter situations are more appropriately addressed in a political forum between governments and can be excluded from this discussion. See DE Denning, *Information Warfare and Security* (NY: ACM Press, 1999); E Fraumann, "Economic Espionage: Security Missions Redefined" (1997), 57 Pub Admin R 303; G Mossinghoff, JD Mason and D Oblon, "The Economic Espionage Act: A New Federal Regime of Trade Secret Protection" [1997] JPTOS 191, 192-193; S Porteous, "Economic/Commercial Interests and Intelligence Services - Commentary No. 59" (Ottawa: CSIS, 1995); "Economic Security" (Ottawa: CSIS, 1996). For an economic treatment of these issues, see M Whitney and J Gaisford, "Economic Espionage as Strategic Trade Policy" (1996), Can J Econ (Special Issue) 627.

[17] AS Weinrib, "Information and Property" (1988), 36 UTLJ 117, 133 . For example, *Murray v. Yorkshire Fund Managers Ltd* [1998] 1 WLR 951; *Boardman v. Phipps* [1967] 2 AC 46, 107.

[18] JE Penner, *The Idea of Property in Law* (Oxford: Clarendon Press, 1997), 119.

[19] The matter was left open by the House of Lords in the *Spycatcher* litigation; *Attorney General v. Guardian Newspapers Ltd. (No. 2)*[1990] 1 AC 109, 281 per Lord Goff.

[20] *Oxford v. Moss* (1978), 68 Cr App R 183; *Absolom* (The Times, 14 September 1983); *Jeffreys v. Boosey* (1854), 4 HLC 814; *Nicrotherm Electrical Co. Ltd. v. Percy* [1957] RPC 207; *Stewart* [1988] 50 DLR (4th) 1 (SCC).

[21] For a general review of the law on this point, see D Fisch Nigri, "Theft of Information and the Concept of Property in the Information Age" in JW Harris (Ed.), *Property Problems, From Genes to Pensions* (London: Kluwer Law International, 1997); R Dean, *The Law of Trade Secrets* (Sydney: The Law Book Co., 1990), 53-83; S Ricketson, " Confidential Information – A New Proprietary Interest" (1977), 11 MULR 223-245 (Part I) and 289-315 (Part II); AS Weinrib, "Information and Property" (1988), 36 UTLJ 117; JE Stuckey, "The Equitable Action for Breach of Confidence: Is Information Ever Property?" (1981), 9 Syd LR 402; SJ Soltysinski, "Are Trade Secrets Property?" (1986), 3 IIC 331.

[22] *Oxford v. Moss* (1979), 68 Cr App R 183; *Stewart* [1988] 50 DLR (4th) 1 (SCC); RG Hammond, "Theft of Information" (1984), 100 LQR 252.

[23] For a general review of the American position, see RT Nimmer and PA Krauthaus, "Information as a Commodity: New Imperatives of Commercial Law" (1992), 55 L & Contemp Pr 103; A Beckerman-Rodau, "Are Ideas Within the Traditional Definition of Property: A Jurisprudential Analysis" (1994), 47 Arkansas LR 603.

[24] *Ruckelhaus v. Monsanto Co.*, 467 US 986 (1984). See R Milgrim, *Trade Secrets* (New York: Matthew Bender), §1.7 for the authoritative American position respecting the incorporation of both proprietary and tort approaches to the protection of trade secrets. Also, Jager, §4-15; E Kitch, "The Law and Economics of Rights in Valuable Information" (1980), 13 JLS 683; M Deutch, "The Property Concept of Trade Secrets in Anglo-American Law: An Ongoing Debate" (1997), 31 U Rich LR 313.

[25] *Carpenter v. United States*, 484 US 19 (1984); *United States v. Seidlitz*, 589 F2d 152 (4th Circ., 1978).

[26] Gurry, 58-61; G Jones, "Restitution of Benefits Obtained in Breach of Another's Confidence" (1970), 86 L.Q.R. 463, 464; *Cadbury Schweppes Inc. v. FBI Foods Inc.* [1999] SCJ 6; *Lac Minerals Ltd. v. International Corona Resources Ltd.* (1989), 61 DLR (4th) 14, 47 (SCC); *Aquaculture Corp. v. New Zealand Green Mussel Co. Ltd.* (1985), 5 IPR 353 (NZCA); *Moorgate Tobacco Co. Ltd. v. Philip Morris (No.2)* (1984), 156 CLR 414 (Aust HC).

[27] *Kitechnology B.V. v. Unicor Gmbh* [1995] FSR 765; RP Meagher, WMC Gummow & JRF Lehane, *Equity Doctrines and Remedies* 3rd Ed. (Sydney: Butterworths,1992), para. 4103.

[28] Lord Goff and G Jones, *The Law of Restitution* 4th Ed. (London: Sweet & Maxwell, 1993), ch. 35-36; P Birks, *An Introduction to the Law of Restitution* (Oxford: Clarendon Press, 1989), 343-346; D Friedmann, "Restitution for Wrongs: The Basis of Liability" in WR Cornish, R Nolan, J O'Sullivan, and G Virgo (Eds), *Restitution: Past, Present and Future* (Oxford: Hart Publishing, 1998), 150.

[29] *Attorney General v. Guardian Newspapers Ltd. (No. 2)*[1990] 1 AC 109; *Seager v. Copydex* [1967] 1 WLR 923; *House of Spring Gardens v. Point Blank* [1984] IR 611.

[30] *Report of the Commission on Privacy* (1972, Cmnd. 5012), para. 489.

[31] See JT Cross, "Protecting Confidential Information Under The Criminal Law of Theft and Fraud" (1991), 11 OJLS 264.

[32] *Consultation Paper on Misuse of Trade Secret*s , para. 1.24.

[33] V Tunkel, "Industrial Espionage: What Can the Law Do?" [1995] Denning LJ 99, 103.

[34] English law knows no tort of unfair competition; *Bulmer Ltd. v. Bollinger SA* [1977] 2 CMLR 625; *Moorgate Tobacco v. Philip Morris Ltd.* [1985] RPC 219 (Aust HC); *Erven Warnink BV v. J. Townend & Sons (Hull) Ltd.* [1980] RPC 31; *Hodgkinson & Corby Ltd and Roho Inc v. Wards Mobility Services LtdMogul Steamship Co. v. McGregor & Co* (1889), 23 QBD 598; A Kamperman Sanders, *Unfair Competition Law* (Oxford: Clarendon Press, 1997), 52-54. Interestingly, modern American law in this area is built on the acceptance of unfair competition norms and has been so recognised since the first *Restatement of Torts* (1939), §757. For a review of early American common law on the point, see JL Hopkins, *The Law of Unfair Trade, including Trade-Marks, Trade Secrets and Good-Will* (Chicago: Callaghan & Co., 1900), 153-165; International News Service v. Associated Press, 248 U.S. 215 (1918).

[35] *Francome v. Mirror Group Newspapers Ltd.*, [1984] 1 WLR 892; *ITC Film Distributors v. Video Exchange* [1982] Ch. 431; *Distillers Co (Biochemicals) Ltd. v. Times Newspapers Ltd* [1975] QB 613, 621; G. Wei, "Surreptitious Takings Of Confidential Information" (1992), 12 LS 302.

[36] *Lord Ashburton v. Pape* [1913] 2 Ch. 469; *Argyll v. Argyll* [1965] 1 All ER 611, 627; *Butler v. Board of Trade* [1971] Ch. 680; *Commonwealth v. John Fairfax & Sons* (1980), 147 CLR 39, 50 (Aust. HC); *Webster v. James Chapman & Co.* [1989] 3 All ER 939; RP Meagher, WMC Gummow & JRF Lehane, *Equity Doctrines and Remedies* 3rd Ed.(Sydney: Butterworths,1992), para. 4109; M Richardson, "Breach of Confidence, Surreptitiously or Accidentally Obtained Information and Privacy: Theory Versus Law" (1994), 19 MULR 673; M Richardson and J Stuckey-Clarke, "Breach of Confidence" in P Parkinson (Ed.), *Principles of Equity* (North Ryde, NSW: LBC Information Services, 1996).

[37] G Jones, "Restitution of Benefits Obtained in Breach of Another's Confidence" (1970), 86 LQR 463.

[38] *Franklin v. Giddens* [1978] Qd R 72; R Wacks, *Privacy and Press Freedom* (London: Blackstone Press, 1995), 61.

[39] *Restatement of Torts* (1939), §757; *Restatement of Unfair Competition (Third)*(1995), §43. See also *Ansell Rubber Co. Pty Ltd v. Allied Rubber Industries Pty Ltd* [1967] VR 37.

[40] *Creation Records Ltd. v. The News Group* [1997] EMLR 444; *Shelley Films Limited v. Rex Features Limited* [1994] EMLR 134; *Linda Chih Ling Koo v. Lam Tai Hing* [1993] 2 HKC 1. See R Wacks, *Privacy and Press Freedom* (London: Blackstone Press, 1995), 63.

[41] WR Cornish, "Protection of Confidential Information in English Law" (1975), 6 IIC 43, 50, 53.

[42] See *Moorgate Tobacco Co. Ltd. v. Philip Morris (No.2)* (1984), 156 CLR 414 (Aust HC), where the claim was raised in relation to breach of confidence as well as being advanced on the purported tort of unfair competition.

[43] See E Kitch, "The Expansion of Trade Secrecy Protection and the Mobility of Management Employees: A New Problem for the Law" (1996), 47 So Car LR 659.

[44] R Whitaker, *The End of Privacy* (NY: WW Norton, 1999), 55.

[45] See generally H Cornwall, *Data Theft: Computer Fraud, Industrial Espionage and Information Crime* (London: Heinemann, 1987).

[46] *RTC and Bridge Publications Inc. v. FACT NET Inc., Wollersheim and Penny*, 901 F Supp 1519 (D Colo, 1995) and 901 F Supp 1528 (D Colo, 1995); *RTC v. Lerma*, 908 F Supp 1353 (ED Va, 1995). See N Hanlon-Leh, "Lessons from Cyberspace & Outerspace: the Scientology Cases" (1998), 27 Sum Brief 48.

[47] *Consultation Paper on Misuse of Trade Secrets*, para. 3.28. This is essentially an *ultima ratio* policy similar to the position recommended by the Council of Europe in relation to interference with protected personal data; see Recommendation R(89)9 (13 September 1989) and the position advocated to the Council by the Select Committee of Experts on Computer-Related Crime of the Committee on Crime Problems. In general terms, the Law Commission's provisional model is a narrow one which builds upon its recommendations respecting the equitable action of breach of confidence made in 1981; see *Report on Breach of Confidence* (Law Com. No. 110) in which it was recommended that a statutory tort be enacted to replace the current common law and equitable regime. The Law Commission recognises that whilst the government of the day accepted its recommendations in 1989, there was no political will to legislate in the area; *Consultation Paper on Misuse of Trade Secrets*, para. 2.13.

[48] GE Lynch, "The Role of the Criminal Law in Policing Corporate Misconduct" (1997), 60 L & Contemp Pr 23, 64.

[49] C Steele and A Trenton, "Trade Secrets: The Need for Criminal Liability" [1998] EIPR 188, 192.

[50] RG Bone, "A New Look at Trade Secrets Law: Doctrine in Search of Justification" (1998), 86 Calif LR 241, 296.

[51] See LL Hicks and JR Holbein, "Convergence of National Intellectual Property Norms in International Trading Arrangements" (1997), 12 Am UJ Intl L & Pol 769; J.H. Reichman, "Beyond the Historical Lines of Demarcation: Competition Law, Intellectual Property Rights, and International Trade after GATT's Uruguay Round" (1993), 20 Brooklyn J Intl L 75,76.

[52] *Paris Convention for the Protection of Industrial Property* (Stockholm Act of 14 July 1967 of the Paris Convention for the Protection of Industrial Property), Art 10*bis* provides for member states to have effective protection against unfair competition covering "any act of competition contrary to honest practices in industrial and commercial matters" with specific examples; see GHC Bodenhausen, *Guide to the Paris Convention for the Protection of Industrial Propert*y (Geneva: BIRPA, 1968), 145, who presents a history of the Convention and these provisions from the original 1883 Convention.

[53] Institute of Law Research and Reform and a Federal Provincial Working Party, *Trade Secrets* (Report No. 46, 1986), para. 2.13. Similar views were expressed in the Judiciary Committee, House of Representatives report to the U.S. Congress with the tabling of the bill that became the *Economic Espionage Act of 1996*; Report No. 104-788, 104th Congress (2d Session); also the Senate Report, No. 104-359. Similarly, the *Annual Report to Congress on Foreign Collection and Industrial Espionage* by the President under the *Intelligence Authorization Act for Fiscal Year 1995*, s.809(b).

[54] ASIS conducts research on industrial property losses; see the 1998 Report, covering 1996-1997, by R Heffernan and D Swartwood (Arlington, Va.: ASIS, 1996). A similar survey is the 1996 Information Systems Security Survey in SM Shaker and MP Gembicki, *The WarRoom Guide to Competitive Intelligence* (NY: McGraw Hill, 1999), 223-228.

[55] Porteous, 4. Perry puts the costs to the American economy as a result of economic espionage at between $50-240 billion annually; S Perry, "Economic Espionage and Corporate Responsibility" (1995), 11 Crim J Intl. 3.

[56] For example, J Fialka, *War by Other Means: Economic Espionage in Americ*a (NY: WW Norton & Co, 1997) and "Stealing the Spark: Why Economic Espionage Works in America" (1996), 19 Wash Q 175; I Winkler, *Corporate Espionage* (Prima Publishing, 1997); B Parad, *Commercial Espionage: 79 Ways Competitors Can Get Any Business Secret* (Skokie, Ill.: Global Connection, 1997), are just a few of the books recently published.

[57] See SL Burr, "Protecting Business Secrets in National and International Commerce" (1996), 17 Science Communication 274. See also LF Mock and D Rosenbaum, "A Study of Trade Secrets Theft in High Technology Industries" (Washington, DC: US National Institute of Justice, 1988).

[58] See IC Ballon, "The Law of the Internet: Developing a Framework for Making New Law (II) (1997), 10 Cyber L 16; SM Hanley, "International Internet Regulation: A Multinational Approach" (1998), J Marshall J Comp & Info L 997.

[59] *Digital Millennium Copyright Act*, 17 USC §1201(a)(1) (1998). The legislation was enacted to incorporate the WIPO copyright treaties into American law, and includes a number of provisions aimed at the distribution and broadcast of copyright-protected items on the Internet.

[60] *Saltman Engineering Co Ltd v. Campbell Engineering Co Ltd* [1948] RPC 203, 215.

[61] *Faccenda Chicken v. Fowler* [1987] Ch 117, 137-138.

[62] *Consultation Paper on Misuse of Trade Secrets*, para. 4.22.

[63] "Trade Secret Misappropriation: A Cost-Benefit Response to the Fourth Amendment Analogy" (1992), 106 Harv LR 461.

[64] Lecture on Discoveries and Inventions, in RP Basler, MD Pratt and LA Dunlap, *The Collected Works of Abraham Lincoln* (New Brunswick : Rutgers University Press, 1953, supplemented).