# PART I
# INTRODUCTION

### THE BACKGROUND TO THIS CONSULTATION PAPER

1.1 This consultation paper is concerned with the issue of whether there should be criminal liability for the deliberate misuse of the trade secrets of another. As we shall show,[1] the misuse of trade secrets cannot found a charge of theft. There has been much criticism of this. For example, a distinguished parliamentarian[2] complained that "It is not too much to say that we live in a country where … the theft of the board room table is punished far more severely than the theft of the board room secrets".[3] Professor Glanville Williams wrote:

> It is absurd and disgraceful that we should still be making do without any legislation specifically designed to discourage this modern form of commercial piracy. Abstracting or divulging an official secret is an offence under the Official Secrets Act 1911, sections 1 and 2; but Leviathan is not much concerned to protect the secret and immensely valuable know-how of its subjects.[4] [RJH1]

1.2 We have also become increasingly conscious that many other jurisdictions, by contrast, extend the protection of the criminal law to the misuse of confidential business information.[5] It is noteworthy, in particular, that the majority of the American states and a number of European countries, including France and Germany, provide criminal sanctions against the abuse of trade secrets; and a number of people advocate similar legislation in this country.

1.3 In our working paper on conspiracy to defraud,[6] we considered whether to propose any new offence of taking confidential information by dishonest means, or an extension of any existing offence or offences in that area. We concluded, however, that the working paper was not the appropriate place to conduct a review of the need for such a sanction.[7] On consultation, substantial support was expressed for the application of a criminal sanction to at least some forms of misuse of information.[8] Those in favour of such a sanction were able to point to the illogical

[1] See paras 1.4 – 1.7 below.

[2] The Rt Hon Sir Edward Boyle MP (later Lord Boyle).

[3] *Hansard* (HC) 13 December 1968, vol 775, col 806.

[4] *Textbook of Criminal Law* (2nd ed 1983) p 739.

[5] See Appendix B.

[6] Criminal Law: Conspiracy to Defraud (1987) Working Paper No 104.

[7] *Ibid*, paras 10.44 – 10.48.

[8] Those in favour of introducing liability included the Inland Revenue; the Serious Fraud Office; the Crown Prosecution Service; British Telecom; the Department of Trade and Industry Insolvency Service; the Confederation of British Industry; and Judge Rant QC.

criteria for determining criminal liability under the present law.[9] The Solicitor-General has welcomed the work on this project.[10]

## THE PRESENT LAW

### Theft

1.4 At present the criminal law gives no specific protection to trade secrets. In particular, trade secrets cannot, in law, be stolen: they do not constitute "property" for the purpose of the Theft Act 1968,[11] section 1 of which defines the offence of theft as the dishonest appropriation of property belonging to another with the intention of permanently depriving the other of it. In the leading case, *Oxford v Moss*,[12] an undergraduate obtained the proof of an examination paper before the examination. After reading the proof he returned it, retaining the information for his own use. He was held not guilty of stealing the information.

1.5 The principle is strikingly illustrated by *Absolom*,[13] which followed *Oxford v Moss*. The defendant, a geologist, obtained and then tried to sell to a rival company details of a leading oil company's exploration for oil off the Irish coast. The information, which was contained in a "graphalog" (a record of geological data and an indication of the prospects of finding oil), was unique, since the company was the only oil company exploring the area. The company had invested £13 million in drilling operations, and the information could have been sold for between £50,000 and £100,000. Although the judge stated that the defendant had acted in "utmost bad faith", he directed the jury to acquit him of theft, on the ground that the information in the graphalog was not capable of founding such a charge.

1.6 A further difficulty with applying the law of theft to the misappropriation of a trade secret arises from the requirement that the defendant must intend permanently to

[9] For example, if a trade secret is on a sheet of paper, a wrongdoer who removes it may be liable for theft of the paper; but a person who merely memorises the secret, and subsequently misuses it, incurs no criminal liability.

[10] The Solicitor-General, The Lord Falconer of Thoroton QC, said recently:

> The modern sorts of commercial activity, and the modern methods by which dishonest activity may be effected make one constantly worried that the unoverhauled bus may not be able to cope. Simply by way of example, one asks how is the law going to cope with the increasing prevalence of commercial espionage both by computer and otherwise where the commercial rival or predator obtains information which he then covertly uses to benefit himself in his dealings with the victim, for example by photocopying documents without authority, or by entering the victim's computer systems. No doubt the law will be able to concoct some niche in the criminal calendar. But it depends on the ingenuity of the prosecutor, the learning and advocacy of the defence, and the judge on the day. I welcome the fact that the Law Commission is due to publish a consultation paper next month looking at the operation of trade secrets.

"Commercial Fraud or Sharp Practice – Challenge for the Law", Denning Lecture, 14 October 1997.

[11] Notwithstanding that the Act defines property as including "money and all other property, real or personal, including things in action and other intangible property": s 4(1). By contrast, a patent or an application for a patent is personal property (Patents Act 1977, s 30(1)) and so capable of being stolen.

[12] (1979) 68 Cr App R 183.

[13] *The Times*, 14 September 1983.

deprive the owner of the property. "It is difficult to see how there is any question of deprivation where someone has, in breach of confidence, forced the original holder to share, but not forget, his secret."[14]

1.7 Normally the information amounting to a trade secret will be recorded on a physical medium such as paper, microfiche or a computer disk. In that case, the physical medium is property, and a dishonest taking of it can therefore be charged as theft. But a charge of stealing an object worth a few pence would scarcely represent the gravamen of the defendant's conduct. And even this charge is unavailable if the information is absorbed without the taking of the medium on which it is recorded, or if (as in *Oxford v Moss*) there is no intention permanently to deprive the secret's owner of the *medium* (as distinct from the secret).

1.8 There are, however, a number of existing offences of infringing rights in intellectual property; and there are other offences which are not primarily concerned with intellectual property but which might be committed in the course of acquiring, using or disclosing another's trade secret.

## Intellectual property offences

### *Copyright and performers' rights*

1.9 The Copyright, Designs and Patents Act 1988 contains two main offence-creating provisions which target the infringement of copyright[15] and the production or use of illicit recordings.[16]

1.10 Section 107 creates the offence of making for sale or hire, or importing otherwise than for private and domestic use, any article which is an "infringing copy"[17] without the licence of the copyright holder.[18] It is also unlawful for any person in the course of a business and without the copyright holder's permission, to possess an infringing copy with a view to committing an act which breaches the copyright; or in the course of business (a) sell or let for hire; (b) offer or expose for sale or hire; (c) exhibit in public; or (d) distribute an infringing copy.[19] The distribution of infringing copies other than in the course of business, but to such an extent as to affect prejudicially the copyright holder, is also criminalised.[20] The prosecution must prove that the accused knew or had reason to believe that the article was an infringing copy.

1.11 Section 198 aims to protect performers' rights by targeting "illicit recordings" – defined as the recording (in whole or of a substantial part) of a performance, if

[14] N E Palmer and Paul Kohler, "Information as Property", in Norman Palmer and Ewan McKendrick (eds) *Interests in Goods* (1993) p 203.

[15] Copyright, Designs and Patents Act 1988, s 107.

[16] 1988 Act, s 198.

[17] Section 27(2) of the 1988 Act provides that an article "is an infringing copy if its making constituted an infringement of the copyright in the work in question".

[18] 1988 Act, s 107(1)(a), (b).

[19] 1988 Act, s 107(1)(c), (d).

[20] 1988 Act, s 107(1)(e).

made for other than private purposes and without the performer's consent.[21] A person is guilty of an offence if without the requisite consent, he or she makes an illicit recording for sale or hire,[22] or imports such a recording otherwise than for private and domestic use,[23] or possesses such a recording with a view to infringing the performer's rights.[24] It is also an offence if a person, in the course of business (a) sells or lets for hire; (b) offers or exposes for sale or hire; or (c) distributes an illicit recording.[25] In keeping with section 107, it must be shown that the accused knows or has reason to believe that the recording is illicit.

1.12 Both offences are supplemented by ancillary enforcement powers. The Act empowers the court to order delivery up of an impugned copy or recording[26] and permits magistrates to issue search warrants on specified grounds.[27]

***Registered trade marks***

1.13 Section 92 of the Trade Marks Act 1994 creates a number of offences of counterfeiting registered trade marks.[28] It is a crime (1) to apply to goods or their packaging a sign identical, or likely to be mistaken for, a registered trade mark; (2) to sell, let for hire (or expose for sale or hire) or to distribute goods which bear such a sign; or (3) to possess any such goods with a view to selling them, or letting them for sale or hire etc.[29] It is also an offence for a person to apply a sign identical to, or likely to be mistaken for a registered trade mark, to certain other materials, for example materials intended to be used for advertising. Using such materials in the course of a business, or possessing them with a view to doing so, is likewise criminalised.[30]

1.14 Finally, section 92 makes it unlawful for a person to make an article for the purpose of making copies of registered trade marks or signs likely to be mistaken for them, or to have such an article in his or her possession.[31] All the section 92 offences require the accused to act with a view to gain or with an intent to cause loss to another. He or she must also be acting without the consent of the proprietor of the registered trade mark. It is a defence for the accused to show that he or she believed, on reasonable grounds, that the use or intended use of the sign

[21] 1988 Act, s 197(2). See also s 197(3) which extends protection to those who have *recording rights* in the performance, eg record companies.

[22] 1988 Act, s 198(1)(a).

[23] 1988 Act, s 198(1)(b).

[24] 1988 Act, s 198(1)(c). Or with a view to infringing the rights of those with recording rights: see n 20 above.

[25] 1988 Act, s 198(1)(d).

[26] 1988 Act, ss 108, 199.

[27] 1988 Act, ss 109, 200.

[28] A trade mark is defined as "any sign capable of being represented graphically which is capable of distinguishing goods or services of one undertaking from those of other undertakings": Trade Marks Act 1994, s 1(1). Registration gives the owner of the trade mark a property right in it which is subject to the protection of the 1994 Act: *ibid*, s 2(1).

[29] 1994 Act, s 92(1).

[30] 1994 Act, s 92(2).

[31] 1994 Act, s 92(3).

was not an infringement of the trade mark.[32] It is also an offence to falsify the register, or falsely represent that a trademark is registered.[33]

### *Other intellectual property*

1.15 The offences in the other intellectual property statutes adopt a different approach. The protection of patents and registered designs, like that of trade marks, results from registration or official grant; but the offences under the legislation target only dishonest interference with such procedures, not infringement in itself.[34] We consider in Part III below a possible justification for this distinction between copyright and registered trade marks on the one hand, and patents and registered designs on the other, and its implications for trade secrets.[35]

### The Computer Misuse Act 1990

1.16 Where the information in question is held on computer, it may be protected by the Computer Misuse Act 1990. Section 1 creates the summary offence of gaining unauthorised access to data held on a computer. Section 2 provides a further and more serious offence[36] of committing the section 1 offence with intent to commit or facilitate an arrestable offence.[37]

1.17 The access sought by the defendant must be unauthorised, and he or she must know this at the time of causing the computer to function. This requirement limits the protection afforded by the Act. In the recent case of *DPP v Bignall*[38] police officers had extracted information from the Police National Computer for private purposes. They were authorised to access the computer, but only for official purposes. The Divisional Court held that persons entitled to access information on a computer are not guilty of an offence under the Act even if they use that information for an unauthorised purpose. Thus the protection conferred by the Act on confidential information is very partial: its primary purpose is to protect the integrity of computer systems, not the information held on them. It extends to industrial espionage by outsiders, but not to breach of confidence. Breach of confidence may, however, be covered by the Data Protection Act.

### The Data Protection Act 1984

1.18 The Data Protection Act 1984 imposes a registration scheme on those who hold personal data on computer, and contains offences to punish those who breach the Act's safeguards. For example, a person who holds or uses data other than for a

[32] 1994 Act, s 92(5).

[33] 1994 Act, ss 94, 95.

[34] For example, it is an offence to secure false entries on the register: Patents Act 1977, s 109; Registered Designs Act 1949, s 34. See W R Cornish, *Intellectual Property* (3rd ed 1996) para 2-19.

[35] See paras 3.40 – 3.48 below.

[36] Triable either way, and punishable on conviction on indictment with five years' imprisonment.

[37] It is immaterial whether the ulterior offence is to be committed at the time of access or on some future occasion: s 2(3). The definition of "arrestable offence" includes offences punishable with five or more years' imprisonment: Police and Criminal Evidence Act 1984, s 24(1)(b).

[38] (1997) 161 JP 541.

purpose set out in the register entry is guilty of an offence.[39] The disclosure of personal data to persons not described in the register is, subject to certain exceptions, also an offence.[40] To be guilty of these offences the defendant must act knowingly or recklessly.

1.19 As with the Computer Misuse Act, a recent case restricts the protection afforded by the Data Protection Act. In *Brown (Gregory)*[41] a police officer entitled to use the Police National Computer did so for a non-registered[42] purpose. He called the information up on screen but made no later use of it. The House of Lords held by a majority that a person who merely retrieves information in the form of a display on screen or a print-out does not *use* data for the purposes of the offence. The data must be used subsequent to this, and the defendant was not therefore guilty of an offence.

1.20 For present purposes this restriction may be of limited significance, since our main concern is not with the mere *acquisition* of trade secrets (albeit without authority and for improper purposes) but with their disclosure or misuse – either of which might found a charge under the Act. The main disadvantage of the Act as a weapon against trade secret misuse is the fact that most trade secrets are not *personal* data. Thus it might catch the unauthorised use of, for example, a customer list, but not that of a secret formula or process.

**Conspiracy to defraud**

1.21 Where two or more people dishonestly use or disclose another's trade secret, they may be guilty of the common law offence of conspiracy to defraud. The element of fraud is so widely defined that, on such facts, it may be readily established.[43] The main reason why conspiracy to defraud is not a complete solution under the existing law is the requirement of *conspiracy*: it is probably illegal for two people to agree to "steal" a trade secret, but not for one person to do it alone.

1.22 It might be thought that the obvious solution is therefore to turn the offence of conspiracy to defraud into a general offence of fraud, not requiring proof of a conspiracy. In so far as a conspiracy to use or disclose a trade secret is now a conspiracy to defraud, the use or disclosure of a trade secret would itself be criminal. The possibility of extending the offence in this way was considered in our report Criminal Law: Conspiracy to Defraud.[44] We there concluded that it would

[39] Data Protection Act 1984, ss 5(2)(b), 5(5).

[40] *Ibid*, ss 5(2)(d), 5(5).

[41] [1996] 1 AC 543.

[42] The defendant was retrieving the information held in a database in order to assist a friend who ran a debt-collecting agency. He made checks on vehicles thought to be owned by debtors from whom the agency had been asked to collect debts.

[43] Defined in the leading case, *Scott* [1975] AC 819, 840F, *per* Viscount Dilhorne (with whom the other law lords agreed) as "an agreement by two or more by dishonesty to deprive a person of something which is his or to which he is or would be or might be entitled or … an agreement by two or more by dishonesty to injure some proprietary right" of the victim's. There is authority for the view that this definition is not exhaustive, and that an agreement to cause prejudice to another in any way will suffice: eg *Welham* [1961] AC 103, 124, *per* Lord Radcliffe, and p 133, *per* Lord Denning; *Wai Yu-tsang* [1992] 1 AC 269, 277 (PC).

[44] (1994) Law Com No 228.

be premature to recommend either the abolition of conspiracy to defraud or its conversion into a general fraud offence; but we stated our intention to examine the areas where it currently supplements the rest of the criminal law, to consider how the law in those areas might be put on a more rational basis, and finally to return to the question of whether conspiracy to defraud is still needed. Our provisional view is that, if trade secret misuse ought to be made criminal, the right way to do it is by means of a specific offence, not the general law of fraud.

### Obtaining information in particular ways

1.23 Although trade secret misuse is not an offence in itself, the way in which a secret is obtained may incidentally trigger liability for a more general offence. Where secret information is obtained by deception, for example, on the understanding that it has been or will be paid for, there may be an obtaining of services by deception, contrary to section 1 of the Theft Act 1978. Obtaining information by bribery or corruption may be an offence under the Prevention of Corruption Acts 1889 to 1916.[45] Again, industrial espionage may involve the commission of the offence of intercepting post or of telephone tapping.[46] But there is no offence if an employee simply discloses or uses the secret in breach of confidence, or an outsider obtains it in a manner not specifically prohibited.

### The lacuna

1.24 It thus appears that the protection afforded to trade secrets by the existing criminal law is limited. There may be no offence if an individual, acting alone, dishonestly uses or discloses secret information (not protected by copyright or a registered trade mark, and not amounting to personal data protected by the Data Protection Act 1984) without authority, provided that that individual

(1) obtains the information with the consent of its owner (albeit in confidence) – for example where an employee is given the information for the purposes of his or her work – or

(2) though not authorised to have the information at all, obtains it without resorting to deception,[47] corruption, unauthorised access to a computer, intercepting post, telephone tapping or any other prohibited means. A simple example would be the industrial spy who gains access to premises without forcing entry (which would involve an offence of criminal damage) and inspects the contents of an unlocked filing cabinet.

## APPROACH TO THIS PROJECT

1.25 We will start this paper by setting out in Part II some of the previous reform proposals which have not been successful, but which indicate the concern about the present state of criminal law in relation to the misappropriation of trade secrets. In Part III, we deal with the need for reform and provisionally propose that there should be an offence of deliberately misusing a trade secret. Part IV contains

[45] See Legislating the Criminal Code: Corruption (1997) Consultation Paper No 145.

[46] Interception of Communications Act 1985, s 1.

[47] Or does resort to deception, but there is no understanding that the information is to be paid for (as the Theft Act 1978, s 1, requires) – for example, a person obtains access to business premises by pretending to be a prospective client, and reads papers lying on a desk.

our provisional conclusions concerning the definition of a "trade secret". In Part V, we set out the elements of our proposed offence, before dealing with our suggested defences to it in Part VI.

1.26 Industrial espionage is dealt with in Part VII. We then examine, in Part VIII, the relationship between civil claims for trade secret misuse and criminal proceedings for our proposed offence. This involves considering the right of a defendant in civil proceedings to rely on the privilege against self-incrimination for our proposed new offence. We also discuss whether, and how, the courts should stay civil proceedings where criminal proceedings for the same matters (in particular, for our new proposed offence) are expected or pending.

1.27 We are very grateful for the assistance that we have received from our consultant on this project, Professor William Cornish FBA, the Hershell Smith Professor of Intellectual Property at the University of Cambridge. Mr David Ormerod, Lecturer in Law at the University of Nottingham, has also helped us with the section dealing with the need for the new offence, and we are obliged to him.

### PROVISIONAL CONCLUSIONS AND PROPOSALS

1.28 The first point we consider is whether the misuse of trade secrets should be criminalised. We provisionally conclude that the arguments in favour provide a strong case for criminalisation, provided that the necessary offence can be drafted in sufficiently precise terms.[48]

1.29 We consider a provisional definition of the term "trade secret". We think the term should apply to information (i) which is not generally known,[49] (ii) which derives its value from that fact,[50] and (iii) as to which its "owner" has indicated (expressly or impliedly) his or her wish to preserve its quality of secrecy.[51] We ask for views on this. We also seek views on (i) whether there should be an additional requirement that the information be used in a trade or business; and if so, (ii) the extent to which the definition should exclude professional secrets, and (iii) the extent to which the definition should extend to pure research.[52]

1.30 Our provisional view is that our proposed new law should criminalise the *use or disclosure* of another's trade secret where the "owner" does not consent to its use or disclosure.[53] We propose that consent should be negatived if obtained by deception, as defined by section 15(4) of the Theft Act 1968.[54] The mental element of the proposed offence requires the prosecution to prove that the defendant knew the information was a trade secret. However, we do not propose that the prosecution should have to prove any ulterior intent.[55] We are very

[48] Para 3.61 below.

[49] Para 4.29 below.

[50] Para 4.35 below.

[51] Para 4.18 below.

[52] Para 4.28 below.

[53] Para 5.3 below.

[54] Para 5.7 below.

[55] Para 5.10 below.

concerned that our proposed offence, or the threat of prosecution for it, could be used to apply undue pressure on defendants to settle civil claims. We therefore provisionally propose that prosecutions for the offence be brought only with the consent of the Director of Public Prosecutions.[56]

1.31 We suggest certain exclusions from the scope of the offence. For example, we exclude confidential information which it was in the public interest to use or disclose.[57] Another proposed exclusion is information acquired by the defendant without his or her knowing that it was a trade secret, or that its previous acquisition involved the commission of an indictable offence or the summary offence of "hacking" into a computer contrary to section 1 of the Computer Misuse Act 1990.[58] We also exclude information disclosed in accordance with a statutory obligation or power, or pursuant to a court order or otherwise for the purpose of legal proceedings.[59] For each of the defences the accused would have an "evidential burden": he or she would have to adduce evidence that there was a reasonable possibility that the exclusion applied.[60] We conclude that liability should be negatived where the defendant mistakenly *believes* in the existence of a fact which, if it were true, would constitute an exclusion.[61] In all these matters the views we express are purely provisional.

1.32 In Part VII we look at whether the mere *acquisition* of confidential information should be criminalised. We make no provisional proposals on this matter, but discuss the forms that such an offence might take. Finally we consider the relationship between civil and criminal proceedings for trade secrets misuse. This raises two main questions: first, the extent (if any) to which a defendant can refuse to answer questions or produce documents by relying on the privilege against self-incrimination. We provisionally propose that the privilege should not be invoked in civil proceedings on the grounds of fear of prosecution for our proposed offence or for any conspiracy offence.[62] Secondly, we also invite views on whether civil proceedings should be stayed when criminal proceedings for the same matter are expected or have been commenced.[63]

[56] Para 5.15 below.

[57] Para 6.54 below.

[58] Para 6.28 below.

[59] Paras 6.56 – 6.57 below.

[60] Paras 6.1 – 6.2 below.

[61] Para 6.1 below.

[62] Para 8.37 below.

[63] Para 8.43 below.

# PART II
# PREVIOUS PROPOSALS FOR REFORM

2.1 The enormous increase of the importance of information in recent years, coupled with a corresponding growth in the availability and use of surveillance devices, has given rise to concern over the ease with which confidential information can be acquired and misused. There have been a number of attempts to change the law with a view to maintaining proper standards of fair dealing in this area of commercial life.

### LORD BOYLE'S BILL (1968)

2.2 In 1968 Lord (then Sir Edward) Boyle introduced an Industrial Information Bill aimed at rendering criminal (as well as giving a civil remedy for) industrial espionage, described as the "misappropriation of industrial information".[64] The Bill defined such information, apparently exhaustively, as comprising

> unregistered or incomplete patent, trade mark, or design information, know-how, research and technical data, formulae, calculations, drawings, results, conclusions, costings, price structures, contracts, lists of suppliers or customers, and private business discussions, or memoranda of the same.[65]

2.3 Under the Bill the offence would be committed by a person who "without the consent of the rightful owner and possessor" of the information,[66]

> (a) reads, copies, receives or records such information with any photographic and/or electronic device, or
>
> (b) obtains such information from any computer, data bank, memory core, laser beam, satellite, or from any cable telephonic or television system.[67]

2.4 The Bill was not supported by the Government.[68] The debate on the Second Reading was adjourned[69] and never resumed.

[64] *Hansard* (HC) 13 December 1968, vol 775, cols 802–828.

[65] Clause 3.

[66] Defined as: respectively, any person who at the time of the alleged misappropriation had a bona fide de jure claim, and de facto control of access to, the information; "save that in relation to receiving or recording private business discussions the rightful owner or possessor shall be deemed to be all parties to such discussion": cl 7.

[67] Clause 1.

[68] Mr Edmund Dell (the Minister of State, Board of Trade) stated, however, that the Government proposed to consider the problem, and was prepared to discuss it with interested individuals and the CBI: *Hansard* (HC) 13 December 1968, vol 775, col 823.

[69] *Ibid*, at col 828.

## THE REPORT OF THE YOUNGER COMMITTEE ON PRIVACY (1972)[70]

2.5 The Younger Committee's terms of reference were:

> To consider whether legislation is needed to give further protection to the individual citizen and to commercial and industrial interests against intrusions into privacy by private persons and organisations, or by companies, and to make recommendations.[71]

2.6 The Committee considered, among many other matters, industrial espionage (under the heading "Intrusion in Business Life"). In considering how to define industrial and commercial espionage for its purposes, the Committee referred both to the definition of industrial information in Sir Edward Boyle's Bill and to a definition of industrial espionage suggested to the Committee by Interpol, which referred to

> intellectual property (inventions, results of experimentation, new processes) belonging to a person or corporate body, which has been developed or legally acquired by that person or body for the purpose of producing something that has or may have industrial value and, in more general terms, value to the national economy.

The Committee accepted both definitions, which it summarised as "the improper acquisition for gain of valuable industrial or commercial information".[72]

2.7 The Committee explained that it had experienced difficulty in getting "hard facts" about cases of industrial and commercial espionage,[73] and that its main difficulty about formulating any proposal lay

> in deciding where to draw the line between methods which consist of the 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 promotion methods 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.[74]

[70] Cmnd 5012. Its chairman was the Rt Hon Kenneth Younger.

[71] *Ibid*, at para 1.

[72] *Ibid*, at para 479.

[73] The Committee was, however, "not surprised" at this. It observed (at para 492):

> In many cases it appears that companies simply do not know that they are the targets of such activity. In others they are reluctant to admit that through ignorance or complacency they have suffered. There are cases which never reach the courts either because the offences are trivial, because they are more easily dealt with by dismissing a suborned or otherwise disloyal employee, or because the victim wishes to hush the matter up. Some concerns – particularly the larger and more vulnerable – employ their own or outside security organisations to combat malpractices. It is possible that some organisations regard it as a legitimate tactic in a competitive world and that some actively engage in it.

[74] At para 493.

2.8 The Committee made no recommendations relating specifically to industrial and commercial espionage. It pointed out, however, that three recommendations made elsewhere in the report would give better protection against the unauthorised extraction and use of confidential information. Only one of the recommendations involved criminal sanctions – namely, that there should be a new criminal offence (as well as a new tort) of unlawful and surreptitious surveillance.[75] The other recommendations were that the law of breach of confidence should be considered by the Law Commissions (of England and Wales and of Scotland), and that there should be a new tort of disclosure or other use of unlawfully acquired information.

### OUR BREACH OF CONFIDENCE REPORT (1981)

2.9 This Commission came to consider the protection of confidential information in its report on breach of confidence,[76] which was based on a 1974 working paper.[77] Both were a sequel to the Younger report.[78] The second limb of our terms of reference required us

> to consider and advise what remedies, if any, should be provided in the law of England and Wales for persons who have suffered loss or damage in consequence of the disclosure or use of information unlawfully obtained and in what circumstances such remedies should be available.

2.10 We regarded this as directing our enquiry to whether remedies for breach of confidence should cover situations where there is no acceptance of an obligation of confidence but it is right that one should be constructively imposed.[79]

2.11 Our central recommendation was that breach of confidence at common law should be abolished and replaced by a statutory tort of breach of confidence.[80] We further concluded that an obligation of confidence should arise where information is acquired by certain reprehensible means.[81] For example, a duty of confidence would arise where the information was obtained by an unauthorised taking, handling or interfering with anything containing the information; where it was

[75] See para 563. The offence would comprise the following elements:

a. a technical device;
b. surreptitious use of the device;
c. a person who is, or his possessions which are, the object of surveillance;
d. a set of circumstances in which, were it not for the use of the device, that person would be justified in believing that he had protected himself or his possessions from surveillance whether by overhearing or observation;
e. an intention by the user to render those circumstances ineffective as protection against overhearing or observation; and
f. absence of consent by the victim.

[76] Breach of Confidence (1981) Law Com No 110.

[77] Breach of Confidence, Working Paper No 58.

[78] See paras 2.5 – 2.8 above.

[79] Law Com No 110, para 2.5.

[80] *Ibid*, at para 6.5.

[81] *Ibid*, at para 6.46.

obtained by violence, menace or deception; or where it was acquired by a device made or adapted solely for the purpose of surreptitious surveillance and the user would not have obtained the information without using the device.[82] The report emphasised that only the *use* or *disclosure* of the wrongfully acquired information would attract civil liability.[83] We considered that the information should be protected only where

> after balancing the respective public interests in confidentiality on the one hand and in disclosure or use of the information on the other, the information is found to merit such protection.[84]

2.12 We also recommended that the remedy for breach of confidence where damage had already been suffered should be damages or an order to account for profits.[85] For an anticipated breach we recommended that injunctions and adjustment orders be available.[86] The report did not propose the creation of any criminal offences.[87]

2.13 The Government accepted our recommendations, but they have not become law. In 1989 the Attorney-General[88] stated that the report, for the most part, amounts to a restatement of the common law, and that the Government therefore did not intend to give its implementation high priority.[89] The relevant clause in the draft legislation annexed to the report is set out in Appendix A to this paper.

### THE REPORT OF THE CALCUTT COMMITTEE ON PRIVACY (1990)[90]

2.14 The Calcutt Committee was concerned not with commercial or industrial information, but with the protection of individual privacy against the press. It recommended (among other things) the introduction of three offences proscribing certain kinds of activity conducted with the intention of obtaining personal information.[91] The offences were:

(1) Entering private property, without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication.

[82] *Ibid*.

[83] *Ibid*, para 6.59. See paras 5.1 – 5.2 below.

[84] *Ibid*, para 6.84. See para 6.40 below.

[85] *Ibid*, para 6.114.

[86] *Ibid*.

[87] See *ibid*, para 2.7.

[88] The Rt Hon Sir Patrick Mayhew QC, MP.

[89] Written Answer, *Hansard* (HC) 2 March 1989, vol 148, col 257.

[90] Report of the Committee on Privacy and Related Matters (1990) Cm 1102. The Committee was chaired by David Calcutt QC, who in 1992 was asked to consider whether self-regulation by the press had worked. He concluded in his Review, Cm 2135 (1993), that it had not, and he recommended that the Government should now give further consideration to the introduction of a new tort of infringement of privacy: paras 5.26, 7.33 – 7.42.

[91] Calcutt report, at para 6.33.

(2) Placing a surveillance device on private property, without the consent of the lawful occupant, with intent to obtain personal information with a view to its publication.

(3) Taking a photograph, or recording the voice, of an individual who is on private property, without his consent, with a view to its publication and with the intent that the individual shall be identifiable.

2.15 The Committee further recommended[92] that an individual with a "sufficient interest"[93] should be able to apply for an injunction against the publication of material obtained by means of any of the proposed offences or, where the material had already been published, damages or an account of profits.

[92] *Ibid*, at para 6.38.

[93] The phrase used by Lord Denning MR in *Chief Constable of Kent v V* [1983] QB 34, 43.

# PART III
# THE NEED FOR NEW OFFENCES

3.1 In this Part we examine the arguments for and against the creation of criminal offences of trade secret misuse. We provisionally conclude that the case for creating such offences is a strong one. It rests primarily on the argument that the "theft" of a trade secret is closely analogous to the theft of property in the strict sense, and on the economic importance of protecting businesses' investment in research, coupled with the inability of the civil law alone to provide effective protection.

3.2 The question of whether or not to criminalise any given conduct involves many different issues, and it is easy to lose sight of the relationship between them. For the purpose of the present exercise we have tried to structure the discussion, by considering separately the following issues:

(1) In what ways is the misuse of trade secrets *harmful*?

(2) Is criminalisation *necessary*?

(3) Is criminalisation *practical*?[94]

### IN WHAT WAYS IS THE MISUSE OF TRADE SECRETS HARMFUL?

3.3 In one sense, "harm" may be defined as the "thwarting, setting back, or defeating of an interest".[95] An interest can be said to have been "set back" by an invasion of it when it is in a "worse condition than it would otherwise have been in had the invasion not occurred at all".[96] An interest can be set back without the "owner" of the interest being wronged – for example, where a company undercuts a competitor to force it out of business. We are not concerned with this kind of case. The misuse of trade secrets is, in general, remediable as a matter of civil law, and we do not suggest that it might be made criminal in any case where it is not already actionable. Only conduct which is both damaging *and* wrongful (that is, actionable) would be caught by the offences we envisage.

[94] This approach owes much to the work of Jonathan Schonsheck: *On Criminalisation: An Essay in the Philosophy of the Criminal Law* (1994). For present purposes, however, we have omitted what arguably should be the first stage of the enquiry, namely, from what *perspective* should it be determined whether criminalisation is justified? This initial stage would be concerned with the limits of the state's moral authority over individuals, and would require an assessment of the main philosophical perspectives towards the issue of what conduct can properly be made criminal. We included a survey of these perspectives as Appendix C to Consent in the Criminal Law (1995) Consultation Paper No 139. Depending on the particular kind of conduct under discussion, it might be important to clarify which of these theories is the basis for the argument that that conduct should or should not be criminal. For the purposes of the present paper, however, we believe that this exercise is unnecessary and would not be particularly helpful, since the conduct with which we are here concerned is the kind of conduct which no-one would seriously argue to lie outside the scope of the state's moral authority: it causes harm to persons other than the actor, and therefore satisfies even the liberal's criterion of what can justifiably be criminalised.

[95] J Feinberg, *Harm to Others* (*The Moral Limits of the Criminal Law*, vol 1, 1984) p 33.

[96] *Ibid*, p 34.

3.4 We will now try to identify the various kinds of harm that trade secret misuse may cause.

### Confidentiality

3.5 The exchange of information between people working in the course of a business, which relies on the withholding of that information from competitors and the public, places all such individuals in a confidential relationship. Failure to protect obligations of confidentiality could inhibit both the quantity of information exchanged and its quality. But this is not in itself a particularly strong argument for criminalisation: no-one would suggest that breach of confidence should be criminal *in itself*. The question is whether, and if so why, trade secret misuse is *more* harmful than the breach of other forms of confidence.

### Economic interests

3.6 The "owner" of the secret will in most cases have worked to discover or create the secret. He or she has a clear *economic* interest in the information, and an equally clear interest in its remaining secret.[97]

3.7 In addition to this *private* economic interest there is a general *public* interest in protecting the secrecy of such information. If society fails to protect it, there is no incentive to do the work necessary to discover or create it. This aspect of trade secrecy has attracted considerable attention from the Chicago school of economic theorists.[98] The concern for these theorists is to maximise *efficiency*. Although the main focus of the economic analysis has been in relation to the law of tort and contract, there have been numerous attempts both to explain the existing criminal law and to make reform proposals on the basis of the economic theory. An economic explanation of *all* crime is clearly unrealistic,[99] but in the context of economic harms (such as trade secret misuse) the theory may be helpful. It is used to explain the operation of the criminal justice system in deterring rational individuals from engaging in criminal activity "by imposing costs on [crimes], thereby providing the individual with an economic incentive to choose not to commit a crime".[100] Crime is assumed to be an economic activity with rational participants. A person will commit a crime only if his or her expected utility exceeds the level of utility he or she could derive from alternative, lawful activities.

[97] See C R J Pace, "The Case for a Federal Trade Secrets Act" (1995) 8 Harv J Law and Technology 427, 438.

[98] Including Ronald Coase, Guido Calabresi (a Judge of the US Court of Appeals, Second Circuit, and formerly Dean of the Yale Law School) and Richard Posner (who is a Chief Justice of the US Court of Appeals, Seventh Circuit and Senior Lecturer at the University of Chicago Law School).

[99] It has been suggested, for example, that the criminalisation of rape is justified as maximising the efficiency of marriage.

[100] R A Posner, *Economic Analysis of Law* (3rd ed 1986) p 200. See also G Becker, "Crime and Punishment: An Economic Approach" (1968) 78 J Pol Econ 169–217.

3.8 According to Posner, "The purpose of ... according legal protection to secrecy … is to create an incentive to invest in the creation of information".[101] Similarly, Scheppele argues that there is a public interest in the production of "knowledge":

> Scientific knowledge, for example, is generally the product of much time and effort. It is expensive to produce. Whether rational actors will engage in the production of costly information depends on whether they can recoup enough of the benefits the knowledge brings to make the search worth their while.[102]

3.9 There are also economic *dis*advantages in the production of secret information. These stem from the fact that the producer will keep secret about the research until it can be protected, thereby leading to a great deal of duplicated research – which is not efficient.[103] Similar criticisms of inefficiency can be levelled at the concealment of information which, if known to one's competitors, would save them from duplicating *unproductive* research. At one level these considerations need to be balanced against the economic harm done by trade secret misuse. But this is the role of the civil law, not the criminal. In certain circumstances it has been decided that the misuse of secrets should be actionable. In those circumstances it would be inconsistent for the *criminal* law to steer clear on the ground that there are economic disadvantages in keeping information secret. If the disadvantages outweighed the advantages, the civil law should not be intervening either.

**Use value and monopoly value**

3.10 One useful analysis is that of Cross.[104] He argues that information may exhibit one or both of two characteristics: *use value* and *monopoly value*.

> Broadly speaking, information has use value if it can be utilized to lower the marginal costs of producing that firm's output … Monopoly value is the value attributable to being the only person who has access to the item of information.[105]

3.11 A trade secret has both monopoly value *and* use value, but only the former will normally be affected by misuse of the secret.

> [T]he spy does not actually take the information from the original holder, but instead merely copies the information. Copying, of course, leaves the information itself in the hands of the owner. Because the owner still retains possession and use of the information, its use value remains unaffected. The owner will be able to produce the product as cheaply and efficiently as before. Only monopoly value will be affected,

[101] R A Posner, *The Economics of Justice* (1981) p 244.

[102] K L Scheppele, *Legal Secrets: Equality and Efficiency in the Common Law* (1988) p 29.

[103] *Ibid*, p 30.

[104] J T Cross, "Trade Secrets, Confidential Information, and the Criminal Law" (1991) 36 McGill LJ 524.

[105] *Ibid*, pp 557–558.

and even then only if the information is made available to one or more competitors of the original owner.[106]

3.12 Cross goes on to assess the protection offered to use and monopoly value by the existing offences under Canadian criminal law. He identifies two basic types of harm – deprivation of information and copying information. He concludes that the offences of theft and vandalism will not adequately protect the interests of use and monopoly. Generally, theft will be ill suited to the protection of monopoly value because it focuses on deprivation and is tied in with the use value and rights of possession. It is important to note that in cases of copying there is no effect on the use value, and thus the theft provisions will not be applicable.[107] Cross concludes that it will be necessary to create new offences to protect property in information.

**Information as property**

3.13 The fact that property is regarded, in our society, as an interest worthy of protection (often by the use of criminal sanctions) is so well established as to require no further elucidation. What does need examination is whether trade secrets can properly be regarded as a form of property.

3.14 This is not a new idea: the debate as to whether information in general can be treated as a form of property has generated a considerable academic literature.[108] However, these discussions tend to be centred on the civil law. If they supported the general thesis that the civil law regards trade secrets as property for all purposes, that might, in itself, suggest that the criminal law ought to do the same. Unfortunately few of the commentators address themselves to this general question: rather, they analyse the decided cases in an attempt to discover whether property rights are the real basis of the action for breach of confidence.

3.15 A further difficulty is that many of the arguments are purely descriptive: in search of consistency they compare the attributes of "orthodox" property with those of information. These analyses are not necessarily helpful, because society's

[106] *Ibid*, p 560 (footnote omitted).

[107] Similarly the vandalism offence focuses primarily on use value.

[108] Including R G Hammond, "Theft of Information" (1984) 100 LQR 252; F R Moskoff, "The Theft of Thoughts: The Realities of 1984" (1984–85) 27 Crim LQ 226; J E Stuckey, "The Equitable Action for Breach of Confidence: Is Information Ever Property" (1981) 8 Sydney LR 402; S Ricketson, "Confidential Information – A New Proprietary Interest?" (1977–78) 11 Melb LR 223; N E Palmer, "Information as Property" in L Clarke (ed), *Confidentiality and the Law* (1990), reworked as N E Palmer and Kohler, "Information as Property" in N E Palmer and E McKendrick, *Interests in Goods* (1993); J T Cross, "Trade Secrets, Confidential Information, and the Criminal Law" (1991) 36 McGill LJ 524; R G Hammond, "Electronic Crime in Canadian Courts" (1986) 6 OJLS 145; D F Libling, "The Concept of Property: Property in Intangibles" (1978) 94 LQR 103; R G Hammond, "Quantum Physics, Econometric Models and Property Rights to Information" (1981) 27 McGill LJ 47, 59–60. On philosophical reflections on property generally see E F Paul, F D Miller and J Paul (eds) *Property Rights* (1994); A S Weinrib, "Information and Property" (1988) 38 UTLJ 117. See also Allison Coleman, *The Legal Protection of Trade Secrets* (1992) pp 48–49; W R Cornish, *Intellectual Property* (3rd ed 1996) paras 8.49 – 8.53; Breach of Confidence (1981) Law Com No 110, para 2.10.

perceptions of property change through time.[109] To be constrained by conventional perceptions is to ignore the rapid advances made in the uses and availability of information technology, which have led some to suggest that information is in fact the "currency of the age".

3.16 Nevertheless, in deciding whether it is possible to treat trade secrets as a form of property, a comparison of the attributes of trade secrets with those of orthodox property is a sensible starting point. And some of the key attributes of orthodox property – rights to create, use, alter, destroy, exchange etc – do seem to be shared by information.

### *A tradeable commodity?*[110]

3.17 Information, like property, is a tradeable commodity. This fact brings the economic arguments discussed earlier more clearly into focus. For example, the argument that the owner's investment in research and technology should be promoted by protecting the findings of that research is all the stronger if the owner's purpose is not merely to *use* those findings but to *sell* them.

### *Replication*

3.18 If information is property, does this mean that a new piece of property comes into existence every time the information is passed on? It is sometimes said that information cannot be property because it cannot be the subject of "exclusive ownership".[111] This is not in fact true, since everyone has information which no-one else knows; but that is of little assistance in the context of trade secrets which are disclosed by one person to another. A stronger argument in this context is that the information continues to be the same property when it is disclosed: it is its *ownership* that changes.

### *Infringement without harm*

3.19 If confidential information were characterised as property for the purposes of the criminal law, the logical consequence would be that *any* unauthorised use or disclosure of the information would be prima facie unlawful, without proof of harm to the information's "owner" – for example, where a secret technique is applied in a new field in which the "owner" does not do business. But this result could be defended on the basis that such use or disclosure must inevitably cause harm, if only in the sense that the "owner" has been deprived of the opportunity to charge for the use of the secret. Conversely, and for the same reason, a new offence might be framed in non-proprietary terms and yet *not* require proof of harm.

[109] As evidenced recently by cases dealing with computer disks, eg *Cox v Riley* (1986) 83 Cr App R 54.

[110] For a rather dated discussion of the assignable nature of trade secrets see R Ellis, *Patents Assignments and Licenses including Trade Secrets* (2nd ed 1943) ch IV.

[111] See also Organisation for Economic Co-operation and Development, *Computer-Related Crime* (1986) pp 24–26.

### *Judicial comment*

3.20 There is a substantial body of authority, from this country and elsewhere, which has considered, to varying degrees and in very varied contexts, the classification of information as a form of property.[112] As we have seen, the cases of *Oxford v Moss*[113] and *Absolom*[114] decide that information is not property for the purposes of the English law of theft. A similar conclusion was reached, after a much fuller analysis of the issues, by the Supreme Court of Canada in *Stewart*.[115]

3.21 On the other hand there are many civil cases in which the property model appears to be used – albeit sometimes as shorthand or metaphor.[116] The strongest of these cases, in English law, seems to be *Exchange Telegraph Co (Ltd) v Howard*,[117] where the plaintiffs complained of the defendant's unauthorised use of the plaintiffs' news of the latest cricket scores. Buckley J said:

> The knowledge of a fact which is unknown to many people may be the property of a person in that others will pay the person who knows it for information as to that fact. In unpublished matter there is at common law a right of property, or there may be in the circumstances of the case. The plaintiffs here sue, not in copyright at all, but in respect of that common law right of property in information which they had collected and which they were in a position to sell. Their case is that the defendant has stolen their property ... .[118]

3.22 Similarly in *Boardman v Phipps*[119] Lord Hodson said:

> Each case must depend on its own facts and I dissent from the view that information is of its nature something which is not properly to be described as property. We are aware that what is called "know-how" in

[112] Eg *Shelley Films Ltd v Rex Features Ltd*, 10 December 1993 (unreported, Ch D); *Helitune Ltd v Stewart Hughes Ltd* [1994] FSR 422; *PSM International plc & McKechnie plc v Whitehouse & Willenhall Automation Ltd* [1992] IRLR 279, 282; *Pickering v Liverpool Daily Post and Echo Newspapers plc* [1991] 2 AC 370; *Graeme John & Partners (A Firm) v Morgan*, 11 January 1990 (unreported, CA); *Brady v Chemical Process Equipments Pte Ltd* [1988] FSR 457 (High Court of Delhi); *Attorney General v Newspaper Publishing plc* [1988] Ch 33; *Norbrook Laboratories Ltd v King* [1984] IRLR 200, 206 (Northern Ireland CA); *Court Homes Ltd v Wilkins* (1983) 133 NLJ 698; *House of Spring Gardens Ltd v Point Blank Ltd* [1983] FSR 213 (High Court of Ireland); *Strathclyde Regional Council v Neil* [1984] IRLR 11, 12 (Sheriff Court, Edinburgh); *Thomas Marshall (Exports) Ltd v Guinle* [1979] Ch 227; *Yates Circuit Foil Company v Electrofoils Ltd* [1976] FSR 345, 384; *Ansell Rubber Co Pty Ltd v Allied Rubber Industries Pty Ltd* [1967] VR 37 (Supreme Court of Victoria); *Gledhow Autoparts Ltd v Delaney* [1965] 1 WLR 1366; *Routh v Jones* [1947] 1 All ER 179, 181.

[113] (1979) 68 Cr App R 183; para 1.4 above.

[114] *The Times* 14 September 1983; para 1.5 above.

[115] (1983) 149 DLR (3d) 583.

[116] See Allison Coleman, *The Legal Protection of Trade Secrets* (1992) p 98. On the use of property as a metaphor see Francis Gurry, *Breach of Confidence* (1984) pp 46–48.

[117] (1906) 22 TLR 375.

[118] *Ibid*.

[119] [1967] 2 AC 46.

> the commercial sense is property which may be very valuable as an asset.[120]

Lord Guest also saw no reason why information and knowledge should not be trust property.[121]

3.23 Others, however, have regarded this approach as something of an over-simplification. For them, the similarity of confidential information to property lies less in its *nature* than in the fact that equity protects it with the *remedies* appropriate to property rights. In the Australian case of *De Beer v Graham*,[122] rejecting a claim to property in an unpatented secret recipe, Owen CJ in Equity said:

> Property may be defined to be the exclusive right to the possession or enjoyment of something; such right may be limited in time or by conditions, but while it lasts it must be exclusive. So long as the secret remains undivulged it remains the exclusive possession of him who has the secret, but when divulged or rediscovered, the exclusive possession has ceased and I cannot see any principle on which the divulgence of the secret can be restrained, unless there be contract or relationship between the parties of trust or confidence, or some fraud in acquiring the secret. … [T]he Court acts on the conscience of the party, and not on any ground of property.

Similarly in *Boardman v Phipps* Lord Upjohn, while acknowledging that "confidential information is often and for many years has been described as the property of the donor", concluded that

> in the end the real truth is that it is not property in any normal sense but equity will restrain its transmission to another if in breach of some confidential relationship.[123]

3.24 Reviewing the authorities in *Smith Kline & French Laboratories (Australia) Ltd v Secretary, Department of Community Services and Health*,[124] Gummow J noted that trade secrets may devolve by operation of law, as upon bankruptcy,[125] and by testamentary provision;[126] that a secret process employed in a business may be held in trust in connection with a trust of the business,[127] or the subject of an equitable charge given to a creditor;[128] and that in some circumstances the obligation to

[120] *Ibid*, at p 107.

[121] *Ibid*, at p 115.

[122] (1891) 12 NSWLR (E) 144, 146.

[123] [1967] 2 AC 46, at pp 127, 128.

[124] (1990) 95 ALR 87. The Federal Court of Australia upheld Gummow J's decision but did not find it necessary to express a view on his analysis of the proprietary character of confidential information: (1991) 99 ALR 679.

[125] *Re Keene* [1922] 2 Ch 475. Gummow J noted that the secret formulae in issue in that case had never been committed to writing.

[126] *Morison v Moat* (1851) 9 Hare 241, at pp 241, 265; 68 ER 492 at pp 493, 502.

[127] *Scott on Trusts* (4th ed 1987) §82.5.

[128] *Struthers v Hospital Products Ltd* (unreported, Sup Ct of NSW, 25 February 1984).

observe an obligation of confidence may be extended to a third party.[129] He cited the dictum of Lord Wilberforce in *National Provincial Bank Ltd v Ainsworth*[130] that

> Before a right or an interest can be admitted into the category of property, or of a right affecting property, it must be definable, identifiable by third parties, capable in its nature of assumption by third parties, and have some degree of permanence or stability …

3.25 He concluded:

> The degree of protection afforded by equitable doctrines and remedies to what equity considers confidential information makes it appropriate to describe it as having a proprietary character.

But he added:

> This is not because property is the basis upon which protection is given, but because of the effect of that protection.[131]

As it was later put in the leading textbook (of which Gummow J is a co-author),

> The point is that the effect of the protection given endows confidential information with some proprietary characteristics, although they are not the reason for equitable intervention.[132]

3.26 We respectfully agree. Our provisional view is that confidential information is not property *in the strict sense*, and that it would be a mistake for the criminal law to pretend that it is. For this reason, the extension of the criminal law that we propose is not modelled on the law of theft or other offences against property. This approach is supported by the fact that trade secret misuse typically affects only the "monopoly value" of the secret, not its "use value".[133] But the *form* that an offence might take is a separate issue.[134] On the question whether an offence should be created at all, our provisional view is that the similarities between confidential information and property are such as to outweigh the differences between them. As one Canadian judge pointed out:

> If questioned, a businessman would unhesitatingly state that the confidential lists were the "property" of his firm. If they were surreptitiously copied by a competitor or outsider, he would consider his confidential data to have been stolen.[135]

[129] *Malone v Metropolitan Police Commissioner* [1979] Ch 344, 361; *Wheatley v Bell* [1982] 2 NSWLR 544.

[130] [1965] AC 1175, 1247–1248.

[131] (1990) 95 ALR 87, 135–136.

[132] Meagher, Gummow and Lehane, *Equity: Doctrines and Remedies* (3rd ed 1992) para 4117.

[133] See paras 3.10 – 3.12 above.

[134] See Part V below.

[135] *Stewart* (1983) 149 DLR (3d) 583, 600, *per* Cory JA.

### Conclusion

3.27 There can be no doubt that the misuse of trade secrets causes direct and indirect harms to very valuable interests, both private and public. The obvious conclusion is that such misuse requires regulation. This conclusion leads to the next stage of the enquiry: is it necessary to regulate such misuse via the *criminal* law as well as the civil?

## IS CRIMINALISATION NECESSARY?

3.28 Our starting point is the principle that criminalisation should be a last resort, and is justified *only* if civil liability is clearly an inadequate remedy for the mischief in question. We must therefore consider whether civil liability *is* in any respects inadequate as a means of regulating the misuse of trade secrets, and, if so, whether criminal liability would in those respects be more effective.

3.29 The imposition of liability in respect of a particular kind of harm may have various objectives, chief among them being

(1) prevention of the harm by pre-emptive action (such as injunctions, Mareva orders etc);

(2) compensation for the victim, where the harm has already been done; and

(3) discouraging prospective wrongdoers with the threat of liability for any harm that may be done.[136]

Each of these objectives may be important in a given situation; and, for the purpose of the first two, civil liability is clearly the more appropriate approach. If those two were the *only* objectives, there would be little or no purpose in resorting to the criminal law. It is the third objective, that of deterrence, that arguably justifies the imposition of criminal liability as well as civil.

3.30 We must therefore consider the following issues:

(1) How important is it to *prevent* the misuse of trade secrets, as well as providing compensation for the victim of such misuse when it occurs?

(2) How important is it to prevent such misuse *generally*, by deterrence, as well as specifically (for example, by injunction)?

(3) How effective as a deterrent is the threat of civil liability in damages? And could this threat be *made* sufficiently effective (for example, by making exemplary damages more widely available)?

[136] Another important objective of civil liability is the avoidance of unjust enrichment, eg by requiring an account of profits: *Seager v Copydex (No 1)* [1967] 1 WLR 923; *Seager v Copydex (No 2)* [1969] 1 WLR 809; P Birks, *An Introduction to the Law of Restitution* (1985) p 343; W R Cornish, *Intellectual Property* (3rd ed 1996) paras 2.42 – 2.43; G Jones, "Restitution of Benefits Obtained in Breach of Another's Confidence" (1970) 86 LQR 463; Breach of Confidence (1981) Law Com No 110, paras 4.78, 4.101. But, in the context of potential *criminal* liability, the possibility of unjust enrichment is insignificant by comparison with the potential harm to the victim.

### The need for prevention as well as compensation

3.31 The primary aim of a civil law action is generally to compensate the plaintiff; but in the case of trade secret misuse mere compensation will often be inadequate or impossible. The loss suffered may well be incapable of quantification, especially in cases of negative information. Compensation would be inadequate as a remedy where the owner's entire business depended on the secret. And in many cases an award of compensation is unlikely to be satisfied, because the defendant has insufficient means: he or she may have dissipated the profits or spirited them away, or may have acted out of malice rather than with a view to gain. It is therefore important not only to compensate the victims of trade secret misuse but also, as far as possible, to ensure that such misuse does not occur in the first place.

### The need for deterrence

3.32 The civil law offers machinery for the prevention of wrongs which are known to be threatened. For example, injunctive relief may be available to prevent an anticipated or continuing breach of confidence. But this may be of limited use where the owner of the secret has no advance warning of the intention to misuse it: by the time legal action can be taken, the damage may already have been done. The law also needs to deter those who are tempted to misuse secrets *without* any advance warning. This means that the risk of liability for such misuse needs to be such as to outweigh the reasons (mercenary, malicious or otherwise) for engaging in it.

### Damages as a deterrent

3.33 Our provisional view is that the remedies mentioned above are no more adequate to discourage trade secret misuse than they are to discourage simple theft. The only remedy that is likely to be effective in counterbalancing the chance of profit (or the satisfaction of paying off a grudge, or any other motive that may induce a person to misuse another's secret) is a *deterrent*; and the most obvious form of deterrent is the threat of imprisonment or some other punitive sanction. The question therefore arises: how effective a deterrent is the threat of civil liability in damages? In general, the function of damages is to compensate the victim, not to deter others who might be tempted to follow the defendant's example; and therefore the risk of being held liable in damages is rarely a significant deterrent. But it must not be overlooked that damages can also take a deterrent form, namely that of *exemplary* damages.

3.34 There appears to be no authority for the award of exemplary damages for breach of confidence, such as trade secret misuse, and it is uncertain whether such damages could be awarded in the present state of the law.[137] But for present

[137] Exemplary damages are available only to the extent that they were available before the House of Lords' restatement of the position in *Rookes v Barnard* [1964] AC 1129: *AB v West Water Services* [1993] QB 507. It was recognised in *Rookes v Barnard* that exemplary damages might be awarded where the defendant had cynically committed the tort in order to make a profit; but it is not clear whether trade secret misuse is better regarded as a tort or as a purely equitable wrong. Exemplary damages are not available for breach of contract: *Addis v Gramophone Co Ltd* [1909] AC 488. See Aggravated, Exemplary and Restitutionary Damages (1993) Consultation Paper No 132, para 3.78.

purposes this is immaterial: if the availability of exemplary damages *would* be an adequate deterrent then it follows that there is no pressing need for criminalisation. The more appropriate response would be to make it clear that exemplary damages *are* available. The question here is not whether they are available now, nor even whether they should be *made* available, but whether, *if* they were made available, this would be enough of a deterrent.

3.35 Where the actors involved in the trade secret misuse are corporate actors, there is no possibility of imprisonment,[138] and the deterrent effect of the threat of exemplary damages may be equal to that of a criminal fine. For an individual, however, the threat of imprisonment or other criminal sanctions is likely to be a more effective deterrent than the risk of having to pay exemplary damages.

3.36 Moreover, in many cases the defendant will not be *able* to pay damages. The profits actually derived from the misuse of the secret may be far less than an appropriate level for an award of exemplary damages. There may never have been any profit at all, for example where the defendant is motivated by spite rather than greed. Or the profits may have disappeared before judgment can be obtained.

3.37 We provisionally conclude that none of the remedies that are currently available in the civil courts, or that might be made available, are or would be sufficient in themselves to discourage those with access to trade secrets from misusing them.

### Cost and delay

3.38 Even if the remedies available were adequate, a further difficulty for the plaintiff lies in the cost and length of the procedure for obtaining them. The costs involved in bringing an action in tort must be borne by the individual plaintiff. This presents a considerable disadvantage in the civil law system. Where a small company possesses the trade secret, and it is obtained by a multi-national, it is all too easy to imagine the potential for abuse of the smaller company. The cost of litigation to prevent the multi-national using the trade secret may well be too great.

3.39 Delay is also a relevant factor. The large company is more financially capable of stalling the proceedings for as long as possible; the smaller firm is less able to deal with the expense inherent in such delay.

### Consistency

3.40 Over recent years there has been increasing concern about the damage that can be caused by the illicit use of intellectual property. As Professor A T H Smith explains, "The harm to the producer is obvious enough: he does not make profits

Under the Copyright, Designs and Patents Act 1988, ss 97(2) and 229(3), the court may award "additional damages" having regard to the flagrancy of the infringement and any benefit accruing to the defendant. Additional damages are permissible without the court having to consider whether effective relief is otherwise available. Professor Cornish gives the example of a professional photographer who supplies to the press a wedding photograph of a murder victim, without the consent of the victim's family (who own the copyright): *Intellectual Property* (3rd ed 1996) para 11–61.

[138] See C Wells, *Corporations and Criminal Responsibility* (1993); J Gobert, "Corporate Criminality: New Crimes for the Times" [1994] Crim LR 722.

he would otherwise have made, his investment in development and research does not earn its full reward, and his business is less profitable".[139] As a result, various kinds of infringement of intellectual property rights have been made criminal. The Copyright, Designs and Patents Act 1988 created a number of offences, mostly aimed at commercial counterfeiters and those who dishonestly exploit the work of performers.[140] Trade marks are also increasingly protected by criminal sanctions;[141] indeed, the maximum penalties for the fraudulent use of a trade mark are greater than those available for theft.[142] There are now criminal sanctions for unauthorised access to information held on computers, and for unauthorised use of information protected by the data protection legislation. These offences are outlined in Part I.[143]

3.41 Given the availability of criminal sanctions for the misuse of information in these situations, it is arguably inconsistent for the legal system to impose no such sanction for the misuse of a trade secret. There are obvious parallels between trade secret misuse and, for example, breach of copyright. Indeed, the former may in some circumstances inflict greater loss than the latter.

3.42 A possible counter to this argument is the fact that many deliberate infringements of intellectual property rights are *not* criminal, by statute at any rate.[144] Breaches of copyright and of registered trade marks are;[145] infringements of patents, design rights, plant variety rights, semiconductor topography right, and unregistered marks and names, are not. At present, the misuse of confidential information such as trade secrets falls into the latter category. It may be asked why the misuse of trade secrets should be singled out from the others in that category and transferred to the former. Given that it is desirable for the law to treat similar situations in a similar way, why is the misuse of a trade secret *more* analogous to the infringement of a copyright or a registered trade mark than to that of (for example) a patent or a design right?

3.43 This argument invites the question why the existing law draws this distinction between different kinds of intellectual property. A possible answer is that it is a historical accident rather than the application of any general principle. But we think it may be possible to justify the existence of the distinction (though not necessarily the precise point at which it is currently drawn) by reference to our basic principle: that criminalisation is justified only if it is both *necessary* (because

[139] A T H Smith, *Property Offences*, para 10–02.

[140] See paras 1.9 – 1.12 above.

[141] See paras 1.13 – 1.14 above.

[142] The maximum penalty on conviction on indictment is ten years' imprisonment, a fine or both: Trade Marks Act 1994, s 92(6)(b).

[143] See paras 1.16 – 1.20 above.

[144] Where such an infringement is the work of two or more people acting in concert, it is likely to constitute a conspiracy to defraud at common law: see paras 1.21 – 1.22 above. But the anomalous character of conspiracy to defraud makes it an unhelpful example in the context of *consistency*. It could scarcely be argued that conduct ought to be criminal merely because it is comparable to some other conduct which would amount to a conspiracy to defraud.

[145] Copyright, Designs and Patents Act 1988, s 107; Trade Marks Act 1994, s 92.

civil liability is an inadequate remedy) and *practical*. There is no reason to assume that criminal liability is necessary for *all* intellectual property infringements: it may be necessary for some but not others. Similarly, there may be some kinds of infringement for which civil liability is not an entirely effective remedy but which it would be impracticable to criminalise.

3.44 Our main reason for suggesting that the civil law may not be a completely effective remedy for trade secret misuse is that the prospect of being held liable in damages (even exemplary damages) is no great deterrent to a potential wrongdoer who has insufficient assets to satisfy a judgment. For infringements by large corporations, the civil law is largely effective, and could doubtless be made more so; in the case of less affluent defendants, we suggest, it may have little effect. If this is indeed the case, it may help to explain the present distinction between those infringements that are criminal and those that are not. Pirated and counterfeit products, which copyright and trade mark legislation seeks to eliminate, are often made or distributed (or both) by small operators who can be caught *only* by some form of policing: in their case, civil process is probably not sufficient. In the case of protected inventions and designs, on the other hand, an infringer is arguably more likely to be an enterprise of substance.

3.45 Obviously there is no clear line between the kinds of infringement that are perpetrated by operators too small for the threat of civil liability to be an effective deterrent, and the kinds that are not. But it may be that some kinds of infringement are *commonly* (if not chiefly) committed by small operators, whereas in others the role of such operators is comparatively insignificant. Infringements of copyright and trade marks probably fall into the former category, infringements of patents and design rights arguably the latter. If this is the correct explanation of the present position, the question is: in which category does trade secret misuse belong?

3.46 This is essentially a question of fact, of the kind that we do not have the resources to answer without the assistance of consultees; and we should be particularly interested to see evidence as to the extent of the problem of trade secret misuse by small operators who are not amenable to control by the civil courts. The informal soundings that we took while writing this paper suggest that it is indeed a substantial problem. Admittedly it may not happen as *often* as copyright piracy or the counterfeiting of trade marks; but, on the other hand, any given instance of it is likely to result in *more serious damage* than a single act of piracy or counterfeiting. The significance of the problem may therefore be just as great.

3.47 The present position may also be influenced to some extent by practical considerations which militate against the criminalisation of certain kinds of infringement. It is possible, for example, that patents may in fact be infringed by small and impecunious operators as often as trade marks are – in which case civil liability might be an inadequate remedy in *both* cases. It would not follow that the law is defective in imposing no criminal liability for patent infringement, because there may be other factors at work. Proceedings for patent infringements are "notoriously complex"[146] and often lengthy. It might not be desirable for a criminal

[146] Laddie, Prescott and Vitoria, *The Modern Law of Copyright and Designs* (2nd ed 1995) para 43.41.

court to spend months determining, on the basis of highly technical scientific evidence, whether a patent had in fact been infringed. Similar considerations might, of course, apply to trade secret misuse; we return to this point below, when we consider whether criminalisation is *practical* as well as necessary.[147]

3.48 We invite the views of consultees on the principles that ought to determine which forms of intellectual property infringement should be criminal and which should not; and also, on the basis of our suggested distinction between infringements that are and are not commonly committed by *small* operators, into which category trade secret misuse properly falls. But our provisional view is that, if considered in terms not only of its frequency but also of its potential for damage to the owner's business, the misuse of trade secrets by individuals and small enterprises is a sufficiently serious problem to necessitate the supplementing of the civil law with criminal sanctions.

### Conclusion

3.49 We provisionally conclude that criminal liability would be a more effective way of regulating trade secret misuse than civil liability alone.

## IS CRIMINALISATION PRACTICAL?

3.50 But this is not the end of the enquiry: one further stage remains, namely to examine whether the social costs of criminalisation would exceed the social benefits. Even if criminalisation is theoretically the most appropriate approach, does it have too many practical disadvantages? Some of the factors that are relevant here overlap with the arguments addressed at the previous stage.

### Certainty

3.51 Perhaps the most important constraint on the choice to criminalise, rather than rely on the civil law, is the accompanying need for the certainty for which penal legislation ought to strive. Where the question is whether a person should be required to pay compensation or to account for a profit, it may be acceptable for the court to have a good deal of discretion in the application of general principles to the facts of the case. Where the question is whether that person should be convicted of an offence punishable with imprisonment, however, much greater certainty is required. It is unacceptable in principle that citizens should not be able to tell in advance whether particular conduct would or would not amount to a criminal offence.

3.52 In the case of economic activity, moreover, this is particularly undesirable. If it is efficient for a person to use certain information in the course of his or her business, it would be inefficient for the law to discourage that person from using it out of a groundless fear that a criminal court might hold such use to be unlawful. Those making decisions as to the allocation of resources should be able to do so on the basis of a clear understanding as to what is and is not permitted.

[147] Para 3.56 below.

3.53 It follows that, however ineffective the regulation of trade secret misuse by the civil law alone, it would not be practical to criminalise it unless the offence or offences can be drafted in terms that are reasonably precise. In the subsequent Parts of this paper we suggest ways in which this might be done, and we invite consultees to comment on whether we have achieved the degree of certainty that is required (and if not, how else we might do so).

### Costs of policing

3.54 Some crimes would be so difficult or costly to detect that it would be impossible to criminalise them. The cost of policing trade secret misuse is impossible to estimate in the absence of empirical material as to the frequency and seriousness of the offences.

3.55 As with the creation of any criminal offence, there will be demands on the resources of the police, prosecutors and so on. It is unlikely that *detection* would involve significant costs, since the investigation will always be in response to the complaint of an aggrieved individual, but prosecutions might be difficult and costly. In addition there is the danger that lengthy, expensive and high-profile trials would have (or be perceived to have) a disproportionate impact, as has recently been the case with serious fraud.

### Complexity of trials

3.56 We have suggested that the absence of any criminal remedy for patent infringements may be attributable not to the adequacy of the civil law but to the fact that the issues in such cases tend to be too complex for a criminal court.[148] It may be arguable that this is equally true of the issues likely to be raised in a case involving trade secrets. But not all trade secrets are scientific or technical, and the issues would often be comparatively simple. If trade secret misuse were made criminal, the likely length, complexity and cost of the proceedings would presumably be one factor to be taken into account by the Crown Prosecution Service[149] in deciding whether the public interest required a prosecution in any given case.

### Implications for civil liberties

3.57 There is no reason to suspect that the policing of trade secret misuse would result in an increase in the abuse of power by an enforcement agency. The policing may well have to involve covert surveillance techniques, but this will always be with the consent of the individual who believes that his secret is under threat.

## CONCLUSIONS

3.58 Like other forms of intellectual property, such as patents and copyrights, trade secrets are valuable commercial assets. The creator of the information that constitutes the trade secret commonly expends considerable resources to gain or

[148] Para 3.47 above.

[149] We provisionally propose that prosecutions for any new offence should be brought only by or with the consent of the DPP: see para 5.15 below.

to retain a competitive advantage over a competitor, which would be destroyed by the unauthorised use or public disclosure of that information.

3.59 Although trade secrets have existed for many years, the development in recent years of computers and telecommunications technology has enormously increased their relative importance. Many businesses, indeed, consider intangible information to be their most important asset. Civil remedies, under the law relating to breach of confidence, are available. We have little doubt, however, that the time is ripe for the civil law to be buttressed by an extension of the criminal law which would catch the person who deliberately, and with knowledge that particular information is a trade secret, deprives the holder of the benefit of the secret by destroying its quality of secrecy. In our view, it is anomalous that the criminal law should provide sanctions against the misappropriation of the physical medium on which information may happen to be stored (which may itself have little value) but not the misuse of the information itself. It is also noteworthy that Parliament has decided that the improper use of other forms of intellectual property (such as copyright and trade marks) should be criminal. We see no reason why different considerations should apply to the misuse of trade secrets.

3.60 **We provisionally conclude that the main arguments in favour of criminalising trade secret misuse are as follows:**

**(1) that there is no distinction in principle between the harm caused by such misuse and the harm caused by theft;**

**(2) that the imposition of legal sanctions is necessary in order to protect investment in research;**

**(3) that civil remedies alone are insufficient to discourage trade secret misuse (and would continue to be insufficient even if exemplary damages were made more widely available), because many wrongdoers are unable to satisfy any judgment against them;**

**(4) that it is inconsistent for the law to prohibit the infringement of copyright and registered trade marks but not the misuse of trade secrets; and**

**(5) that criminalisation would help to preserve standards in business life.**

We invite views on each of these arguments.

3.61 Our provisional view is that these arguments amount to a strong case for criminalisation, provided that the necessary offence or offences can be drafted in terms that are sufficiently precise. In the following Parts we consider how an offence of trade secret misuse might be framed with the necessary degree of precision, and provisionally conclude that this can indeed be done. **We therefore provisionally propose that the unauthorised use or disclosure of a trade secret should, in certain circumstances, be an offence.**

# PART IV
# THE DEFINITION OF A TRADE SECRET

### IS A DEFINITION NECESSARY?

4.1 It would in theory be possible to leave the expression "trade secret" undefined in legislation creating a new offence of trade secret misuse. There is precedent for this: for example, section 135 of the Factories Act 1961 (replacing earlier legislation), which formerly imposed on employers an obligation to give to pieceworkers particulars of work and wages, provided that it should be an offence for an employee to disclose those particulars "for the purpose of divulging a trade secret";[150] but the Act did not define a trade secret. Again, a number of modern Acts contain provisions prohibiting the unauthorised disclosure of (without definition) "trade secrets" obtained in connection with the exercise of a power of entry or inspection given by the Act.[151] We are unaware of any authority on the construction of the phrase in these provisions.

4.2 In Australia the term "trade secrets" has been used, without definition, in the (Commonwealth) Freedom of Information Act 1982. Its interpretation in that context fell for consideration by the Federal Court of Australia in *Searle Australian Property Ltd v Public Interest Advocacy Centre*.[152] The court held that, at least in the context of legislation relating to freedom of information, "trade secrets" was an ordinary term of the English language[153] and primarily involved a question of fact.[154] The court also ruled that, to constitute a trade secret, the information need not be of a technical nature, and drew a distinction[155] between a trade secret and confidential information:

> [T]he secrets must be used in or useable in the trade. A trade secret is an asset of the trade. Past history and even current information, such as mere financial particulars, may be confidential. The law may protect the disclosure of such information by a person who has obtained it in the course of a relationship which requires confidentiality, such as that

[150] Section 135(3). Subsection (4) provided for a further offence of, "for the purpose of obtaining knowledge of or divulging a trade secret", soliciting or procuring an employee to disclose such particulars (or paying an employee to disclose them) . The section was repealed by the Wages Act 1986, s 11 and Sch 1, and not replaced.

[151] Eg, by s 325(3) of the Town and Country Planning Act 1990 it is an offence for a person who, in compliance with a power of entry under the Act, is admitted into a factory, workshop or workplace, to disclose any information obtained there "as to any manufacturing process or trade secret". The offence is triable either way. Conviction on indictment attracts a maximum penalty of two years' imprisonment and an unlimited fine: s 325(5).

[152] (1992) 108 ALR 163.

[153] *Ibid*, at p 171. The court cited the *Oxford English Dictionary*, which defined "trade secret" as "a device or technique used in a particular trade or ... occupation and giving an advantage because not generally known".

[154] *Ibid*, at p 172.

[155] *Ibid*, at p 174. The court said, however, that "the more technical information is, the more likely it is that, as a matter of fact, the information will be classed as a trade secret".

of employee, solicitor or accountant. But such information may not be a trade secret.[156]

4.3 We do not, however, favour the introduction into the criminal law of a wholly new general offence which is aimed at the misappropriation of a particular category of information but leaves that category completely undefined.

4.4 We might have taken a different view had there existed a definition of trade secrets that was widely accepted in some field of the law; but this is not the case. In particular, there is in the area of employment law a substantial body of authority which reveals a range of judicial opinion on the definition (and the significance) of the term;[157] and this renders impracticable a second possible option, of embodying in legislation a definition that is already of general application in that field.

4.5 **We provisionally conclude that, for the purpose of any new offence of trade secret misuse, it would be necessary to provide a definition of a trade secret.**

## THE ELEMENTS OF A DEFINITION

### Categories of information that may constitute a trade secret

4.6 We mention four broad categories of information that, in our view, the definition of trade secrets should cover. The first comprises secrets relating to highly specific products, such as the formula for Coca-Cola, where, even if the secret is patentable, no patent has in fact been sought. It is a characteristic of this type of trade secret (a) that those who own it pass it down within a tightly controlled hierarchy; (b) that the product is freely available on the market, so that in principle a competitor could break the secret and so imitate (or even replicate) the product; and (c) that the business, being wholly dependent on the secret, would be likely to be destroyed if the secret came into the hands of a competitor.

[156] *Ibid*.

[157] There is no generally accepted definition of the term "trade secrets" in that context. It has been used in some cases to signify *confidential* information, as distinct from information amounting to the enhancement of an employee's skill or knowledge. In other cases (eg *Faccenda Chicken Ltd v Fowler* [1987] Ch 117) a distinction has been drawn between trade secrets on the one hand and merely confidential information on the other; see further para 4.21 below. However, the existence of that distinction has in turn been questioned. In *Lansing Linde Ltd v Kerr* [1991] 1 WLR 251, 260A–D, Staughton LJ said:

> [T]he problem is one of definition: what are trade secrets, and how do they differ (if at all) from confidential information? [Counsel] 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 the 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.

4.7 The second category comprises technological secrets. The ability of an enterprise to flourish (or sometimes even to survive) is directly related to its success in acquiring, protecting and exploiting some aspect of modern technology. By contrast with the first category of trade secret, an enterprise would not necessarily be ruined if information of this kind became available to others in the industry; but its ability to compete would be impaired.

4.8 The third category consists of strategic business information, such as internal marketing studies, industry forecasts and lists of customers. This type of information forms the data on which decisions on, for example, marketing or finance may be based. Its acquisition could alert a competitor to the business strategy likely to be adopted in a particular sector of the market, or save valuable start-up or expenditure in assembling the information.

4.9 The fourth category might not, in everyday parlance, be regarded as secret.[158] It consists of private collations of individual items of publicly available information, the value of which lies in their "packaging".[159] Information of this kind has become of much greater practical significance with the advent of the computer.[160]

### Other definitions

#### *The Alberta report*

4.10 In 1984 the Alberta Institute of Law Research and Reform produced a report for discussion on the protection of trade secrets under the civil law. Subsequently, it was decided that criminal sanctions should also be considered. The Deputy Attorneys General Responsible for Criminal Justice therefore set up a joint Federal/Provincial Working Party to examine both the civil and the criminal aspects of the subject.[161] They reported in 1986.[162] We refer to their report as the "Alberta report".

4.11 The term "trade secret" is defined in the draft Bill annexed to the report[163] as

[158] As the Alberta report (see para 4.10 below) points out, at para 2.7:

> "Secrecy" in such cases is something of a misnomer. It applies either because no one else has the equipment or know how to collate the relevant information or has not invested the time and resources required to do so.

[159] The inclusion of this category reflects the approach we adopted in Breach of Confidence (1981) Law Com No 110. See para 4.33 below.

[160] To cite the Alberta report (see para 4.10 below), at para 2.7:

> The greatest attribute of the computer is its ability to store and collate information. A new industry which utilizes this potential in the form of packaged information services has come into being. Individual bits of information, useless in themselves, are collated into usable packages and sold like any other commodity.

[161] In Canada the provinces are responsible for civil law, but criminal law is a federal matter.

[162] Alberta Institute of Law Research and Reform and a Federal Provincial Working Party, Trade Secrets (1986) Report No 46.

[163] As a proposed s 301.3(7) of the Canadian Criminal Code.

information including but not limited to a formula, pattern, compilation, program, method, technique or process, or information contained or embodied in a product, device or mechanism which:

(i) is, or may be used in a trade or business

(ii) is not generally known in that trade or business

(iii) has economic value from not being generally known, and

(iv) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[164]

### *The United States*

4.12 The first United States source is section 757 of the American Law Institute's Restatement of the Law of Torts (1939).[165] That section concerns liability for the disclosure or use of another's trade secret. The Restatement itself contains no definition of the term; but Comment (b) to the section,[166] while recognising the impossibility of supplying a precise definition, says:

> A trade secret may consist of any formula, pattern, device or compilation of information which is used in one's business, and which gives … an opportunity to obtain an advantage over competitors who do not know or use it. It may be a formula for a chemical compound, a process of manufacturing, treating or preserving materials, a pattern for a machine or other device, or a list of customers.[167]

4.13 The Restatement also contains a list of factors to be used in determining whether information can constitute a trade secret. They are:

(1) the extent to which the information is known outside the business;

(2) the extent to which it is known by employees and others involved in the business;

(3) the extent of measures taken to guard the information;

(4) the value of the information to the trader and his competitors;

(5) the amount of effort or money expended in developing the information; and

(6) the ease or difficulty with which the information could be properly acquired or duplicated by others.

[164] We consider at paras 4.18 – 4.22 below the requirement in these concluding words of the definition.

[165] Although intellectual property law, relating to such matters as patents and copyright, is governed by federal jurisdiction, the law of trade secrets is a matter for individual states. The Restatement definition has been adopted by the courts of most states. The second, updated, Restatement of the Law of Torts (1979) excluded trade secrets, on the ground (see 4 Restatement of Torts 2d at 1–2) that it no longer formed part of the general law of torts and merited separate treatment in a Trade Practices Restatement (which, however, has not emerged).

[166] Comment (b) has been very widely cited by courts throughout the United States and has acquired almost the same standing as s 757 itself.

[167] This definition was adopted in, eg, New York and Massachusetts: *Gilson v Republic of Ireland* 606 F Supp 38 (1984).

4.14 Comment (b) contained a further requirement, that of "continuous use": a trade secret, it explained, was a "process or device for continuous use in the operation of the business", and differed from other information in that

> it is not simply information as to single or ephemeral events in the conduct of a business, as for example the amount or other terms of a secret bid for a contract, or the salary of certain employees, or the security investments made or contemplated, or the date fixed for the announcement of a new policy or for bringing out of a new model or the like.[168]

4.15 Unlike the other elements of the Restatement definition, however, this requirement has not been adopted by courts in the United States.[169] Nor does it play any part in the English civil law relating to confidential information. In our view, it is plainly open to objection on grounds both of principle and of practicability. As to principle, we see no reason why, for example, the making of a take-over bid should be incapable of being a trade secret; and it could give rise to practical difficulty in determining whether, say, the annual accounts of a company at a certain date should be categorised as a continuous process or as a single "event".

4.16 The second source is the United States Uniform Trade Secrets Act, which defines a trade secret as meaning

> information, including a formula, pattern, compilation, program, device, method, technique, or process, that:
>
> (a) derives independent economic value, actual or potential, from not being generally known to, and not readily available by proper means by, other persons who can obtain economic value from its disclosure or use,[170] and
>
> (b) is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.[171]

4.17 According to this definition, although the information must have *some* actual or potential economic value to someone other than the holder of the secret, that other need not be a competitor at the material time. The reason for this, it has been suggested,[172] is that "even negative information that certain approaches are commercially unfeasible may be of economic value". In our view this is right in

[168] The instances cited by the Comment as falling within the definition included "a code for determining discounts, rebates or other concessions in a price list or catalogue, or a list of specialised customers, or a method of bookkeeping or other office management".

[169] Nor does it appear in the definition recommended in the Alberta report (set out at para 4.11 above).

[170] This definition, like that in the Restatement, is not exhaustive, and the meaning of the specific items is left to judicial interpretation. The definition does not, by contrast with that in the Restatement, expressly refer to lists of customers. It has been held, however, that the word "compilation" applies to such lists if they comply with the other elements of the definition: *United Centrifugal Pumps v Cusimano* 9 USPQ 2d 1171, 1178 (1989).

[171] See paras 4.18 – 4.22 below.

[172] Alberta report, para 10.15.

principle: for example, the results of experiments conducted by the research department of company A which reveal that the only method of manufacturing a product is prohibitively expensive would clearly be of value to company B which is considering whether to manufacture a product of that kind.

### Our provisional conclusions

#### *The conduct of the "owner"[173] of the secret*

4.18 If at the material time the owner of information does not regard it as secret, there is no reason why its use by another person should attract a criminal sanction, and **we provisionally propose that the definition of a trade secret should include a requirement that its owner has indicated, expressly or impliedly, a wish to keep it secret**. This principle is similar to that underlying the long-established definition developed in German law – namely

> facts existing in connection with a business enterprise, known only to a strictly limited group of persons or, stated differently, not publicly known, *which are to be kept secret according to the expressly stated or presumed intention of the enterprise*, having a justified interest in keeping these facts secret.[174]

4.19 In the United States a more rigorous requirement is imposed on the owners of trade secrets, who must take "sensible, effective, and affirmative steps to safeguard that which is said to be of commercial value".[175] Courts in the United States have carefully scrutinised the steps taken by companies in this respect, and have required a high standard.[176]

4.20 The rationale of this requirement seems to be that "the possessor [of] the information, if he says it *is* valuable, should be required to protect it".[177] It seems that the test is not whether the owner of the information was negligent on the particular occasion on which it came into unauthorised hands, but whether *in general* the owner made reasonable efforts to preserve its quality of secrecy.

4.21 In the English law of breach of confidence, this element appears to play a part, though indirectly rather than in terms, in determining whether information can

[173] We use this term here purely for convenience; it does not imply that a proprietary right is involved. See para 5.4 below.

[174] F-K Beier, "The Protection of Trade Secrets in Germany: A Short Appraisal in View of Japan's New Trade Secret Legislation" in H G Leser & T Isomura (eds), *Wege zum japanischen Recht* (1992) 817, 819 (italics supplied).

[175] Alberta report, para 10.22. The report instances the case of a major new development, where it may well be necessary for a special security system to be set up. In those circumstances, merely *telling* employees that the information is secret is unlikely to suffice.

[176] In, eg, *Electro-Craft v Controlled Motion Inc* 332 NW 2d 890 (1983) (Minn SC).

[177] See the Alberta report, para 10.16 (emphasis in original). The report adds: "The means and extent of protection will vary with the circumstances of the particular case, in the context of a particular trade or industry".

properly be regarded as a trade secret. Delivering the judgment of the Court of Appeal in *Faccenda Chicken Ltd v Fowler*,[178] Neill LJ explained:

> [T]he following matters are among those to which attention must be paid:
>
> (a) The nature of the employment … .
>
> (b) The nature of the information itself. … It is clearly impossible to provide a list of matters which will qualify as trade secrets or their equivalent. Secret processes of manufacture provide obvious examples, but innumerable other pieces of information are *capable* of being trade secrets … . In addition, the fact that the circulation of certain information is restricted to a limited number of individuals may throw light on the status of the information and its degree of confidentiality.
>
> (c) Whether the employer impressed on the employee the confidentiality of the information. Thus, though an employer cannot prevent the use or disclosure *merely* by telling the employee that certain information is confidential, the attitude of the employer towards the information provides evidence which may assist in determining whether or not the information can properly be regarded as a trade secret.
>
> (d) Whether the relevant information can be easily isolated from other information which the employee is free to use or disclose.[179]

4.22 For reasons both of principle and of practicality, we are not attracted by this alternative approach. As to principle, we do not believe that what is, in effect, the negligent failure of the owner of the secret to take adequate steps to protect it should in any circumstances negative the criminal liability of someone who, knowing of the owner's *intention* in this respect, deprives the owner of the secret. Our second, practical, reason for this view is that we regard the issue as inappropriate for determination by a jury in a criminal trial. There may, however, be other considerations that should be taken into account. **We ask for views on whether the definition of a trade secret should include a requirement that its owner has taken steps to keep it secret.**

### *Use in a trade or business?*

4.23 We have considered whether it should be a requirement, as the authors of the Alberta report propose, that the information is used in a trade or business. They favour this restriction on the ground that they are concerned

> to avoid giving any greater coverage to a trade protection secret statute than is warranted by the legitimate interests of the business community. To do otherwise would be to cut into what we regard as a cardinal principle – an open system of ideas and information.[180]

[178] [1987] Ch 117.

[179] *Ibid*, at pp 137, 138 (emphasis in original).

[180] Alberta report, para 10.23.

4.24 By contrast, the requirement does not appear in the definition in the (United States) Uniform Trade Secrets Act.[181]

4.25 The question involves policy issues on which we have not yet formed a view. However, on the assumption that the definition should include *some* reference to the use of the information in a trade or business, we have identified two matters for consideration.

4.26 The first is whether the secrets of someone engaged in a *profession* should be covered. It is arguable that, for example, a firm of accountants should be entitled to the same kind of protection for secret information relating to its practice as the lists of customers held by a commercial concern.[182]

4.27 The second question is whether the definition should extend to "pure" research – that is, research conducted outside the commercial context, at (for instance) a university. According to the Alberta report,

> It is plausible – and doubtless occasionally happens – that a researcher conceives and begins to develop something (which is kept secret) without any thought [of] or reference to commercial application. The reason for the secrecy is then likely to be either scientific caution or scientific pride (a desire to be first past the post). But if such a researcher (or his institution) can show even *some* potentiality of business use, the definition would apply, and that researcher would get protection, whatever the original motivation for the secrecy may have been.[183]

4.28 **We invite views on**

**(1) whether the definition of a trade secret should make reference to the use of the information in a trade or business; and**

**(2) if so, whether the definition should extend to**

**(a) information used in a profession, or**

**(b) "pure" (non-commercial) research.**

### *The information must not be generally known[184] and must derive value from that fact*

4.29 Obviously, information that "everyone knows" cannot be a trade secret. Moreover, information that is originally secret may lose its quality of secrecy by subsequent dissemination (as where, for instance, its owner includes it in the specification for

[181] Set out at para 4.16 above.

[182] Moreover, professional practitioners will often have entrusted to them in confidence trade secrets "belonging" to commercial clients, and will thereby be the "owners" of such secrets for the purpose of the offence that we propose in this paper: see para 5.4 below.

[183] Para 10.23 (emphasis in original).

[184] If it is decided that the information must be used in a trade or business (see paras 4.23 – 4.28 above), the question will arise: ought there to be an additional requirement, that the information is not generally known *in the particular trade*?

the purpose of a patent application)[185] and cannot thereafter be subjected to a right of confidentiality. This principle may apply even if the dissemination is wrongful;[186] and our intention is that, for the purpose of the proposed offence, it should apply in such circumstances.[187] **We provisionally propose that it should be an element of the definition of a trade secret that the information is not generally known.**

4.30 Where the information is disclosed only to a limited part of the public, the question is one of degree:[188] information may still be regarded as confidential even if it is quite widely available.

4.31 In some cases, however, there may be information which, though not (in the ordinary sense of the expression) generally known, is obtainable from sources that are publicly available. The question therefore arises: to what extent (if any) should such information be capable of amounting to a trade secret? A possible view is that, if the information is not, in that sense, "generally known", it is immaterial that the defendant could have acquired it from another source.[189] We do not share this view, however: we see no reason why the criminal law (any more than the law

[185] *O'Mustad & Son v Dosen* [1964] 1 WLR 109.

[186] There is a conflict of authority on the question whether publication of the information by a stranger or by the confidant necessarily destroys the confidential nature of the information. *Cranleigh Precision Engineering Ltd v Bryant* [1965] 1 WLR 1293, 1316, *per* Roskill J and *Speed Seal Products Ltd v Paddington* [1985] 1 WLR 1327, 1331D–1332B, *per* Fox LJ suggest that such publication does not necessarily destroy confidentiality. However, in *A-G v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109 Lord Goff of Chieveley disagreed with this view.

[187] In this respect we share the view expressed by Lord Goff of Chieveley in *A-G v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109. He explained, in relation to publication by a third party (at p 286A), that he could not see how the secret could continue to exist when the publication had been made by a third party. As to publication by the confidant (see p 28G–H), Lord Goff found it difficult to see how

> a confidant who publishes the relevant information to the whole world can be under any *further* obligation not to disclose the information, simply because it was he who wrongfully destroyed its confidentiality.

(Italics supplied)

[188] See, eg, *A-G v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 177C–D, *per* Sir John Donaldson MR. Bingham LJ referred (at p 215B) to F Gurry, *Breach of Confidence* (1984) p 70: "The basic attribute which information must possess before it can be considered confidential is inaccessibility – the information must not be common knowledge".

[189] This is the approach adopted by the Alberta report, para 13.41:

> If information in fact exists elsewhere, a sufficient degree of availability of that information would mean that it is no longer a secret. Thus, there is the possibility of an "open" secret: information lying undetected in publicly available documents. Nevertheless, our offences seek to proscribe socially unacceptable conduct. It is anomalous to permit an accused to escape sanction on the basis that, while his or her conduct was egregious, and fell within the definition of the offence, it need not have been so since, had the accused wished, he or she might have acquired the secret from another source.

The authors of the report refer to the fact that in Wisconsin, Maryland and Minnesota it is a defence to a charge of misappropriation that the trade secret was rightfully known to the accused or that it was available from another source: para 13.40.

of confidence) should protect, for instance, information which, though easily obtainable by anyone from consulting standard reference books in a public library, a company directs its employees to treat as secret.

4.32 On the other hand, under the law of confidence, it is possible to have, for example, a confidential document which is the result of work done by its maker upon materials available to anybody; what makes the document confidential is the fact that the maker has "used his brain and thus produced a result which can only be produced by somebody who goes through the same process".[190] And there may be confidentiality in a compilation of individual items, none of which is itself confidential.[191]

4.33 This approach accords with the policy that underlies our provisional proposals in this paper;[192] and it is reflected in clause 2 of the draft Bill annexed to our Breach of Confidence report,[193] which provides (in part):

> (1) An obligation of confidence can arise under this Act only with respect to information which is not in the public domain …
>
> (2) Information in the public domain includes information which is public knowledge or accessible to the public (whether or not on payment of a fee or subject to any other restriction); but, for the purposes of this Act, information which is capable of being extracted from any matter in the public domain (whether a document, product, process or anything else) is not in the public domain on that ground alone if such extraction would require a significant expenditure of labour, skill or money.

**We provisionally propose that, for the purpose of the requirement that the information is not generally known, the expression "generally known" should be (partially) defined in terms similar to the definition of "information in the public domain" in the draft Bill annexed to our Breach of Confidence report (Law Com No 110).**

4.34 It would, we believe, be unduly burdensome to require the prosecution to prove the existence of this negative element in every case, and **we provisionally propose that the prosecution should not have to establish that the information was not generally known**[194] **unless there is some evidence that it was**. The defendant would, in other words, have an "evidential" burden on the issue.[195]

[190] *Saltman Engineering Co Ltd v Campbell Engineering Co Ltd* (1948) 65 RPC 203, 215, *per* Lord Greene MR.

[191] Eg a list of customers: *Roger Bullivant Ltd v Ellis* [1987] IRLR 491.

[192] See para 4.9 above.

[193] (1981) Law Com No 110.

[194] As distinguished from the separate question whether, where it is established (or not disputed by the defendant) that the information is not generally known, that it derived economic value from that fact.

[195] The nature of this burden is more fully considered at para 6.1 below.

4.35 As to the requirement that the economic value of the information must arise from the fact that it is not generally known, we agree with the suggestion of the authors of the Alberta report that

> The appropriate benchmark is simply that the information must not be devoid of value. It should have *some* economic value to somebody which derives from the fact that that information is not generally known. Otherwise, why protect it?[196]

**We provisionally propose that it should be an element of the definition of a trade secret that the information should have some economic value which derives from the fact that it is not generally known.**

### *Specific items*

4.36 Since we propose that the expression "trade secrets" should be defined "functionally",[197] it might be thought unnecessary to include a reference to any of the various forms that such secrets may take. On the other hand judges and practitioners might well find it helpful if the definition referred, without being restricted, to some of those forms, especially (or, on one view, only)[198] where a doubt might otherwise arise.[199]

4.37 The definition in the Alberta report refers, non-exhaustively, to

> information including but not limited to a formula, pattern, compilation, program, method, technique or process, or information contained or embodied in a product, device or mechanism … .[200]

4.38 We incline to the view that, subject to two possible qualifications, the better course would be the adoption of a general "functional" definition, without elaboration in the form of a reference to specific items. The first qualification relates to a compilation of information. As we explained above,[201] there are compilations in

[196] Para 10.21 (emphasis in original). The definition would extend to "negative information", such as the results of research that has revealed that certain approaches are not commercially feasible: see para 4.17 above.

[197] We agree with the view expressed in the Alberta report, para 10.11:

> It is probably impossible to arrive at an intrinsic definition of a trade secret. The potential subject-matter is limitless. We have emphasized the importance of avoiding technology bound definitions. The alternative is to move to a more functional description of the requisite elements of a trade secret. This is the course which US legislators have taken, and is the approach we recommend.

[198] Cf, in the context of drafting legislation, Lord Thring's advice in *Practical Legislation* (1902) p 96: "The proper use of definitions is to include or exclude something with respect to the inclusion or exclusion of which there is a doubt without such a definition … ."

[199] Cf the apparently exhaustive definition in Lord Boyle's Bill (para 2.2 above) and the definition proposed by the Younger Committee (para 2.6 above).

[200] See para 4.11 above. This list is similar to that in the definition of trade secrets in the United States Uniform Trade Secrets Act set out at para 4.16 above (except that the definition in that Act does not refer to "information contained or embodied in a product, device or mechanism").

[201] See paras 4.9 and 4.31 – 4.33 above.

which no individual item meets the requirements of the definition. We suggest that it would be desirable, therefore, to obviate a possible argument that a compilation consisting of such items falls outside the definition.

4.39 The second qualification concerns information embodied in a tangible object – as the definition proposed in the Alberta report puts it, "information contained or embodied in a product, device or mechanism".[202] A specific reference to such forms of information might be helpful to judges and legal practitioners. It should be borne in mind, however, that information obtained solely by "reverse engineering" – that is, taking the product apart in order to work out how it is made – is expressly excluded from the proposed offence.[203]

4.40 **We invite views on the extent, if any, to which the definition of a trade secret should include a reference to specific forms of information.**

[202] The report instances, at para 10.20, a secret computer program "in firmware form (ie burned into a silicon chip)".

[203] See paras 6.13 – 6.15 below.

# PART V
# THE ELEMENTS OF THE PROPOSED OFFENCE

### USE OR DISCLOSURE

5.1 The law of breach of confidence is concerned not with the acquisition of information, but with its subsequent "use or disclosure". As to that expression, we explained in our Breach of Confidence report, in terms that (with adaptation) are equally applicable to the proposed offence:

> It is one of the characteristics of information that it is capable of dissemination in a variety of ways. In the context of the law of breach of confidence, it is, therefore, not possible to provide a definition of the different kinds of misuse of information impressed with an obligation of confidence which should attract liability … . It seems necessary to us to put the duty [arising under an obligation of confidence] in terms of "use or disclosure" because of the nature of information. In some cases the breach will be constituted by wrongful disclosure, as where information subject to the obligation is passed to a trade rival or published in a paper. The duty should, however, be broader and prevent, for example, a company which has received information in confidence during the course of licensing negotiations from turning that information to its own use, though without disclosing it further.[204]

5.2 We did not recommend that the mere acquisition of information, even by reprehensible means, should be capable of founding an action for breach of confidence. That approach, we explained, would be appropriate only in the different context of a law of privacy, which was not our concern.[205]

5.3 We have started from the principle that a new offence should, similarly, be restricted to cases in which the defendant uses[206] or discloses the trade secret. On this view the mere *acquisition* of a secret, even by reprehensible means, would not without more be caught by the offence that we provisionally propose.[207] **We provisionally propose that the new offence should be committed by a**

[204] (1981) Law Com No 110, para 6.56 (footnotes omitted).

[205] *Ibid*, at para 2.6.

[206] The House of Lords recently held (by a 3:2 majority) that, for the purpose of the Data Protection Act 1984 (by s 5 of which the unauthorised use of certain personal information stored on a computer is an offence), a person does not, in the ordinary and natural meaning of the word, "use" information merely by causing it to be displayed on a computer screen: *Brown (Gregory)* [1996] AC 543. See para 1.19 above. It would seem, however, that a person may "use" information by negative conduct, eg, by refraining from research into a possible method of manufacturing a product that previous secret research conducted by a competitor has shown to be commercially impracticable: see para 4.17 above. As Lord Hoffmann (one of the majority) pointed out in *Brown*, at p 562H: "A person who refrains from entering a field with a notice saying 'Beware of the bull' is using the information obtained from the notice."

[207] This approach does not address the problem of the acquisition of information by means of industrial espionage, which we consider separately in Part VII below.

**person who uses or discloses a trade secret belonging to another without that other's consent.**

### TO WHOM DOES A TRADE SECRET BELONG?

5.4 **We provisionally propose that a trade secret should be regarded as belonging to anyone entitled to the benefit of it.** This approach has what we regard as the merit of recognising that concurrent and different interests may be held in a trade secret by different individuals. It would include, for instance, the interest of a licensee of the trade secret. The effect is that only the consent of *all* the secret's "owners"[208] to its use or disclosure would negative liability.

### CONSENT OBTAINED BY DECEPTION

5.5 Where the owner's consent to the use or disclosure of the trade secret is obtained by deception, the defendant should be, in our view, in no better position than if the owner had not given consent.

5.6 The definition in section 15(4) of the Theft Act 1968 seems appropriate to the present purpose. The subsection, which applies to a range of deception offences under that Act (as amended by the Theft (Amendment) Act 1996) and the Theft Act 1978, provides that deception means

> any deception (whether deliberate or reckless) by words or conduct as to fact or law, including a deception as to the present intentions of the person using the deception or any other person.

5.7 There is a substantial body of case law on the meaning of deception, which would therefore apply for the purposes of the proposed offence. **We provisionally propose that consent to the use or disclosure of a trade secret should not negative liability for the offence if it is obtained by deception.**

### THE MENTAL ELEMENT

5.8 Even without express provision the courts normally require a mental element in respect of the circumstances of the offence. Our intention is that this principle should apply to the offence we propose; so the prosecution would have to establish that the accused knew that the information in question was a trade secret.[209] More precisely stated: it would be a requirement of the offence that the defendant knows[210] of facts whose existence has the effect in law of rendering the relevant information a trade secret,[211] and one which belongs to another. The requirement

[208] We sometimes use the term "owners" to refer to those entitled to the benefit of the trade secret. We do so entirely for convenience: the use of this term does not imply that we are treating information of this kind as property in the strict sense. Cf paras 3.13 – 3.26 above.

[209] Where the defendant does not contend that the information was generally known, so that there is no issue as to that point (see paras 4.29 – 4.34 above), no question of the mental element will arise in *that* respect.

[210] We use the word "know" in the sense used in the Draft Criminal Code (1989) Law Com No 177. Clause 18(a) (p 51) provides that a person acts "knowingly" with respect to a circumstance "not only when he is aware that it exists or will exist, but also when he avoids taking steps that might confirm his belief that it exists or will exist".

[211] The Alberta report proposes a similar approach. Its authors explain at para 13.29:

of a mental element would also negative liability where the defendant mistakenly believes that the owner[212] of the trade secret consents to the use or disclosure in question.[213] **We provisionally propose that it should be an element of the new offence that the defendant**

**(1) knows that the information in question is a trade secret belonging to another, and**

**(2) is aware that that other does not, or may not, consent to the use or disclosure in question.**

5.9 There may well be cases, however, in which the defendant knows that the owner of the trade secret has not in fact consented to the use or disclosure in question but acts in the belief that the owner would have consented had he or she known of the circumstances. Bearing in mind that we intend criminal liability to attach only to cases where the defendant behaves very badly, we consider that a defendant who acts in this state of mind ought not to be liable.[214] **We provisionally propose that a person should not commit an offence by using or disclosing a trade secret in the belief that every person to whom the secret belongs would consent to that use or disclosure if he or she knew of it and the circumstances of it.**

5.10 Some offences require that the defendant must act with some ulterior intention. In theft, for example, the defendant must act with the intention of permanently depriving the owner of the property.[215] The offence that we propose, however, would require no *ulterior* intent. In other words, assuming the presence of the other mental and physical elements of the offence, the defendant would be liable without more if he or she intentionally[216] uses or discloses the trade secret. It would be

> While this … may seem unduly biased in favour of trade secret "thieves", we are satisfied that in most cases but one it is consistent with the balancing of interests involved in extending legal protection to trade secrets. Punishing an individual who discloses or uses information that is a trade secret but who does not know that it is a trade secret would create a substantial, and in our opinion, unjustifiable barrier to the free flow of information.

The exceptional case referred to in this passage is immaterial, since it has no counterpart in our provisional proposals.

[212] In this context the term "owner" signifies every owner of the secret of whose existence the defendant is aware.

[213] Or is correct in thinking that the owner consents but is not aware that that consent was obtained by deception: cf paras 5.5 – 5.7 above.

[214] Section 2(1)(b) of the Theft Act 1968 provides in relation to theft that, subject to an immaterial exception, a person does not act dishonestly "if he appropriates … property in the belief that he would have the [owner's] consent if the [owner] knew of the appropriation and the circumstances of it". The effect of this provision is that, where it applies, the defendant is not guilty of theft. The Act expressly negatives liability in these circumstances for the offences of removing articles from places open to the public (s 11(3)) and taking a conveyance without authority (s 12(6)), neither of which requires dishonesty.

[215] Theft Act 1968, s 1.

[216] We recommended in Breach of Confidence (1981) Law Com No 110 that negligent use or disclosure should suffice to found an action for breach of confidence: see para 6.57 and draft Bill p 202, cl 8(1)(b). However, we do not consider that an unintended use or disclosure, even if negligent, should suffice for criminal liability.

immaterial that the defendant does not intend to cause harm to the owner or owners, or does not even foresee the risk of such harm.

### MODE OF TRIAL

5.11 In some cases, trials for the proposed offence may involve difficult issues, such as whether information amounted to no more than the enhancement of the personal experience of an employee;[217] or whether the defendant's disclosure of a trade secret was justified in the public interest.[218] In our view questions of this kind are not well suited to determination at a summary trial, and **we provisionally propose that the new offence should be triable only on indictment.**[219]

### PENALTIES

5.12 If, in the light of consultation on this paper, we make a recommendation in our final report for the introduction of an offence, and if that recommendation is implemented, others will undoubtedly give consideration to the maximum sentence that it should attract. We see no purpose in selecting a figure which may or may not prove acceptable to Parliament. We therefore express no view on the matter.

### CONSENT TO PROSECUTION

5.13 The discretion of the Crown Prosecution Service (the "CPS") whether or not to prosecute is governed by the principles set out in the Code for Crown Prosecutors.[220] The Code sets out in detail the matters which have to be considered before a prosecution can be brought or continued. They include both an evidential test[221] and the public interest considerations[222] that the CPS should take into account in making a decision.

5.14 By contrast, in the absence of express provision relating to a particular offence, there is nothing to prevent the bringing of a private prosecution for that offence, without regard to the considerations set out in the Code for Crown Prosecutors.[223] The right to bring a private prosecution in general is, we appreciate, generally regarded as of constitutional significance,[224] and in our recent Consultation Paper

[217] See para 6.6 below.

[218] See para 6.54 below.

[219] In reaching this provisional conclusion, we have also borne in mind the prosecution's duty to disclose materials to the defence. A dispute about the production of such material falls to be resolved by the court. The proposed offence is perhaps especially likely to involve sensitive information, and so produce difficult problems in this area.

[220] The Code is issued pursuant to s 10 of the Prosecution of Offences Act 1985 and is included in the Director's Annual Report to the Attorney-General, which is laid before Parliament and published: s 9. The Code is, therefore, a public declaration of the principles which the CPS applies in the exercise of its functions.

[221] See the Code for Crown Prosecutors, paras 5.1 – 5.4, which refer to a "realistic prospect of conviction".

[222] *Ibid*, at paras 6.1 – 6.9.

[223] Prosecution of Offences Act 1985, s 6(1).

[224] See, eg, *per* Lord Diplock in *Gouriet v Union of Post Office Workers* [1978] AC 435, 498A–B:

No 149, on consents to prosecution, we expressed support for this view.[225] We are conscious, however, that the existence of the offence that we propose might be used to improve the commercial bargaining power of a party to a civil dispute who is alleging misuse of a trade secret. As Hoffmann J has pointed out:

> There is a strong incentive for employers to launch a pre-emptive strike to crush the unhatched competition in the egg by causing severe strains on the financial and management resources of the defendants or even a withdrawal of their financial support. … . Some employers seem to regard competition from former employees as presumptive evidence of dishonesty.[226]

5.15 In Consultation Paper No 149 we expressed our concern that, as regards a certain category of offences, namely those which might be the subject of either criminal or civil proceedings, there was a risk that criminal proceedings might be against the public interest if instituted in circumstances where civil proceedings were more appropriate. For this reason, we provisionally proposed that the prosecution of such offences should be subject to the prior consent of the Director of Public Prosecutions.[227] We believe that the proposed offence might fall into this category of offences. We are concerned that, since the costs of bringing a private prosecution are likely to be borne (at least in part) by the state,[228] a large organisation may in practice be able to avoid some of the costs of bringing civil proceedings for an injunction by means of a private prosecution. In our view, this is not a use of public funds that should be permitted without restriction. Moreover, the threat of a private prosecution might be made to improve the negotiating position of the party who claims to be wronged; and we would not wish the

> [T]he need for prosecutions to be undertaken (and paid for) by private individuals has largely disappeared; but it still exists and is a useful constitutional safeguard against capricious, corrupt or biased failure or refusal of those authorities to prosecute offenders against the criminal law.

[225] Criminal Law: Consents to Prosecution (1997) Consultation Paper No 149, para 6.4.

[226] *Lock plc v Beswick* [1989] 1 WLR 1268, 1280–1281. The courts have indicated their displeasure at the use of "Anton Piller" orders in such cases. In *Anton Piller v Manufacturing Processes* [1976] Ch 55 the Court of Appeal approved a procedure that is of great practical importance to some owners of intellectual property rights. The plaintiff applies to the High Court in camera for an order that the defendant permit the plaintiff (with his or her solicitor) to inspect the defendant's premises and to seize, copy or photograph material relevant to the alleged infringement. The defendant may be required (among other things) to deliver up infringing goods and even to give information, eg, about the source of supply or the destination of stock passing through the defendant's hands. Anton Piller orders, which are in daily use, "have been a response to growing concern over the current volume of sound recording, video and other copyright piracy and the counterfeiting of popular trade marks, but they are equally available, for instance, in breach of confidence cases": W R Cornish, *Intellectual Property* (3rd ed 1996) para 2–48 (footnote omitted).

[227] Consultation Paper No 149, paras 6.47 – 6.51.

[228] The court may, on the application of a private prosecutor, make an order for payment of the prosecution's costs out of central funds (whether or not the defendant is convicted): Prosecution of Offences Act 1985, s 17(1), (2). A Practice Direction [1991] 1 WLR 498, para 3.1, provides:

> An order should be made save where there is good reason for not doing so, for example, where proceedings have been instituted or continued without good cause.

offence to be used to intimidate potential defendants. We have therefore provisionally concluded that the right to bring a private prosecution for the proposed offence should be restricted.[229] **We provisionally propose that prosecutions for the new offence should be brought only by or with the consent of the Director of Public Prosecutions.**[230]

### THREATS TO PROSECUTE

5.16 We now turn to consider whether a remedy should be granted to those to whom groundless threats of prosecution have been made. Normally, it is not actionable to threaten proceedings, though it is an actionable wrong to maliciously prosecute a claim[231] or commit the tort of intimidation.[232] By way of exception, however, it is actionable to make groundless threats of civil proceedings for infringement of patents,[233] of registered design law,[234] and design rights law[235] (though not of copyright). The provisions in respect of design rights have been criticised on the basis that such provisions originated in patent law, where proceedings are notoriously complex and expensive: there is no reason to expect design rights proceedings to be particularly complex or expensive, or for the threat of them to be more effective as blackmail than any other threat.[236] Professor Cornish describes

[229] The CPS has the power to take over the conduct of a private prosecution and discontinue it: Prosecution of Offences Act 1985, ss 6(2) and 23. It will not necessarily do so, however, even where it has decided not to institute proceedings itself; and even the initiation of a private prosecution would amount to what we consider to be undesirable pressure.

[230] There are a number of offences for which a prosecution cannot be brought without the consent of the Director of Public Prosecutions. They include, significantly, offences under the Data Protection Act 1984 (see s 19). Other instances are: (a) offences of theft or criminal damage when the property in question belongs to the accused's spouse (Theft Act 1968, s 30(4)); (b) offences of assisting offenders and wasting police time (Criminal Law Act 1967, ss 4(4) and 5(3)); (c) homosexual offences where either party is under the age of 21 (Sexual Offences Act 1967, s 8); (d) incest (Sexual Offences Act 1956, Sched 2); (e) aiding and abetting suicide (Suicide Act 1961, s 2); (f) riot (Public Order Act 1986, s 7); (g) offences under the Prevention of Terrorism Act (Temporary Provisions) Act 1989, ss 13A, 16A and 16B (of which the most serious is being in possession of an article for terrorist purposes). Although the unifying principle underlying the consent provision in each of these offences is not obvious (see Consultation Paper No 149, paras 5.32 – 5.42), it has been suggested that "[t]he linking factor between the … disparate offences may be that, in each instance, although sometimes for different reasons, the weighing of the discretionary factors relevant to the decision to prosecute is likely to be a particularly sensitive and difficult exercise, thus making it desirable for the police or the Crown Prosecution Service to obtain prior approval for a prosecution": *Blackstone's Criminal Practice* (1997 ed) para D1.83.

[231] For the ingredients of malicious prosecution see *Clerk & Lindsell on Torts* (17th ed 1995) para 15–05.

[232] For the ingredients of the tort of intimidation see *Clerk & Lindsell on Torts* (17th ed 1995) para 23–38.

[233] Patents Act 1977, s 70.

[234] Registered Designs Act 1949, s 26.

[235] Copyright, Designs and Patents Act 1988, s 253.

[236] Laddie, Prescott and Vitoria, *The Modern Law of Copyright and Designs* (2nd ed 1995) vol 1, para 43.41.

the present position as "an odd patchwork still leaving out copyright, confidential information and those marks and names protected only at common law".[237]

5.17 Our starting point is that it has not been found necessary to have a special remedy for groundless threats of criminal prosecution in any other branch of the law. We provisionally believe that it is generally accepted that the offence of blackmail and, in certain limited circumstances, the torts of defamation and intimidation provide suitable redress for anybody who receives a groundless threat of prosecution. We are not aware of complaints being made of exceptional or groundless threats of prosecutions for the copyright, trademark or other intellectual property offences. At present, we can see no justification for giving redress against those who make unjustified threats to prosecute. However, **we invite views on**

**(1) whether there should be a remedy for unjustified threats to prosecute for the proposed new offence;**

**(2) if so, whether the remedy should be civil or criminal;**

**(3) what conditions should be satisfied before proceedings can be brought; and**

**(4) what defences should be available.**

### PROSPECTIVE EFFECT

5.18 We envisage that, in accordance with the almost invariable practice in criminal matters,[238] the offence would not apply to anything done before the legislation that implemented it came into force. **We provisionally propose that the offence should have prospective effect only.**

[237] W R Cornish, *Intellectual Property* (3rd ed 1996) para 2.87.

[238] Article 7(1) of the European Convention on Human Rights provides that no-one should be held guilty of an offence for any act or omission which did not constitute an offence when it was committed.

# PART VI
# EXCLUSIONS

6.1 We turn now to consider categories of information which, in our view, should not fall within the ambit of the offence we propose. In every case, the defendant would have what is sometimes described as an "evidential" burden – that is, the prosecution would need to prove that the exclusion was inapplicable only where there was evidence that might lead the jury to conclude that there was a reasonable possibility that the exclusion applied.[239] If, however, such evidence is adduced, it would then be for the prosecution to establish that the exclusion did not apply. It should be borne in mind that, in accordance with the general principles of criminal law governing offences that require mens rea, liability is negatived where the defendant mistakenly *believes* that facts exist which, if his or her belief were true, would constitute an exclusion. In this respect also the defendant would have an evidential burden.

6.2 We should emphasise that this principle applies only to questions of fact, and not to matters of law, which are for the judge alone to determine and involve no burden of proof. It would be a question of law, for example, whether (on the basis of the circumstances as the defendant correctly or mistakenly thought them to be) the disclosure of the trade secret was justified on the ground of public interest.[240]

### SUMMARY OF THE EXCLUSIONS THAT WE PROVISIONALLY PROPOSE

6.3 Readers may find it convenient to have the following summary of the proposed exclusions, each of which we consider in turn in this part of the paper.

(1) Information which, under the law of confidence, constitutes the enhancement of an employee's (or independent contractor's) personal knowledge, skill or experience.[241]

(2) Information acquired by independent development.[242]

(3) Information acquired solely by "reverse engineering".[243]

(4) Information which the defendant acquired innocently – that is, without knowing that it was a trade secret belonging to a person who did not consent to the defendant's acquisition of it, and not being aware (if such was the case) that its previous acquisition had involved the commission of

[239] As we pointed out at para 4.34 above, we intend this principle to apply not only to the exclusions considered in this part of the paper but also to the question whether the information in question was not generally known (an element of the definition of "trade secret").

[240] See paras 6.41 – 6.55 below.

[241] See paras 6.4 – 6.6 below.

[242] See para 6.12 below.

[243] See paras 6.13 – 6.15 below.

an indictable offence or of the (summary) offence, contrary to section 1 of the Computer Misuse Act 1990, of "hacking" into a computer.[244]

(5) Information which it was in the public interest to use or disclose. We canvass the following four possible options for the form that this exclusion might take. (Under every option other than the first, the issue would be a matter of law for the judge to determine.)

(a) The question would be left to the jury.

(b) Public interest would simply be defined as having the same meaning as in the law of confidence.

(c) Public interest would be defined as in the draft Bill annexed to our Breach of Confidence report, with appropriate adaptations.

(d) Specific purposes would be listed which would justify a use or disclosure of the trade secret, but would be combined with a general provision as under option (b).[245]

(6) Information used or disclosed in accordance with a statutory obligation or power.[246]

(7) Information disclosed pursuant to a court order, or otherwise for the purpose of legal proceedings.[247]

(8) The use or disclosure, in the lawful exercise of an official function in regard to national security or the prevention, investigation or prosecution of crime, of information obtained in the lawful exercise of any such function.[248]

## EMPLOYEES

### Information constituting the enhancement of an employee's personal knowledge, skill or experience

6.4 In the civil law, by a long-established principle of public policy, a former employee is free to utilise the general skill and knowledge acquired during his or her employment.[249] In a number of cases information such as details of office

[244] See paras 6.19 – 6.28 below.

[245] See paras 6.29 – 6.55 below.

[246] See para 6.56 below.

[247] See para 6.57 below.

[248] See paras 6.58 – 6.59 below.

[249] Eg in *Mason v Provident Clothing and Supply Co Ltd* [1913] AC 724, 740–741, Lord Shaw of Dunfermline contrasted the divulging of trade secrets with the case of an employee who in that capacity acquired mental or manual skills; the former related to knowledge which was "as real and objective as the possession of material goods", while the latter concerned the subjective equipment of the workman which becomes part of himself and was to be used "for his own maintenance and advancement". Similarly, in *Herbert Morris Ltd v Saxelby* [1916] 1 AC 688 the House of Lords gave authoritative expression to the principle that a person in a particular employment cannot validly covenant not to use, after leaving that employment, "the general skill and knowledge which an employee of any ability must necessarily obtain as opposed to knowledge of any matter and skill in any process in which

organisation, general organisation and general management of the business of the employer has been held to be capable of falling into this category.[250] The exclusion applies not only to the exploitation of the information for the employee's own benefit, should the employee choose to go into business on his or her own account, but also to the employee's use of it for other employers.[251]

6.5 We regard it as virtually beyond question that this category of information should be excluded from the definition of trade secret for the purpose of the offence that we propose. Clause 7 of the draft Bill annexed to our Breach of Confidence report[252] provides:

> Nothing in the preceding provisions of this Act has the effect of imposing an obligation of confidence on any individual with respect to any information which –
>
> (a) is acquired by him in the course of his work (whether under a contract of employment or as an independent contractor or otherwise),[253] and
>
> (b) is of such a nature that the acquisition of it by him amounts to no more than an enhancement of the personal knowledge, skill or experience used by him in the exercise of his calling.

6.6 It is often very difficult in practice to determine the dividing line between trade secrets on the one hand and general knowledge and skill on the other, on which there is a considerable body of authority.[254] In our view, this difficulty is

[his former employer] could be said to have any property at all": at p 711, *per* Lord Parker of Waddington.

[250] Eg, *Herbert Morris Ltd v Saxelby* [1916] 1 AC 688; *Commercial Plastics Ltd v Vincent* [1965] 1 QB 623; *Amway Corporation v Eurway International Ltd* [1974] RPC 82; *Ixora Trading Incorporated v Jones* [1990] FSR 251; *Berkeley Administration Inc v McClelland* [1990] FSR 505.

[251] In *Faccenda Chicken Ltd v Fowler* [1987] Ch 117, 138H–139A, the Court of Appeal left open "for further examination on some other occasion the question whether additional protection should be afforded to an employer where the former employee is not seeking to earn his living by making use of his body of skill, but is merely *selling* to a third party information which he acquired in confidence in the course of his former employment". This is a novel question, involving policy issues that do not hitherto appear to have arisen for judicial consideration. Mehigan and Griffiths, *Restraint of Trade and Business Secrets: Law and Practice* (1986) p 72, suggests that the distinction may be no more than a reflection of a feeling that previous employment cases have been too generous to employees.

[252] (1981) Law Com No 110.

[253] We explained in our report at para 4.35 that this principle is relevant also to the personal skill, knowledge or experience acquired by an independent contractor in the course of carrying out work for another; or to such information acquired by a partner. We instanced a consultant on business management who, during the course of a lengthy assignment on behalf of his client, added to his personal knowledge etc in the same way as an actual employee of the client.

[254] "It is often not too difficult to distinguish between genuine trade secrets of the employer, such as secret processes of manufacture, and general skill and knowledge acquired by the employee in the course of his employment, such as knowledge of general scientific principles and technical principles and methods. However, often between these two extremes there is an intermediate area of information, where it is extremely difficult to differentiate between that which is the employer's confidential information and that which

unavoidable.[255] We envisage, moreover, that prosecutions are unlikely to be brought in cases where it appears that there is a real issue in this respect.[256] **We provisionally propose that the new offence should not extend to the use or disclosure of information which, under the law of confidence, constitutes the enhancement of an employee's (or independent contractor's) personal knowledge, skill or experience.**

### Employees in general

6.7 We have considered whether employees who acquire trade secrets in the course of their employment should be excluded from the offence that we propose.[257] Such an exclusion would apply only to information that the employee acquires *properly*. It would not extend, for example, to an industrial spy who takes up employment with a company, having it in mind to amass information which the spy may not receive in the course of his or her duties, but to which the employment affords access.

6.8 A powerful argument in favour of this approach is that the employment relationship is one which, in the absence of something wrongful in the employee's *acquisition* of the secret, should be left to civil law. In the words of the Alberta report:

> The employer and employee can regulate their relationship by contract, and the contract can be drafted in terms appropriate to the particular fact situation. The thousands of cases decided over the years illustrate how subtle is the distinction between trade secrets and information forming part of the general stock of knowledge. According to this view, it would be unduly harsh to subject the employee who misjudges the character of information to criminal penalties when what is frequently involved is a matter of judgment.[258]

the employee may properly regard as his own skill or knowledge. An example of this is the identity of the employer's customers or even manufacturing knowledge which, although particular to the employer's process, has become part and parcel of the employee's general knowledge": K Brearley and S Bloch, *Employment Covenants and Confidential Information* (1993) para 5.7.

[255] In *Printers and Finishers Ltd v Holloway* [1965] 1 WLR 1, 6, Cross J resorted to the concept of the judgment of the ordinary or average man to determine the issue:

> I do not think that any man of average intelligence and honesty would think that there was anything improper in [the first defendant] putting his memory of particular features of his late employer's plant at the disposal of his new employer. The law will defeat its own object if it seeks to enforce in this field standards which would be rejected by the ordinary man.

[256] In the context of the proposed offence a "real issue" may arise from a contention by the defendant as to his or her *belief* at the material time: see para 6.1 above.

[257] In Maryland, Minnesota and Wisconsin it is a defence to a charge of misappropriating a trade secret that it was "rightfully known" to the accused. The defence is not confined to employees.

[258] Alberta report, para 13.46. The authors of the report none the less conclude, though "not without some hesitancy" (para 13.47), that employees should not automatically be excluded from the offences proposed.

6.9 A related, practical argument in favour of excluding employees is that this approach would obviate the need for the court to distinguish between information that constitutes the enhancement of an employee's personal knowledge, skill or experience and other information acquired by the employee in his or her work.[259] In some cases this may involve complex and difficult issues both of law and of fact.

6.10 On the other hand, we see no ground of principle on which employees should *automatically* fall outside the scope of the proposed offence. In many cases the improper use or disclosure by an employee (or former employee) who has been entrusted with a trade secret would amount to precisely the mischief at which the proposed offence is aimed. We would instance the case of the managing director's secretary who, in the course of employment, quite properly acquires knowledge of the company's trade secrets. We see no reason why, if the secretary betrays the employer's trust by selling those secrets to one of the company's competitors, he or she should escape liability. Again, under a "blanket" exclusion, an employee could with impunity sell the employer's trade secrets after amassing them for that very purpose. Nor is it inconceivable that an industrial spy might obtain employment with an organisation in a capacity in which he or she would *properly* acquire trade secrets. In circumstances like these the question whether the information formed part of the employee's personal skill or knowledge does not call for consideration.

6.11 **We provisionally conclude that employees should not be automatically excluded from the offence.**

### ACQUISITION BY INDEPENDENT DEVELOPMENT

6.12 Where information, though similar to that comprising a person's trade secret, is acquired by independent development, there is nothing reprehensible in its subsequent use or disclosure. **We provisionally propose that the new offence should not extend to the use or disclosure of information acquired by independent development.**

### REVERSE ENGINEERING

6.13 In the law of confidence, this expression signifies the process by which information relating to the creation of a marketed product is obtained by analysing the product.

> [The process] is called reverse engineering, because engineering a new product usually involves working from an idea to a product, whereas reverse engineering involves acquiring a product and working back from this to the idea and the information as to how it was made.[260]

[259] See paras 6.4 – 6.6 above.

[260] Allison Coleman, *The Legal Protection of Trade Secrets* (1992) p 40, n 26. There is a possible exception, of uncertain scope, where there is a "black box" agreement, as in *K S Paul (Printing Machinery) Ltd v Southern Instruments (Communications) Ltd* [1964] RPC 118. The plaintiff supplied to one of the defendants a telephone answering machine under a contract of hire which specified that the defendant was not to move it from the position where it was installed or otherwise interfere with it. In breach of this term, one defendant allowed another to remove the machine, take it apart and examine it. The court granted an

6.14 It is well established that, by contrast with patent law, this method of acquiring information is legitimate. Were this not the case, it would perhaps be arguable that the acquisition of what was hitherto a trade secret by subjecting a product to detailed investigation should not necessarily fall outside the scope of the criminal law. In our view, however, it would be unacceptable to render criminal a practice that does not found a civil action under the present law, and would not do so even if the recommendations made in our Breach of Confidence report were implemented.

6.15 **We provisionally propose that the new offence should not extend to the use or disclosure of information acquired solely by reverse engineering.**

### INFORMATION AVAILABLE FROM ANOTHER SOURCE

6.16 On one view, the fact that the information was available from another source should be immaterial to liability. This approach was adopted in the Alberta report:

> If information in fact exists elsewhere, a sufficient degree of availability of that information would mean that it is no longer a secret. Thus, there is the possibility of an "open" secret: information lying undetected in publicly available documents. Nevertheless, our offences seek to proscribe socially unacceptable conduct. It is anomalous to permit an accused to escape sanction on the basis that, while his or her conduct was egregious, and fell within the definition of the offence, it need not have been so since, had the accused wished, he or she might have acquired the trade secret from another source.[261]

6.17 We see the force of this reasoning; and we do not favour the exclusion of liability merely because the defendant could have obtained the information from some other source. However, as we have explained above in the context of the definition of a trade secret,[262] we take a different view where the information is *publicly* available (that is to say, where it lies in the public domain): it would, we believe, be wrong in principle for such information to attract protection as a trade *secret*. Nor would we regard it as appropriate in this context to create a criminal sanction for conduct which is not actionable in civil law, solely on the ground that it is morally reprehensible.

interlocutory injunction restraining the defendants from using or disclosing confidential information obtained from the unauthorised inspection. It is not clear, however, whether a similar provision in a contract of *sale* would be enforceable. In *Vernon v Universal Pulp Containers Ltd* [1980] FSR 179, on an application for an interlocutory injunction to restrain, among other things, the use of confidential information contained in machines sold to the defendants, Megarry V-C said, obiter (at p 190):

> [A] purchaser of a machine of this sort is entitled, I think, to expect to receive from the vendor some degree of information and advice about the operation without being told that it is confidential.

[261] Alberta report, para 13.41. The authors of the report take as a starting-point the fact that it is a defence to a charge of misappropriation in Winconsin, Maryland and Minnesota for the accused to establish that the trade secret was either rightfully known to him or her or was available from another source: para 13.40.

[262] Paras 4.29 – 4.34 above.

6.18 **We provisionally conclude that, where information otherwise falls within the definition of a trade secret, the fact that it was available from another source at the material time should not exclude liability.**

### INNOCENT THIRD PARTIES

#### The general principle

6.19 We turn now to consider the following position. A trade secret is disclosed without the consent of the owner, and thereby (or subsequently) is acquired by a third party ("T") who does not know that it is a trade secret (or that its previous acquisition involved criminality).[263] T subsequently learns the truth but proceeds nonetheless to use or disclose it. We propose that T's conduct should be excluded from the offence.[264] In this respect we share the view expressed by the authors of the Alberta report:

> [T]he rationales for the intervention of the criminal law are not applicable to the situation of innocent third parties. We have suggested that the criminal law should be reserved for conduct that is reprehensible and for which other means of social control are inadequate. Use of a trade secret by an innocent third party acquirer does not appear to be sufficiently reprehensible to warrant criminal sanction. Indeed in many instances the use seems to be only rational commercial behaviour. It would be illogical for example to require a third party who incorporates a trade secret in a factory to stop using the factory solely because he or she later discovers the criminal history of the trade secret.[265]

6.20 The principle underlying this exclusion is analogous to that of section 3(2) of the Theft Act 1968, which provides:

> Where property … is … transferred for value to a person acting in good faith, no later assumption by him of rights which he believed himself to be acquiring shall, by reason of any defect in the transferor's title, amount to theft of the property.

6.21 The Criminal Law Revision Committee, upon whose proposals the 1968 Act was based, explained:

> A person may buy something in good faith, but may find out afterwards that the seller had no title to it, perhaps because the seller or somebody else stole it. If the buyer nevertheless keeps the thing or otherwise deals with it as owner, he could, on the principles stated above, be guilty of theft. It is arguable that this would be right: but on the whole it seems to us that, whatever view is taken of the buyer's

[263] See further, paras 6.26 – 6.27 below.

[264] We envisage that T would not be liable even where another person subsequently commits the proposed offence. If, eg, T in turn discloses the information to X (who is aware of the true position), with the intention that X should use it, and X does use it, T would not be liable as a secondary party to the offence committed by X, or for conspiring with or inciting X to use the information.

[265] At para 13.51.

> moral duty, the law would be too strict if it made him guilty of theft. Clause 3(2) accordingly ensures that later assumption of ownership in such circumstances will not amount to theft.[266]

6.22 This provision does not apply to the offence of handling stolen goods. The extent to which that offence applies where the defendant did not become aware that the goods were stolen until after he or she had acquired them is not based on any clear principle.[267]

### A requirement that the third party must give value?

6.23 The question arises whether, by analogy with theft, the exclusion for innocent third parties should apply only where T gives value for the information.[268] It might be argued in support of this view that a person who acquires information without paying for it has no valid ground of complaint if, after discovering the true position, he or she is prevented by the criminal law from harming the owner of the information by using or disclosing it. Such a person (the argument would run) has lost nothing. In some cases this may be so. But there may be circumstances, such

[266] Eighth Report: Theft and Related Offences (1966) Cmnd 2977, para 37.

[267] See, eg, Edward Griew, *The Theft Acts* (7th ed 1995) para 15-35:

> It seems that D, although innocent of handling by receiving when he buys the goods, may be guilty of handling by a later dealing with them for the benefit of E, a sub-purchaser (as by undertaking retention for E or assisting in E's sale to F). And if E knows that the goods are stolen when he buys from D, D may be guilty as a secondary party to the handling E commits by receiving them. It is doubtful whether these results were intended.

But a person who buys stolen goods without knowing that they are stolen, and then, having learnt that they are stolen, sells them, does not undertake their "realisation … for the benefit of" the purchaser: *Bloxham* [1983] 1 AC 109.

[268] Under the law of confidence, a person who acquires information without actual (or, it would seem, constructive) notice of its confidential character is free to use or disclose it before he or she has such notice: see, eg, *Malone v Metropolitan Police Commissioner* [1979] Ch 344, 361B, *per* Megarry V-C. However, at least where the defendant did not give value for the information, he or she becomes subject to the obligation from the time that he or she receives notice of its confidential character: *Prince Albert v Strange* (1849) 1 Mac & G 25, 41 ER 1171; *Morison v Moat* (1851) 9 Hare 241, 68 ER 492; *Duchess of Argyll v Duke of Argyll* [1967] Ch 302. It is unclear whether the latter principle applies also where he or she gives value for the information. In *Morison v Moat* (1851) 9 Hare 241, 263, 68 ER 492, 501–502, Turner V-C suggested, obiter, that there was an exception where value was given; and there are dicta by Cross J to the like effect in *Printers & Finishers Ltd v Holloway (No 2)* [1965] RPC 239. On the other hand, there is authority to the contrary, including *Lamb v Evans* [1892] 3 Ch 462; *Richards v Dobell* [1912] Macg Cop Cas 51 (1911–16); *Stevenson Jordan & Harrison Ltd v MacDonald & Evans* (1951) 68 RPC 190. In the last-mentioned case Lloyd-Jacob J refused to recognise that there was an exception. On appeal Lord Evershed MR declined to affirm or disaffirm Lloyd-Jacob J's views: see (1952) 69 RPC 10, 16. After reviewing the authorities, Francis Gurry, *Breach of Confidence* (1984) p 283 suggests, in relation to innocent third parties who have changed their position in reliance on the information:

> The correct approach would seem to be that the court in exercising its *equitable* jurisdiction to grant relief should consider *all* the circumstances of the case – whether the third party is a bona fide purchaser, whether he has altered his position, and any other relevant matter.

(Emphasis in original)

as those referred to in the passage from the Alberta report cited above,[269] in which it would be unfair to prevent T from using the information even if he or she gave no value in return for it. We see difficulty in constructing a formula that would satisfactorily distinguish between those cases in which it would be fair to require T to have given value, and those in which it would not.[270]

6.24 We have provisionally concluded, therefore, that the proposed exclusion should apply whether or not T gives value for the trade secret.

**When is the third party "innocent" for this purpose?**

6.25 The exclusion will not normally apply, of course, if when T acquires the information he or she "knows"[271] that it is a trade secret (unless T believes that its owner consents to T's acquisition of it).[272]

6.26 In our view T should not in principle be regarded as "innocent" where, although he or she does not know that the information is a trade secret, he or she is aware, at the time of acquiring it, that it was at some stage acquired by the commission of a crime. T may know, for instance, that the information was originally extracted from stolen documents. In this kind of case, we believe that T's knowledge from the outset that the information came from a tainted source, in conjunction with the subsequently acquired knowledge that the information is a trade secret, should preclude him or her from using or disclosing it thereafter.

6.27 We have borne in mind, however, that this qualification of the exclusion would operate to defeat an important defence which would otherwise be available. We have therefore provisionally concluded that it should not extend to offences that are comparatively trivial. This conclusion involves the need to provide a test for distinguishing the more serious offences, which prevent the exclusion from applying, from other offences. We have arrived at the provisional view that, with one exception, the commission of a purely summary offence should be disregarded.[273] The exception would apply where T knows that the information

[269] See para 6.19 above.The defence proposed in the Alberta report does not require that the defendant should give value.

[270] A leading academic commentator has observed that it is in the (civil) law relating to third parties that "doubts are thickest and doctrinal differences headiest": W R Cornish, *Intellectual Property* (3rd ed 1996) para 8–32. In our Breach of Confidence report we recommended that the court should have far-reaching discretionary powers to adjust the position between the third party and the person to whom the obligation of confidence was owed: Law Com No 110 (1981) para 6.114; draft Bill, cl 15. The court would be empowered, for example, to require the third party to pay the plaintiff a royalty in respect of his or her further use of the information. This technique is unavailable in the criminal law.

[271] In the sense in which we use that word in relation to the proposed offence: see paras 5.8 – 5.9 above.

[272] This would include the case in which T mistakenly believes that the person from whom he or she acquires the trade secret is its sole owner.

[273] Offences that would be treated as "serious" for this purpose include theft, obtaining by deception and conspiracy (including conspiracy to defraud).

was obtained by the summary offence of "hacking" into a computer.[274] That offence is manifestly of particular significance in the present context.

6.28 **We provisionally propose that the new offence should not extend to the use or disclosure of information by a person who, at the time of acquiring the information (whether or not for value),**

**(1) did not know that it was a trade secret belonging to another, or**

**(2) was not aware that that other did not, or might not, consent to that acquisition (or believed that that other would consent to it if he or she knew of it and the circumstances of it),**

**unless that person was at that time aware that its acquisition by any other person from whom he or she (directly or indirectly) acquired it had (or may have) involved the commission by any person of**

**(a) an indictable offence, or**

**(b) an offence contrary to section 1 of the Computer Misuse Act 1990.**

## PUBLIC INTEREST

### Public interest under the law of confidence

#### *"Iniquity"*

6.29 In an early case, *Gartside v Outram*,[275] an employee was held to be justified in disclosing confidential accounting information which showed that his employer was defrauding customers. Wood V-C said:[276]

> [T]here is no confidence as to the disclosure of iniquity. You cannot make me the confidant of a crime or a fraud, and be entitled to close my lips upon any secret which you have the audacity to disclose to me relating to any fraudulent intention on your part: such a confidence cannot exist.[277]

#### *The modern, wider defence*

6.30 In *Initial Services v Putterill*[278] a former employee argued that there was a public interest in his disclosure of the facts that the employers had entered into an illegal price-fixing agreement[279] and that they had issued misleading statements to the public concerning the effect of the imposition of selective employment tax. The Court of Appeal rejected the employers' argument that only a crime or a fraud could justify disclosure.

[274] Computer Misuse Act 1990, s 1. See paras 1.16 – 1.17 above.

[275] (1857) 26 LJ Ch (NS) 113.

[276] *Ibid*, at p 114.

[277] More recently, in *Finers v Miro* [1991] 1 WLR 35 a solicitor was held to owe no duty of confidentiality to a client engaging in fraud. Balcombe LJ stated, at p 46B: "[F]raud unravels all obligations of confidence".

[278] [1968] 1 QB 396.

[279] Contrary to the Restrictive Trade Practices Act 1956.

6.31 Salmon and Winn LJJ regarded the iniquity rule as extending to the facts of the case, but gave no further guidance as to what it encompassed. Lord Denning MR, on the other hand, went further: in his view there was a defence of public interest, not limited to crime and fraud, which extended to the disclosure of "any misconduct of such a nature that it ought in the public interest to be disclosed to others".[280]

6.32 In *Fraser v Evans*[281] Lord Denning adopted a slightly different approach: the "iniquity" rule was not, he explained, a principle but was merely an instance of "just cause or excuse for breaking confidence". In *A-G v Guardian Newspapers (No 2)*,[282] Lord Goff also saw the "inquity" rule as being embraced by the more general rule that the public interest may sometimes demand disclosure.[283]

6.33 The authorities establish that the disclosure of medically dangerous information is justified, as, for example, in *Church of Scientology v Kaufman*.[284] The defendants proposed to publish a book by the first defendant containing information on scientology which the plaintiffs regarded as confidential. Goff J accepted the first defendant's contention that he had suffered a mental breakdown as a result of attending courses on scientology conducted by the plaintiffs, and held that it was therefore in the public interest that the practice of scientology should be exposed.

6.34 On the other hand, if the danger to public safety has completely passed, there is no ground on which a breach of confidence is justified. Thus, in *Schering Chemicals Ltd v Falkman Ltd*[285] a consultant had helped a drug company to present its case to the public following adverse publicity and findings that one of its drugs could cause abnormalities in unborn children. The drug had, however, been withdrawn from the market and had been the subject of wide publicity and scientific investigation. Subsequently, the consultant proposed to make a television programme on the issue. By a majority, the Court of Appeal restrained him from proceeding, on the ground that the information he would use had been supplied to him in confidence.

6.35 In a dissenting judgment, however, Lord Denning MR emphasised the importance of freedom of the press; and stated that no injunction forbidding publication should be granted

> except where the confidence is justifiable on moral or social grounds … or … on industrial grounds … and, in addition, where the *private* interest in maintaining the confidence outweighs the *public* interest in making the matter known to the public at large.[286]

[280] [1968] 1 QB 396, 405D.

[281] [1969] 1 QB 349.

[282] [1990] 1 AC 109.

[283] [1990] 1 AC 109, 282E–F.

[284] [1973] RPC 635.

[285] [1982] QB 1.

[286] [1982] QB 1, 22 (emphasis in original).

6.36 Again, in *Lion Laboratories Ltd v Evans*[287] the Court of Appeal stated that the defence of public interest was not limited to the disclosure of iniquity, but was based on the wider ground of "just cause or excuse". The case concerned publication in a national newspaper of internal memoranda that cast doubt on the accuracy of breathalyser instruments relied on in prosecutions for drunk driving. The Court of Appeal found that there was a public interest in the disclosure, in that it might lead to the reappraisal of a device having the potential for causing a wrongful conviction of a serious offence.[288] There is support for this in *A-G v Guardian Newspapers (No 2)*, where Lord Goff confirmed that the "principle extends to matters of which disclosure is required in the public interest".[289] The Court of Appeal in *Lion Laboratories* emphasised, however, that there was a difference between matters which might merely be interesting to the public (to which the instant defence did not apply)[290] and those which it was in the public interest to make known.[291]

### *Reasonable grounds for disclosure*

6.37 In the context of public interest[292] there must be reasonable grounds for the employee to suspect the actual or apprehended misdeed in question.[293] Where,

[287] [1985] QB 526.

[288] Stephenson LJ said at [1985] QB 526, 536G–537A:

> The duty of confidence, the public interest in maintaining it, is a restriction on the freedom of the press which is recognised by our law, as well as by article 10(2) of the [European] Convention for the Protection of Human Rights and Fundamental Freedoms … ; the duty to publish, the countervailing interest of the public in being kept informed of matters which are of real public concern, is an inroad on the privacy of confidential matters.

[289] [1990] 1 AC 109, 283F–G.

[290] "The public are interested in many private matters which are no real concern of theirs and which the public have no pressing need to know": *per* Stephenson LJ at [1985] QB 526, 537C.

[291] Griffiths LJ added (at [1985] QB 526, 553F) that the decision should not be treated as a "mole's charter". See also Viscount Dilhorne in *British Steel v Granada* [1981] AC 1096, 1175: "It is not, of course, the case that publication of material however interesting to the public is necessarily in the public interest."

[292] In *Hellewell v Chief Constable of Derbyshire* [1995] 1 WLR 804, 810H, Laws J remarked:

> It is perhaps confusing to put the matter on the basis that, in the celebrated dictum, "there is no confidence in iniquity"; some little difficulty has been caused in the past by the question whether the iniquity must be proved or it is enough that it is the result only of reasonable suspicion.
>
> The better analysis is in terms of the public interest defence, which is always available where the facts support it, against a confidence claim.

[293] See, eg, *A-G v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 262A, *per* Lord Keith of Kinkel: "[I]t is not sufficient to set up the defence merely to show that allegations of wrongdoing have been made. There must be at least a prima facie case that the allegations have substance." Similarly, Lord Goff of Chieveley, at p 283A–B:

> [A] mere allegation of iniquity is not of itself sufficient to justify disclosure in the public interest. Such an allegation will only do so if, following such investigations as are reasonably open to the recipient, and having regard to all the circumstances of the case, the allegation in question can reasonably be regarded as being a credible allegation from an apparently reliable source.

however, disclosure is threatened only to a recipient which has a duty to investigate matters within its remit, it seems that the court need not investigate the substance of the proposed disclosure unless there is ground for supposing that the disclosure goes outside such remit.[294]

### *To whom may disclosure be made?*

6.38 The disclosure must be to someone who has a "proper interest"[295] to receive the information in question.

> In certain circumstances the public interest may be better served by a limited form of publication perhaps to the police or some other authority who can follow up a suspicion that wrongdoing may lurk beneath the cloak of confidence. Those authorities will be under a duty not to abuse the confidential information and to use it only for the purpose of their inquiry. If it turns out that the suspicions are without foundation, the confidence can then still be protected … . On the other hand, the circumstances may be such that the balance will come down in favour of allowing publication by the media … .[296]

6.39 In *Francome v Mirror Group Newspapers Ltd*,[297] for example, the public interest defence was held not to justify disclosure to a national newspaper of telephone conversations between a jockey and his wife which revealed that he had broken Jockey Club regulations and might have committed offences: disclosure to the Jockey Club would have sufficed.

### Our Breach of Confidence report

6.40 In our Breach of Confidence report[298] we made recommendations concerning public interest, which are expressed as follows in clause 11 of the draft Bill annexed to the report:

[294] *Re a Company's Application* [1989] Ch 477, 482H–483A, *per* Scott J, who held that an employee of a company did not breach a duty of confidence to his employer by disclosing financial irregularities to FIMBRA (a regulatory body set up pursuant to the Financial Services Act 1986) which fell under its umbrella of investigation. Disclosure to the Inland Revenue, on the other hand, was permissible only if it related to fiscal provisions which were the concern of the Inland Revenue, and anything beyond this would constitute a breach of confidentiality.

[295] *Initial Services v Putterill* [1968] 1 QB 396, 405, *per* Lord Denning.

[296] *A-G v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 269A–C, *per* Lord Griffiths. "It does not follow that the public interest will … require disclosure to the media, or to the public by the media": *ibid*, at p 283G–H, *per* Lord Goff. Similarly, Sir John Donaldson MR said (*ibid*, at p 177F–G):

> [T]he nature and degree of the communication must be proportionate to the [just] cause or excuse. Thus communication to those who have a duty to receive and act on the information may be justified in circumstances in which indiscriminate communication would not … .

[297] [1984] 1 WLR 892.

[298] (1981) Law Com No 110.

(1) A defendant in proceedings for breach of confidence shall not be liable to the plaintiff in respect of any disclosure or use of information by the defendant in breach of an obligation of confidence if –

(a) the defendant raises the issue of public interest in relation to that disclosure or use in accordance with subsection (2); and

(b) the plaintiff is unable to satisfy the court that the public interest relied on by the defendant under that subsection is outweighed by the public interest involved in upholding the confidentiality of the information.

(2) For the purposes of subsection (1) a defendant raises the issue of public interest in relation to a disclosure or use of information if he satisfies the court that, in view of the content of the information, there was, or (in the case of an apprehended disclosure or use) will be, at the time of the disclosure or use a public interest involved in the information being so disclosed or used.

(3) A public interest may be involved in the disclosure or use of information notwithstanding that the information does not relate to any crime, fraud or other misconduct.

(4) When balancing the public interests involved for the purposes of subsection (1) the court shall have regard to all the circumstances of the case, including –

(a) the extent and nature of the particular disclosure or use in question as compared with the extent and nature of the disclosure or use which appears to be justified by the public interest on which the defendant relies;

(b) the manner in which the information was acquired … ; and

(c) the time which has elapsed since the information originally became subject to the obligation of confidence owed by the defendant … .

### Public interest and the proposed offence

6.41 We regard it as virtually beyond question that, as in the law of confidence, there should be *some* kind of public interest defence.[299] We share the view expressed in the Alberta report,[300] that without a defence of public interest "the criminal law would protect holders of trade secrets whose own conduct is reprehensible or even criminal, eg, withholding a report that the holder's product will cause injury or death".[301]

6.42 The task of formulating such a defence is, however, an exercise of some difficulty, because of the need to bear in mind two conflicting considerations. On the one hand, we seek to define the defence with the degree of certainty appropriate to

[299] Although none of the American states that provide criminal penalties for the misappropriation of trade secrets appears to provide for such a defence.

[300] At para 13.59.

[301] The defence proposed in the report is, however, limited to the disclosure of information for the purpose of exposing crime, fraud or other misconduct or for protecting public health or safety: see cl 301.3(5) of the draft Criminal Code provisions.

criminal legislation. On the other hand, we believe that it is necessary to ensure, as a matter of principle, that a person cannot be convicted of the proposed offence for disclosing information in circumstances in which, under the civil law of breach of confidence, the disclosure would be justified. It might be possible to reconcile the conflict between these two considerations were it possible to provide an exhaustive list of the grounds on which, under the law of confidence, disclosure is justified; but, in view of the uncertainties in that area, we believe that it would be unrealistic to attempt to compile such a list.[302]

6.43 In our view, there are four main options. The first is to provide, without more, that it should be for the jury to determine whether the defendant's use[303] or disclosure of a trade secret was in the public interest. We do not favour this approach. Among other objections, the question whether, on the facts as admitted or established, public interest justified the use or disclosure in question must in our view be a matter of law for the judge.

6.44 The second option is to provide, in terms, that the law should be the same in this respect as in the law of confidence.[304] This would automatically ensure that no one would be convicted of the proposed offence in circumstances in which the civil law would regard his conduct as lawful – a result which seems to us to be right in principle. It would, on the other hand, involve what some might regard as a drawback – namely, that in every trial for the proposed offence in which public interest was in issue, the court would be obliged to consider an area of the civil law which in some respects is unclear.

6.45 The third option would be to provide a statutory code by incorporating, with necessary adaptations, the recommendations in our Breach of Confidence report.[305] This would have the advantage of providing the court with a self-contained statutory code that would obviate the need to investigate the present, uncertain law of confidence.

6.46 We have reservations, however, about incorporating one element of those recommendations in the context of criminal law. Under them the court would be directed to have regard (among other matters) to the manner in which the information was acquired.[306] We included this requirement in our report because

[302] The Lord Chancellor's Department and the Scottish Office, in a joint consultation paper on the civil law relating to privacy published in 1993, canvassed the question whether a public interest defence should be expressed in general terms or should list specific matters which it is in the public interest to know. They agreed (at para 5.66) with the approach adopted by the Calcutt Committee (see n 72 below), which had concluded that it would be preferable to indicate in legislation those matters which were of public interest. The Lord Chancellor's Department and the Scottish Office accepted, however (at para 5.59), that different considerations might well apply in relation to criminal offences.

[303] Although it seems unlikely that in practice the *use* of a trade secret will normally involve a question of public interest, we see no reason to exclude it in principle from the ambit of the defence. It might apply, eg, where a person who has acquired another's trade secret relating to the production of a life-saving drug produces and markets the drug.

[304] See paras 6.29 – 6.39 above.

[305] See para 6.40 above.

[306] See subsection 4(b) of the draft clause set out at para 6.40 above.

we there recommended the imposition of an obligation of confidence on a person who acquired information by any of several specified "reprehensible means".[307] Our provisional view is that this element should not play a part in the offence that we provisionally propose in this paper; and we see force in the argument, expressed by an academic commentator, that

> it is the information which is all important and the question for the court is whether the information should be kept secret, or be disclosed in an appropriate manner. If the defendant murders, rapes, tortures, burgles or steals in order to obtain it, these matters should be subject to separate criminal (or civil) proceedings. They should not be allowed to override the public interest in having the information released.[308]

6.47 The fourth option is a "hybrid". It is based *in part* on a statutory list of the purposes which would justify the use or disclosure in question. The Alberta report was based wholly on this approach: it simply proposed[309] that it should be a defence if the defendant established that the information was disclosed for the purpose of

(a) exposing crime, fraud, or any other unlawful conduct; or

(b) protecting public health or safety.[310]

[307] See para 6.79 of the report.

[308] Allison Coleman, *The Legal Protection of Trade Secrets* (1992) p 74. Although her argument relates to the present law of breach of confidence, we believe that it would apply equally to the proposed offence.

[309] See cl 301.3(5) of the draft Criminal Code provisions. The defence is not expressed to extend to the *use* of information, which in our view should be included: see n 65 above.

[310] Similarly, the Calcutt Committee (see paras 2.14 – 2.15 above) recommended, at para 6.35, that it should be a defence to the offences it proposed that the act was done

a. for the purpose of preventing, detecting or exposing the commission of any crime, or other seriously anti-social conduct; or

b. for the protection of public health or safety; or

c. under any lawful authority.

The Committee recognised, however (at para 7.21), that "seriously anti-social conduct" might be a difficult concept for criminal legislation. It instanced the case of slum landlords.

In 1996 a Public Interest Disclosure Bill was introduced in the House of Commons by a private member, Mr Don Touhig. On 12 July 1996, in the debate on the Bill as amended in Standing Committee, the Government tabled a number of further amendments, and the Bill fell. It would have conferred on individuals civil remedies if penalised (by, among other things, dismissal from employment) or prosecuted for disclosing certain information where (i) the disclosure is one that the courts would find to be justified in the public interest and (ii) a number of other requirements were met. The definition of public interest in the Bill included *both* a requirement that the disclosure was such that in an action for breach of confidence the court has found, or would be likely to find, that the disclosure was justified in the public interest *and* that the disclosure tended to show that "significant misconduct or malpractice" was involved. That phrase was defined as including (but was not limited to): (i) an offence or a breach of any statutory requirement or legal obligation; (ii) improper or unauthorised use of public or other funds; (iii) abuse of authority; (iv) miscarriage of justice; (v) maladministration; and (vi) danger to the health or safety of any individual or to the environment.

6.48 This approach, however, involves the danger that the statutory list may not cover a purpose for which disclosure would be justified under the law of confidence. For example, the formula proposed in the Alberta report might not apply to the disclosure of defects in breathalyser devices which, under the law of confidence, the Court of Appeal has held to be justified.[311]

6.49 We believe that the best way to avoid such a result is to propose a further, residual qualification. The legislation would provide for specific purposes which justify the use or disclosure of confidential information; but, *in addition*, the accused would be able to rely on the public interest defence available under the law of confidence.[312] This residual defence would be available where an accused has used or disclosed a secret for a purpose not protected by the statutory list.

6.50 Before turning to extract from the law of confidence a list of the specific matters which fall under the head of public interest in that context and which seem to us to be appropriate to the proposed offence, we make one preliminary point. Under the law of confidence, the determination of a public interest issue requires the court

> [to balance] the public interest in upholding the right to confidence, which is based on the moral principles of loyalty and fair dealing, against some other public interest that will be served by publication of the confidential material. … I have no doubt … that in the case of a private[313] claim to confidence, if the three elements of quality of confidence, obligation of confidence and detriment or potential detriment are established, the burden will lie on the defendant to establish that some other overriding public interest should displace the plaintiff's right to have his confidential information protected.[314]

6.51 By contrast, we intend that, in the interests of certainty, no such balancing exercise arises in relation to any of the listed purposes; it suffices that the defendant uses or discloses the trade secret for one of those purposes.

6.52 We have provisionally concluded that the use or disclosure of a trade secret for the following specific purposes[315] should be excluded from the proposed offence. They are the prevention, detection or exposure of

(1) a crime,[316] a fraud[317] or a breach of statutory duty,[318] whether committed or contemplated;[319]

[311] *Lion Laboratories Ltd v Evans* [1985] QB 526. See para 6.36 above.

[312] As under the second option: see para 6.44 above.

[313] As distinct from a claim involving government secrets, where the public interest appears to be an ingredient of liability rather than a defence: see *A-G v Jonathan Cape Ltd* [1976] QB 752.

[314] *A-G v Guardian Newspapers Ltd (No 2)* [1990] 1 AC 109, 269, *per* Lord Griffiths (footnote added).

[315] As well as a use or disclosure which is justified on the ground of public interest under the law of confidence.

(2) conduct which is in the nature of a fraud on the general public;[320] and

(3) matters constituting a present or future threat to the health or welfare of the community.[321]

Where an accused justifies his or her disclosure by relying on one of these purposes, the disclosure must be to an "appropriate person".[322]

6.53 With considerable diffidence, we incline to favour a provision along the lines of the fourth option, namely the list of purposes for which disclosure may be made, together with the public interest defence (as it exists in the law of confidence) in reserve.

6.54 **We provisionally propose that the new offence should not extend to**

**(1) the use, or the disclosure to an appropriate person, of information for the purpose of the prevention, detection or exposure of**

**(a) a crime, a fraud or a breach of statutory duty, whether committed or contemplated;**

**(b) conduct which is in the nature of a fraud on the general public; or**

**(c) matters constituting a present or future threat to the health or welfare of the community; or**

**(2) any use or disclosure of information which, under the law of confidence, would be justified on grounds of public interest.**

6.55 More generally, we should welcome views on whether there should be any defence based on public interest and, if so, in what terms it should be formulated (whether or not along the lines of any of the options that we have canvassed).

[316] The Calcutt Committee recommended that it should be a defence to the offences it proposed that the act was done "for the purpose of preventing, detecting or exposing any crime": see n 72 above.

[317] *Gartside v Outram* (1856) 26 LJ Ch (NS) 113 (see para 6.29 above), cited by Lord Denning MR in *Initial Services v Putterill* [1968] 1 QB 396 (see para 6.30 above) at p 405C as establishing that an employee was justified in disclosing to his employer's customers a fraud that the employer proposed to commit on them, notwithstanding that the employer had instructed him not to disclose his plan to anyone.

[318] As in *Initial Services v Putterill* [1968] 1 QB 396.

[319] In *Initial Services v Putterill* [1968] 1 QB 396, 405E–F, Lord Denning MR referred to "crimes, frauds and misdeeds, both those actually committed as well as those in contemplation".

[320] *Initial Services v Putterill* [1968] 1 QB 396; *Church of Scientology v Kaufman* [1973] RPC 635. See paras 6.30 and 6.33 above.

[321] The disclosure of other matters relating to the health and welfare of the community may be held to be justified under the general head of public interest, on a balance of the public interests involved (see para 6.49 above). This would apply, eg, to the disclosure of information which a scientist has discovered about the cause of a particular cancer or the structure of a particular gene, but which he or she decides to keep secret so as to make a commercial profit.

[322] See paras 6.38 – 6.39.

### DISCLOSURE IN ACCORDANCE WITH A STATUTORY OBLIGATION OR POWER

6.56 **We provisionally propose that the new offence should not extend to any disclosure of information made by a person who, by statute or subordinate legislation, is obliged or permitted to make it.**[323]

### LEGAL PROCEEDINGS

6.57 **We provisionally propose that the new offence should not extend to the disclosure of information pursuant to a court order, or otherwise in, or for the purpose of, civil or criminal legal proceedings.** Examples are a disclosure made by way of discovery of documents in civil proceedings; and the disclosure to the defence in a criminal case of material which, although not part of the prosecution's case, is in its possession.[324]

### THE POLICE, SECURITY SERVICES AND PROSECUTING AUTHORITIES

6.58 **We provisionally propose that the new offence should not extend to the use or disclosure, in the lawful exercise of an official function in regard to national security or the prevention, investigation or prosecution of crime, of information obtained in the lawful exercise of any such function.**

6.59 It is arguable that this exclusion is unnecessary, on the ground that, if an official was charged with the proposed offence, he or she could justify the use or disclosure as having been made in the public interest. We do not accept this argument. It would be wholly inappropriate for us to consider in this paper the proper limits of the activities of such authorities or to make any proposals that might indirectly affect them; and in our view it would be an undesirable consequence of the introduction of an offence aimed at commercial impropriety if the authorities in question were ever thereby constrained to reveal the circumstances in which they obtained, used or disclosed the information in question.

[323] Eg, legislative provisions of the kind referred to at para 4.1, n 2 above, which also proscribe the disclosure of a trade secret by officials otherwise than in accordance with their duties under the statute in question.

[324] *Ward* [1993] 1 WLR 619; *Davis* [1993] 1 WLR 613, in both of which the Court of Appeal laid down principles as to the proper approach to disclosure, including the procedure to be followed where the prosecution contends that it would not be in the public interest to reveal particular information. The procedure involves determination of disputes by the court. See now the Criminal Procedure and Investigations Act 1996.

# PART VII
# ACQUISITION OF A TRADE SECRET

7.1 A difficulty with our proposed offence is that, being limited to the *use or disclosure* of a trade secret, it would fail to catch the *acquisition* of information by unacceptable means. Difficulties could arise in circumstances where an individual, in an opportune moment, speculatively gathers confidential information from a commercial enterprise in the hopeful belief that it could be of value, but ignorant of the content or status of the information. Another example might be an employee who, in a fit of rage after his or her dismissal, amasses large amounts of confidential information, to which he or she is not entitled, with the half-formed intent to cause the employer some damage, although this never in fact occurs. Such scenarios raise hard questions of policy as to the forms of behaviour we wish to criminalise or to tolerate.

7.2 The Younger Committee, in its report on privacy,[325] found the weakest aspect of the relevant criminal law to be the absence of any provision whereby the acquisition of information would itself constitute an offence.[326] The inadequacies of the law were more recently illustrated in the case of *Layton*,[327] reputedly "Britain's biggest industrial espionage trial".[328] Agents of the accused were alleged to have infiltrated its rival's premises as employees, copied the rival firm's confidential financial information and taken photographs of its directors. These allegations were not in dispute, but the prosecution was unsuccessful.

### THE SCALE OF THE PROBLEM

7.3 It was pointed out by the Younger Committee that evidence of actual instances of industrial espionage was scarce, and the Committee thus felt unable to estimate the scale of the problem.[329] Companies often did not know that they were the targets of such activity, or were reluctant to admit it; some organisations regarded it as a legitimate tactic in a competitive market, and some actively engaged in it.[330] This problem was also highlighted in Parliament during the debate on Sir Edward Boyle's Industrial Information Bill. Mr Dudley Smith MP asked the Minister of State for the Board of Trade[331] about the incidence of complaints of industrial espionage.[332] The Minister responded that the Ministry had failed to obtain any evidence supporting complaints of industrial espionage, and that it was an area in which it was difficult to obtain evidence. He added:

[325] (1972) Cmnd 5012 ("the Younger report"). See paras 2.5 – 2.8 above.

[326] Younger report, para 488.

[327] *The Times* 13 March 1993.

[328] V Tunkel, "Industrial Espionage: What Can the Law Do?" [1993] Denning LJ 99.

[329] Younger report, paras 477 and 492.

[330] Younger report, para 492.

[331] Edward Dell MP.

[332] *Hansard* (HC) 13 December 1968, vol 775, col 818.

> It may be that firms are not prepared to provide evidence concerning their losses, because they do not want to reveal inadequate industrial security.[333]

7.4 Nonetheless, the Younger Committee received evidence in relation to the problem from a range of respondents, including companies and security firms.[334] One private enquiry agency informed the Committee of fifty cases involving industrial espionage that they had been asked to investigate in the course of two years.[335]

7.5 In his book on the subject,[336] D Del Mar refers to a Harvard study carried out in 1959 which sought to determine the scale and awareness of the activities of industrial spies. The study consisted of two parts. One part consisted of interviews with 200 industrial executives, while the second consisted of a questionnaire sent to 488 companies, 38 per cent of which responded. More than a quarter of the respondents knew of recent instances of spying in their industry, and one fifth said that they thought the practice was on the increase. 22 per cent of the respondents had knowledge of their employees revealing information to outside groups, and 50 per cent of those reported a competitor as the recipient.

7.6 According to J Perham, although accurate figures of the loss to American industry as a result of industrial espionage were hard to come by, estimates ran as high as $4 billion a year.[337] An added loss to industry is the expenditure each year on security and counter-espionage, the latter possibly as a consequence of the current inadequacies in our present law. *Layton*[338] provides an illustration of the drastic measures companies may resort to in the fear of industrial espionage.[339]

7.7 In a number of foreign jurisdictions there has been government concern as to the increase of industrial espionage and the resulting losses to industry and to the wider economy.[340] The German law relating to confidential information was recently extended[341] to cover the acquisition of trade secrets. It was thought that the existing law, in being limited to the use or disclosure of commercial information, merely served as an "encouragement" to industrial spies, and caused severe difficulties where the information had been acquired with the intention of

[333] *Ibid*.

[334] See nn 23–31 below.

[335] Younger report, para 481.

[336] D Del Mar, *The Security of Industrial Information* (1974) p 116.

[337] *Ibid*, at p 122. The sources of these estimates are not cited.

[338] *The Times* 13 March 1993.

[339] See para 7.2 above.

[340] See Appendix B for an account of criminal provisions enacted in foreign jurisdictions.

[341] § 17 (2) 1 UWG was introduced in 1986. See F-K Beier, "The Protection of Trade Secrets in Germany: A Short Appraisal in View of Japan's New Trade Secret Legislation" in H G Leser & T Isomura (eds), *Wege zum japanischen Recht* (1992) 817, at p 823. The extension of the offence under the German law against unfair competition was the result of a recommendation by the Max-Planck Institute which carried out research on the law in this area: *ibid*, at p 818.

disclosing it abroad, or at a much later date if it proved to be of value.[342] The procurement of a trade secret under § 17 (2) 1 of the Law Against Unfair Competition is punishable provided that it was without authorisation, with the necessary intent and achieved by the use of technical means such as the making of reprographic copies.[343]

### DEFINITION OF INDUSTRIAL ESPIONAGE

7.8 The Younger Committee, in looking at the protection of commercial information, identified problems of definition in relation to industrial espionage.[344] In seeking to outline the activities in question, it described industrial espionage as "the improper acquisition for gain of valuable industrial or commercial information".[345]

7.9 The Committee did not accept the commonly held belief that industrial espionage involves the use of optical or electronic devices.

> [S]uch evidence and information as we were given suggested that technical devices for surreptitious intrusion were used in a very small minority of cases … .[346]

7.10 It is thus necessary to consider what activities we are referring to when we speak of industrial espionage. Industrial espionage takes a number of forms, and in proposing any changes to the law in this area it is vital to take account of a wide range of activities. The methods identified by the Younger Committee fell into nine distinct categories, the vast majority of which notably rely on the use of human agency – namely:

(a) theft by an outsider;[347]

(b) use of technical devices;[348]

[342] Dr W Rupp, "Strafrechtlicher Schutz von Computersoft- und Orgware nach para 17 ff UWG unter Berucksichtigung der Reformentwurfe zum UWG" (1985) 12 WRP 676, 677.

[343] F-K Beier, "The Protection of Trade Secrets in Germany: A Short Appraisal in View of Japan's New Trade Secret Legislation" in HG Leser & T Isomura (eds) *Wege zum japanischen Recht* (1992) 817, at p 824.

[344] Younger report, para 479.

[345] *Ibid*.

[346] Younger report, para 482(ix).

[347] Younger report, para 482(i). The Committee learnt of a number of thefts of valuable documents containing commercial information, especially relating to pharmaceutical products in an unnamed European country. The Committee was also informed of a case in which documents, including design drawings and operating manuals, were stolen from a European office of a British organisation, and subsequently discovered during a police raid of the thief's premises which had been prompted by an unrelated offence. It was pointed out to D Del Mar during the course of his research on the subject that, as a result of the absence of patent law for drugs in Italy, that country had "become a haven for those who make a living from stolen drug research secrets": *The Security of Industrial Information* (1974) p 115.

[348] The Committee was informed of cases where companies had discovered electronic listening devices on their premises. Unauthorised entries on to business premises were also instanced, often involving the use of camera equipment: Younger report, para 482(ii). D Del

(c) planting of employees within a rival organisation;[349]

(d) impersonation;[350]

(e) poaching of employees from a rival organisation;[351]

(f) suborning employees;[352]

(g) misappropriation by an agent or employee;[353]

(h) offers for sale by agents or employees;[354] and

(i) exploitation by ex-agents, ex-employees or prospective employees.[355]

Mar cites a case in which the spies resorted to aerial photography: *The Security of Industrial Information* (1974) pp 121–122.

[349] The Committee was informed of a case where an individual was asked by an organisation to take up employment with a rival organisation with a view to obtaining information, in exchange for a fee: Younger report, para 482(iii). The infiltration of spies into the organisation as employees is also cited by D Del Mar as a major form of industrial espionage: *The Security of Industrial Information* (1974) p 114. The author also makes reference to the existence of industrial espionage schools in Japan, with reference to an article in *Time* 14 December 1962, entitled "School for Spies": *ibid*, at p 115. In *Layton, The Times* 13 March 1993, a company employed a number of undercover agents to infiltrate a rival company. One individual obtained a post as car park manager at the rival firm and another obtained the post of personal assistant to the managing director by means of a false curriculum vitae. See V Tunkel, "Industrial Espionage: What Can the Law Do?" [1993] Denning LJ 99.

[350] Eg, as potential customers, an example of which was given to the Committee: Younger report, para 482(iv). The Committee was also informed of a case in which a man offered the secrets of a new product of a company to one of its rivals. He had obtained the information during an extended interview for the post of senior copywriter with the advertising agency used by the company: *ibid*, para 482(ix). Several other guises cited by J Perham in D Del Mar, *The Security of Industrial Information* (1974) at p 123, included those of safety officers, journalists, job applicants and businessmen interested in merging with the company; but concrete examples are not provided, and much of this may be speculation.

[351] The Committee was given a number of examples, by various organisations, of the recruitment of employees in possession of information useful to the recruiting firm, from other firms operating in the same line of business. In one case a company executive took up an appointment with a rival company and was followed by an exodus of employees to the rival firm, together with the theft or copying of plans. In another case, a rival firm attempted to recruit the works manager, the chief production manager and a senior design engineer, succeeding only with the latter. An injunction was granted against using that employee in the relevant field of technology. In a further case, a senior design engineer moved to another firm which subsequently embarked on similar manufacture: Younger report, para 482(v).

[352] The Committee was informed of a number of cases in which employees were bribed or otherwise induced to disclose secret commercial information. In one case a journalist persuaded his girlfriend to steal a computer printout: Younger report, para 482(vi).

[353] The Committee gave details of a conviction of a chemistry student who had stolen papers containing the formula for a drug developed by the firm which employed him. The Committee cited a number of similar cases, and quoted evidence from Sir Richard Powell, then Director General of the Institute of Directors, who referred to the existence of a number of organisations which had been set up to steal formulae and industrial secrets and which provided a lucrative market for those wishing to sell them: Younger report, para 480.

[354] The Committee was informed of a number of instances in which firms had been approached by employees or agents of rival firms offering to sell them information: Younger report, para 482(viii).

7.11 The most serious threat seems to come from employees and the employer's agents, such as individuals recruited for marketing or advertising purposes. For these reasons we explained earlier in this paper that employees would not be excluded from our proposed offence of use or disclosure of a trade secret.[356]

7.12 Although the Committee believed that technical devices were rarely used to obtain information, it proposed the creation of a new criminal offence for the unlawful use of technical surveillance devices alone.[357] Such devices were defined as "electronic and optical extensions of the human senses".[358]

### THE USE OF UNLAWFUL MEANS

7.13 In our Breach of Confidence report[359] we found it to be

> a glaring inadequacy of the present law that … the confidentiality of information improperly obtained, rather than confidentially entrusted by one person to another, may be unprotected.[360]

7.14 We recommended that

> the acquirer of information should, by reason of the way in which he has acquired it, be *treated* as subject to an obligation of confidence in respect of it … .[361]

(1) Where the acquirer without proper authority had taken, handled or otherwise interfered with a thing and had thereby obtained the information, the information ought to be subject to an obligation of confidence by reason of the manner of the acquisition. Our recommendations applied solely to the civil law.

7.15 We recommended a number of circumstances in which the acquisition of information would be improper, even if it did not involve the taking of any tangible document.[362] The recommendation of a special provision for the obtaining of information by the unauthorised use of a computer[363] was in effect implemented by the Computer Misuse Act 1990.[364] We further recommended that the acquirer

[355] A relatively large number of cases were reported to the Committee of exploitation by ex-agents or ex-employees. One firm gave three recent examples where ex-employees had attempted to exploit information of a non-patentable kind after leaving their employment: Younger report, para 482(ix).

[356] See paras 6.7 – 6.11 above.

[357] The offence is set out in the Younger report, para 563.

[358] Younger report, para 504.

[359] Breach of Confidence (1981) Law Com No 110. See paras 2.9 – 2.13 above.

[360] Law Com No 110, at para 5.5.

[361] *Ibid*, at para 6.30.

[362] *Ibid*, at para 6.46.

[363] *Ibid*, at paras 6.32, 6.46.

[364] See paras 1.16 – 1.17 above.

should be subject to an obligation of confidence where the information was obtained by violence, menace or deception.[365]

7.16 We also adopted the Younger Committee's recommendation in relation to technical surveillance devices. We recommended that, where a device had been designed or adapted for surreptitious surveillance, anyone who obtained information by using it should be subject to an obligation of confidence in respect of the information so obtained.

7.17 A further case in which we recommended that the acquirer of information should be subject to an obligation of confidentiality is where the acquirer is, at the time of the acquisition, in any place where he or she has no authority to be.[366] In this way we hoped to avoid importing into this head all the detailed complexities of the law of trespass. We did not propose that the acquirer of the information should be liable for the acquisition as such, but that he or she should come under an obligation not to use or to disclose the information.

7.18 The Scottish Law Commission in 1977, before the publication of our Breach of Confidence report, published a memorandum on confidential information.[367] The provisional recommendations of the memorandum related both to the civil and criminal law of Scotland. In relation to its criminal law proposals, the Scottish Law Commission also considered the *method* of obtaining information, stating:

> In our view the criminal law should not apply if the act in issue is the divulging rather than the obtaining of information; if the method of obtaining is itself not unlawful; and in most cases involving commercial information, unless a person has entered premises without permission, or has searched cupboards or files.[368]

7.19 The Scottish Law Commission provisionally proposed that criminal sanctions be introduced by statute against the following activities:

> (A) It should be a statutory offence to enter upon premises without the occupier's consent, and without lawful authority, for the purpose of obtaining confidential information or information which is of value, whether or not the information is actually obtained …
>
> (B) It should be a statutory offence to search or examine the property owned or lawfully possessed by another person without that person's consent, or without lawful authority, with a view to obtaining confidential information of information which is of value. The term "property" should be sufficiently comprehensive to include vehicles, vessels, personal effects and tapes. It would thus be an offence to search a purse or a briefcase.
>
> (C) The use of certain technical surveillance devices should be made a criminal offence … . We anticipate that [this] category would include

[365] Law Com No 110, at paras 6.33, 6.46.

[366] *Ibid*, at paras 6.34, 6.46.

[367] Confidential Information (1977) Memorandum No 40.

[368] *Ibid*, at para 100.

any electronic or optical devices which permit a man of normal sight or hearing to receive visual or aural signals in circumstances in which he would otherwise be unable to do so, or which permit a record of such signals to be made.[369]

7.20 The Scottish Law Commission's proposals are noteworthy in that they adopt a similar approach to the one taken by us in our Breach of Confidence report[370] in relation to the acquisition of information by unlawful means.[371] Furthermore, they relate to the criminal rather than merely the civil law.

7.21 In its subsequent report on breach of confidence,[372] the Scottish Law Commission stated that the comments received upon consultation, and further analysis of the problems, had persuaded it that its earlier approach had been too ambitious, impinging upon wider issues of privacy and data protection quite unrelated to questions of breach of confidence.[373] The proposals were considered to be too wide, and it was pointed out that it would be difficult to establish when a person entered premises with a view to obtaining confidential information. The Commission also thought there was a danger that a criminal offence designed solely to provide sanctions in the field of confidentiality might, to be effective, have to be couched in terms sufficiently wide to enable it to embrace conduct of a quite different character.[374]

### OPTIONS FOR REFORM

7.22 We have considered possible ways of bringing industrial espionage within the scope of the criminal law. In our view there are three main options.

### Option 1: An offence of acquiring information with the intention of using or disclosing it

7.23 The first option is to create a further offence aimed not at the *use or disclosure* of information, but at the preliminary conduct of *acquiring* it with the *intention* of using or disclosing it. For this purpose, it would suffice if it was the defendant's intention to use or disclose the information only in certain circumstances (for example, if he or she could find a purchaser or, indeed, if it should suit his or her purpose to do so).[375]

7.24 One difficulty about such an offence concerns its mental element. Industrial spies do not necessarily know that the information they acquire is a trade secret:

[369] *Ibid*, at paras 101–102 (footnote omitted).

[370] See paras 2.9 – 2.13 above.

[371] Paragraph (i) above closely resembles the recommendation we made in Law Com No 110 at paras 6.34, 6.46: see para 7.17 above.

[372] Breach of Confidence (1984) Scot Law Com No 90.

[373] *Ibid*, at para 1.6.

[374] *Ibid*, at para 1.9.

[375] The question of so-called "conditional intention" in the law of theft (in connection with the intention permanently to deprive the owner of property) has given rise to difficulties and has been the subject of much academic comment. We envisage that any legislation along these lines would be drafted in terms that obviated any possible argument of that nature.

typically, they go on "shopping expeditions" in order to acquire any information that they may be able to sell or otherwise use. This problem might perhaps be met by a provision that the defendant commits the offence if he or she *either* knows that the information is a trade secret *or* is reckless as to that fact.[376]

7.25 But introducing "recklessness" may present more problems. Recklessness would not suffice for our proposed offence of using or disclosing another's trade secret. In other words, the industrial spy would commit no offence at the time of putting his or her intention into effect, by selling the ill-gotten information; yet he or she would commit an offence at an earlier, preparatory stage, by acquiring the information with that intention. In our view, this result would be anomalous.

7.26 Moreover, such an offence would not be restricted to industrial espionage and would thus extend to some kinds of conduct that we would not wish to criminalise. It might apply, for instance, in the following circumstances: A wishes to sell his business. During negotiations with B, a prospective purchaser, A provides a good deal of information about the business on a confidential basis. B has in mind that, even if the negotiations do not culminate in a purchase, he may be able to use the information. With the exception of one minor item, none of the information falls within the definition of a trade secret, perhaps because it has no value from not being generally known. If, however transiently, it crosses B's mind that some of the information *may* have such value, he might be held to have committed the offence.

### Option 2: an offence aimed at wrongful methods of acquisition

7.27 The second option is to create an offence which would focus not on the state of mind of the person who acquires the trade secret, but on the *means* by which he or she acquires it. This approach involves penalising the use of *methods of acquisition* that are thought unacceptable, whether or not they involve the commission of a crime or are otherwise unlawful.[377] It has been adopted in recent legislation in Bulgaria, where discovery of a trade secret is declared unfair if it is done by eavesdropping, by intrusion, by opening letters, taking away or searching documents and materials which have been filed in a manner restricting access.[378]

[376] More fully stated: the recklessness involved would be subjective. It would require that (a) the defendant was aware of a risk of the existence of the facts that marked the information as a trade secret and that (b), in the circumstances as he or she knew or believed them to be, it was unreasonable to take that risk.

[377] This approach is favoured by Victor Tunkel, "Industrial Espionage: What Can the Law Do?" [1993] Denning LJ 99. He suggests the creation of an offence of industrial espionage, which could be committed in one of two ways. The first would be the dishonest obtaining, or dishonest attempted obtaining, of commercial information for the purpose of making economic gain or causing economic loss (or knowing that such gain or loss was likely to result). Secondly, the offence would be committed by a person who dishonestly accepted or used such information, knowing that it had been so acquired. Although the offence would not be restricted to any particular means employed to obtain the information, certain of such means (including, eg, the unauthorised removal of a document) are specified as unlawful for the purpose of the offence: pp 110–112.

[378] Article 14 (3) of the Bulgarian Law on the Protection of Competition 1991. See Appendix B below.

7.28 We have already referred to the recommendations in our Breach of Confidence report that information obtained by certain reprehensible means should be regarded as impressed with an obligation of confidence.[379] Although we did not recommend that the use of the methods of acquiring information listed in the report should itself give rise to liability,[380] this approach may be thought none the less to merit consideration as a starting-point for the formulation of a possible offence.

7.29 In evaluating the merits of the reprehensible means listed in the Breach of Confidence report, however, it should be borne in mind that its recommendations apply to information of any kind, including personal information.[381] The present approach would involve the introduction of a criminal sanction for some methods of acquiring information, but only where the information was a trade secret. The effect would be that the methods of acquiring information which, in the Breach of Confidence report, we concluded were reprehensible (or those which the Calcutt Committee subsequently proposed should become criminal where personal information was involved)[382] would be proscribed only in the commercial field. By contrast with the proposals of the Scottish Law Commission in its memorandum on confidential information,[383] we are of the firm belief that the actual acquisition of a trade secret should be a necessary requirement. We agree that the proposal of the Younger Committee in relation to the use of technical surveillance devices should be adopted,[384] but believe that by itself it is too limited.

**Option 3: no change to the law**

7.30 The considerations relating to the possible criminalisation of industrial espionage by means of a separate offence are not only different from those that arise in the context of the improper use or disclosure of trade secrets but also involve issues of considerable difficulty and complexity. Moreover, as we explained in Part I of this paper, there are a number of existing offences that might be committed in the course of acquiring another's trade secret.[385] For example, the Computer Misuse Act 1990 makes it an offence to gain unauthorised access to data held on computer.[386] This offence may be committed by an industrial spy who "hacks" into

[379] See paras 2.11 and 7.13 – 7.17 above. The relevant clause of the draft legislation is set out in Appendix A below.

[380] See paras 5.1 – 5.2 above.

[381] A person's *behaviour* may constitute "information". We pointed out by way of example in Law Com No 110, para 6.29 that

> If … the leaders of two political parties were to meet for talks, in circumstances where they clearly wished the meeting to remain a secret, the fact of the meeting, quite apart from what might be said during it, may itself be information which is relevant to an obligation of confidence if it is obtained by improper means.

(Footnote omitted)

[382] See paras 2.14 – 2.15 above.

[383] (1977) Memorandum No 40. See paras 7.18 – 7.21 above.

[384] Younger report, para 563. See para 7.12 above.

[385] See paras 1.8 – 1.23 above.

[386] See paras 1.16 – 1.17 above.

a computer system which he or she is not authorised to use, to obtain data that amounts to a trade secret. Moreover, under the civil law, a person who acquires information (albeit innocently) may well be liable to account for its wrongful use or be ordered to pay damages.[387] These considerations may be thought to point to a third option: namely, to do nothing in the present project about the problem of the *acquisition* of trade secrets by means of industrial espionage.

7.31 **We invite views on**

**(a) whether the criminal law should be extended so as to cover the acquisition of a trade secret; and, if so,**

**(b) whether this should be done by creating**

**(i) an offence of acquiring a trade secret with the intention of using or disclosing it;**

**(ii) an offence of acquiring a trade secret by wrongful methods; or**

**(iii) an offence defined in some other way, and if so what.**

[387] "It may not be a case for injunction or even for an account, but only for damages, depending on the worth of the confidential information to him in saving him time and trouble": *per* Lord Denning, *Seager v Copydex (No 1)* [1967] 1 WLR 923, 932.

# PART VIII
# THE RELATIONSHIP BETWEEN CIVIL AND CRIMINAL PROCEEDINGS FOR TRADE SECRET MISUSE

8.1 If our proposed offence of using or disclosing a trade secret were enacted, wrongdoers would be liable to be prosecuted as well as sued. We now turn our attention to problems which might arise if wrongdoers were to find themselves in this position.

8.2 The first problem is whether, and if so to what extent, a defendant in civil proceedings can refuse to answer questions or produce documents on the basis of the privilege against self-incrimination:[388] if a defendant in civil proceedings does have this form of privilege, the criminalisation of trade secret misuse might make it harder for the owners of trade secrets to enforce their rights in civil proceedings. A further question is how the courts should deal with a civil claim relating to the alleged misuse of trade secrets where there is also an outstanding prosecution arising out of the same allegations.[389] We stress again that we envisage that our proposed criminal offence would apply only in the most serious cases, and that such problems would therefore arise only in a very small number of cases.

## THE PRIVILEGE AGAINST SELF-INCRIMINATION

### The present law

8.3 This privilege has its roots in the unpopularity of the Court of Star Chamber, which used unrestrained and oppressive means to require those brought before it to answer questions on oath. There developed a repugnance to the idea of compelling persons to convict themselves on their own word, and a growing belief that prosecutors should rely on their own machinery to investigate and prove guilt.[390] The privilege is also said to encourage witnesses to come forward and give truthful evidence without fear or confusion, and has recently been described as one of the "basic freedoms secured by English law".[391]

8.4 The privilege against self-incrimination enables a witness to refuse to answer questions, or produce documents, which might tend to incriminate the witness by exposing him or her to any punishment, penalty or forfeiture under English law.[392] The courts have ensured that the privilege can be invoked only where the risk of

[388] See paras 8.3 – 8.37 below.

[389] See paras 8.38 – 8.43 below.

[390] For an outline of the history and rationale behind the privilege against self-incrimination, see K Nouroozi and G Miller, "The Privilege Against Self-Incrimination: A Fraudster's Charter?" (1996) 15 Litigation 280. See also G McCormack, "Self-Incrimination in the Corporate Context" [1993] JBL 425.

[391] *Hamilton v Naviede (Re Arrows Ltd) (No 4)* [1995] 2 AC 75, 95, *per* Lord Browne-Wilkinson.

[392] See *Rio Tinto Zinc Corp v Westinghouse Electric Corp* [1978] AC 547.

incrimination is objectively real, not remote or insubstantial.[393] The privilege does not arise where the witness is already at risk, and the risk would not be increased if he or she were required to give the information, produce the documents or otherwise comply with what is sought.[394]

8.5 This privilege is now provided for in section 14(1) of the Civil Evidence Act 1968, which provides:

> The right of a person in any legal proceedings other than criminal proceedings to refuse to answer any question or produce any document or thing if to do so would tend to expose that person to proceedings for an offence or for the recovery of a penalty –
>
> (a) shall apply only as regards criminal offences under the law of any part of the United Kingdom and penalties provided by such law; and
>
> (b) shall include a like right to refuse to answer any question or produce any document or thing if to do so would tend to expose the husband or wife of that person to proceedings for any such criminal offence or for recovery of any such penalty.

8.6 The privilege is available not only to witnesses giving oral testimony but to any person required to provide information[395] or to disclose documents,[396] even under the Bankers' Books Evidence Act 1879.[397] The problem we are considering might arise in many different circumstances in which a defendant in civil proceedings claims to be fearful that he or she might be prosecuted for our proposed new offence.

8.7 Under the civil law, various forms of equitable relief have been developed by the courts to assist the plaintiff in the pursuance of a civil action. For instance, Anton Piller orders were introduced so as to enable premises to be searched for documents which the plaintiff feared might be destroyed, and to require the defendant to give information about the whereabouts of documents[398] or to permit

[393] *Sociedade Nacional de Combustiveis de Angola UEE v Lundqvist* [1991] 2 QB 310. The rule is that no-one is bound to answer any question if the answer thereto would, in the opinion of the judge, have a tendency to expose him or her to any criminal charge, penalty or forfeiture which the judge regards as reasonably likely to be preferred or suitable: *Blunt v Park Lane Hotel* [1942] 2 KB 253, 257.

[394] *Sociedade Nacional de Combustiveis de Angola UEE v Lundqvist* [1991] 2 QB 310, 324G–H, *per* Staughton LJ, citing *Khan (Mohammed Krim) v Khan (Iqbal Ali)* [1982] 1 WLR 513, 520F–H and 521F–G. See also *Marcel v Commissioner of Police of the Metropolis* [1992] Ch 225, 257F-G. See I Moulding, "The Privileged Fraudster" [1996] The Litigator 354, 356–357 for the modern rationale of the privilege.

[395] *Sociedade Nacional de Combustiveis de Angola UEE v Lundqvist* [1991] 2 QB 310.

[396] *Rank Film Distributors Limited v Video Information Centre* [1982] AC 380, 441–444.

[397] See *Waterhouse v Barker* [1924] 2 KB 759.

[398] These orders derive their name from the first case in which relief was granted, *Anton Piller KG v Manufacturing Processes Ltd* [1976] Ch 55: see para 5.14, n 23 above. For details of the circumstances in which such relief may be granted see S Gee, *Mareva Injunctions and Anton Piller Relief* (3rd ed 1995) pp 192–196. Anton Piller orders have recently been put on a statutory footing by the Civil Evidence Act 1997, s 7.

the plaintiff to enter the defendant's premises to search for and seize documents.[399] The privilege against self-incrimination began to cause serious problems when it led to the frustration of these forms of relief: as a result of the privilege being raised by defendants, plaintiffs were no longer able to ascertain the whereabouts of their property and prevent its further misuse. The basic principle still is that an Anton Piller order should not be made if it includes provisions likely to require defendants to incriminate themselves.[400]

8.8 As a consequence, the courts have become increasingly troubled by the privilege.[401] For example, Lord Templeman thought that the privilege could be justified on two grounds only, first that it discouraged ill-treatment of a suspect and second, that it discouraged the production of dubious confessions.[402] He believed that it was difficult to see any reason why in civil proceedings the privilege should be exercisable to enable a litigant to refuse to disclose relevant documents.[403] He concluded that the privilege was an "archaic and unjustifiable survival from the past",[404] while, in the same case, Lord Griffiths believed that it was "in need of radical reappraisal".[405]

8.9 Parliament has appreciated the unsatisfactory results of the privilege, and it has in consequence been abrogated or modified by statute in certain circumstances.[406] For example, under section 31 of the Theft Act 1968,[407] the privilege is removed

[399] *Tate Access Floors Inc v Boswell* [1991] Ch 512, 530.

[400] *Cobra Golf Inc v Rata* [1997] 2 WLR 629, 644, *per* Rimer J. See Civil Evidence Act 1997, s 7(7).

[401] See I Moulding, "The Privileged Fraudster" [1996] The Litigator 354, 357–360.

[402] *AT &T Istel Ltd v Tully* [1993] AC 45, 53B. See also *Hamilton v Naviede (Re Arrows Ltd) (No 4)* [1995] 2 AC 75, 95–96, where Lord Browne-Wilkinson stated that this "raised in an acute form the conflict between the witness's basic right to rely on the privilege on the one hand and the public interest in successfully pursuing and recovering the fruits of such fraud".

[403] *AT & T Istel Ltd v Tully* [1993] AC 45, 53C.

[404] *Ibid*, at p 53D.

[405] *Ibid*, at p 57G.

[406] Eg Criminal Justice Act 1988, s 77, in conjunction with the decision in *Re O* [1991] 2 QB 520; Criminal Justice Act 1987, s 2(13), to assist the Serious Fraud Office in carrying out its investigations; Companies Act 1985, s 434, to assist inspectors of the Department of Trade and Industry in carrying out their investigations; Insolvency Act 1986, ss 243–236, 433, which empower administrators, receivers and liquidators to request the disclosure of documents and impose duties upon the company's officers to assist the receiver or office-holder of a company; Banking Act 1987, s 39, which confers on the Bank of England powers similar to those conferred by the Criminal Justice Act 1987 on the Serious Fraud Office.

[407] Section 31(1) provides:

> A person shall not be excused, by reason that to do so may incriminate that person or the wife or husband of that person of an offence under this Act –
>
> (a) from answering any question put to that person in proceedings for the recovery or administration of any property, for the execution of any trust or for an account of any property or dealings with property; or
>
> (b) from complying with any order made in any such proceedings;

when a person may be incriminated with "an offence under this Act"; but our proposed offence would fall outside the Act. In addition, as we have previously said, a prosecution for wrongfully acquiring and misusing trade secrets can, where the appropriate circumstances prevail, be brought for conspiracy to defraud.[408] It was held in *Sociedade Nacional de Combustiveis de Angola UEE v Lundqvist*[409] that section 31 can apply only to offences under the Theft Act 1968, and not to a charge of conspiracy to defraud at common law[410] or of statutory conspiracy;[411] but the courts take a realistic view if a defendant claims that he or she might be prosecuted for offences other than those under the Theft Act 1968.[412]

8.10 The problem with the privilege against self-incrimination was shown acutely by the decision of the House of Lords in *Rank Film Distributors Ltd v Video Information Centre*.[413] In that case the plaintiffs brought an action for copyright infringement on the grounds of video piracy. The plaintiffs obtained Anton Piller relief so as to search the defendants' premises for pirated videos. The order was set aside on the grounds that it interfered with the defendants' privilege against self-incrimination: there was a risk of their incriminating themselves in circumstances where there was a real appreciable risk of a prosecution for conspiracy to defraud.

8.11 This decision provoked great concern because the more serious the wrongful conduct of the defendant, the stronger would be the claim to the privilege against self-incrimination. Sir Nicolas Browne-Wilkinson VC said that "the effectiveness of civil remedies designed to redress fraud will be seriously impaired".[414]

8.12 In that instance he was referring to Mareva injunctions, but the same argument applies to other remedies designed to ensure that a plaintiff is not prejudiced by

> but no statement or admission made by a person in answering a question put or complying with an order made as aforesaid shall, in proceedings for an offence under this Act, be admissible in evidence against that person or (unless they married after the making of the statement or admission) against the wife or husband of that person.

[408] See para 1.21 above.

[409] [1991] 2 QB 310.

[410] See *Scott v Metropolitan Police Commissioner* [1975] AC 819; Criminal Justice Act 1987, s 12.

[411] Criminal Law Act 1977, s 1.

[412] In *Renworth Ltd v Stephansen* [1996] 3 All ER 244, the Court of Appeal disallowed a claim of privilege on the grounds that the defendant might be prosecuted for conspiracy in addition to proceedings for theft. Morritt LJ (with whom Sir John Balcombe agreed) explained that the matter should be approached by considering the claims to privilege in respect of the Theft Act offences and the other offences separately. In *each* case the test would be "whether to answer the question would tend to expose the relevant person to proceedings for the relevant offence in the sense of creating or increasing the risk of proceedings for that offence": *ibid*, at p 254h.

[413] [1982] AC 380.

[414] *Sociedade Nacional de Combustiveis de Angola UEE v Lundqvist* [1991] 2 QB 310, 338. See also A Zuckerman, "Mareva Injunction v Privilege Against Self-Incrimination" (1990) 106 LQR 389, pointing out the paradox that a defendant may be ordered to disclose details of assets innocently obtained, but is immune from giving details of assets gained by criminal conduct.

the delay before trial, such as orders for information which would enable the assets in issue to be traced. The Vice-Chancellor believed[415] that section 31(2) of the Theft Act 1968 should be extended to all offences committed in the course of financial fraud.[416]

8.13 Parliament sought to reverse the decision in *Rank Film Distributors v Video Information Centre*[417] by passing section 72 of the Supreme Court Act 1981.[418] This takes away the privilege against self-incrimination in certain classes of case, but protects the person giving the information against the use of the information in any criminal proceedings save for perjury or contempt of court. This achieves a balance between the interests of the defendant and the party claiming to be aggrieved.

8.14 Under subsection (1) a person is not excused from answering questions in any proceedings to which section 72 applies, or from complying with any order, by reason that to do so would expose that person (or his or her spouse) to proceedings for a "related offence". This term is defined by subsection (5) as meaning –

[415] *Sociedade Nacional de Combustiveis de Angola UEE v Lundqvist* [1991] 2 QB 310, 388. See also *Tate Access Floors Inc v Boswell* [1991] Ch 512, 532.

[416] Similar views were expressed by Lord Donaldson MR and Neill LJ in *AT & T Istel Ltd v Tully* [1992] 1 QB 315.

[417] [1982] AC 380. See para 8.10 above.

[418] Section 72 provides, in part:

> (1) In any proceedings to which this subsection applies a person shall not be excused, by reason that to do so would tend to expose that person, or his or her spouse, to proceedings for a related offence or for the recovery of a related penalty –
>
> (a) from answering any question put to that person in the first-mentioned proceedings; or
>
> (b) from complying with any order made in those proceedings.
>
> (2) Subsection (1) applies to the following civil proceedings in the High Court, namely –
>
> (a) proceedings for infringement of rights pertaining to any intellectual property or for passing off;
>
> (b) proceedings brought to obtain disclosure of information relating to any infringement of such rights or to any passing off; and
>
> (c) proceedings brought to prevent any apprehended infringement of such rights or any apprehended passing off.
>
> (3) Subject to subsection (4), no statement or admission made by a person
>
> (a) in answering a question put to him in any proceedings to which subsection (1) applies; or
>
> (b) in complying with any order made in any such proceedings,
>
> shall, in proceedings for any related offence or for the recovery of any related penalty, be admissible in evidence against that person or (unless they married after the making of the statement or admission) against the spouse of that person.
>
> (4) Nothing in subsection (3) shall render any statement or admission made by a person as there mentioned inadmissible in evidence against that person in proceedings for perjury or contempt of court.

(1) in the case of proceedings for infringement of rights pertaining to any intellectual property, or for passing off, or proceedings brought to obtain disclosure of information relating to any infringement of such rights, or to any passing off,

(a) "any offence committed by or in the course of the infringement or passing off to which those proceedings relate", or

(b) any other offence "committed in connection with that infringement or passing off, being an offence of fraud or dishonesty"; or

(2) in the case of proceedings brought to prevent any apprehended infringement of such rights, or any apprehended passing off, "any offence revealed by the facts on which the plaintiff relies in those proceedings".[419]

8.15 The words "an offence involving fraud or dishonesty" *might* cover some instances of our proposed offence, and trade secrets might in some cases be regarded as "intellectual property".[420] Thus section 72 might ensure that a party to a civil claim could not justify a refusal to give information by relying on the possibility of a prosecution for our new offence. Although the witness would be protected to the extent that any information given in civil proceedings would be inadmissible in criminal proceedings for our new offence or for conspiracy to defraud,[421] it would be admissible in proceedings for perjury or contempt of court.[422]

8.16 The courts have tried to overcome the problems of the privilege against self-incrimination by including, in an order for disclosure in civil proceedings, a direction that any material disclosed is not to be used in subsequent criminal

[419] See *Coca Cola Co v Gilbey* [1996] FSR 23, 27. "[T]he privilege against self-incrimination is withdrawn only so far as the answer or compliance with the order would expose the defendant to proceedings for a "related offence" – I leave aside penalties which must, I think, clearly refer to statutory penalties and have no relevance in the context of the instant case. Secondly, to be a related offence, the offence must be one which is committed by the very act of infringement complained of or one committed in the course of carrying out that infringement or it must have been an offence involving fraud or dishonesty which is committed in connection with the infringement complained of or an offence revealed by the facts on which the plaintiff relies in the proceedings": *per* Lord Oliver in *Crest Homes plc v Marks* [1987] AC 829, 856.

[420] "Intellectual property" is defined to mean "any patent, trade mark, copyright, registered design, *technical or commercial information* or other intellectual property": s 72(5) (italics supplied). But in *AT & T Istel Ltd v Tully* [1993] AC 45, 64H–65A, Lord Lowry said:

> [T]he concluding words, "or other intellectual property", show that the "commercial information" which the definition contemplates must be information of the same type ("ejusdem generis") as the other examples of intellectual property which are listed in subsection (5).

[421] See para 8.9 above.

[422] See s 72(4). It was held in *Cobra Golf Inc v Rata* [1997] 2 WLR 629 that proceedings for civil contempt were proceedings for "the recovery of a penalty" within section 14(1) of the Civil Evidence Act 1968 (which is set out in para 8.5 above) in respect of which there was a privilege against self-incrimination, but that section 72 withdrew that privilege in appropriate civil proceedings.

proceedings.[423] Doubts have been cast on this approach,[424] but in any event it is only effective in the rare cases where the prosecuting authority is either a party to an application in the civil proceedings[425] or voluntarily[426] gives an undertaking not to use the material disclosed.[427]

### The Lord Chancellor's Department consultation paper

8.17 In July 1992, the Lord Chancellor's Department published a consultation paper on the privilege against self-incrimination in civil proceedings.[428] At that time, there was substantial concern that the privilege operated as a serious obstacle in civil proceedings by "allowing criminals to rely on the criminality of their own acts to escape the just claims of their victims, involving many millions of pounds".[429]

8.18 Thus in a recent case,[430] the Vice-Chancellor reluctantly set aside part of an Anton Piller order which had required the respondents to produce and verify information and documents and to allow entry, search and seizure, due to evidence indicating a real risk that execution of the order would have incriminated the respondents on a charge of conspiracy to defraud their employer. The ironical position was that the court was then precluded from making the order, although satisfied that there was a "grave danger" or "real possibility" that the defendant would destroy vital evidence. Faced with this fact, the Vice-Chancellor asked that Parliament should give urgent consideration to the problem and to the closely related problem which had arisen in the context of Mareva injunctions.[431]

[423] As in *Re O* [1991] 2 QB 520.

[424] See *United Northwest Co-operatives Ltd v Johnstone*, *The Times* 24 February 1994.

[425] As in *Re O* [1991] 2 QB 520.

[426] In *AT & T Istel Ltd v Tully* [1993] AC 45, 56E, Lord Templeman said that the CPS could not be bound against its wishes. "It must remain entirely a matter for the discretion of the prosecuting authorities as to whether they are in a position to and are prepared to give an assurance": *per* Lord Ackner at p 63H.

[427] In *AT & T Istel Ltd v Tully* [1993] AC 45 the plaintiffs obtained an order requiring the defendants to disclose information relating to dealings with certain assets in proceedings for fraud and breach of trust. A condition was attached to the order prohibiting the use of the material so disclosed in the prosecution of the defendants. The CPS made it clear that in any prosecution it would rely only on material obtained through sources other than the defendant's disclosure. The order was subsequently set aside on the ground that it infringed the defendants' privilege against self-incrimination. On appeal to the House of Lords it was held that, although the privilege against self-incrimination subsisted and could only be removed or altered by Parliament, there was no reason to allow a defendant in civil proceedings to rely on it where the defendant's own protection was adequately secured by other means, viz the CPS's statement that it would not rely on the defendant's disclosure.

[428] The Privilege Against Self-Incrimination in Civil Proceedings: A Consultation Paper (Lord Chancellor's Department, 1992).

[429] *Ibid*, at para 13.

[430] *Tate Access Floors Inc v Boswell* [1991] Ch 512.

[431] *Sociedade Nacional de Combustiveis de Angola UEE v Lundqvist* [1991] 2 QB 310, 338. The Court of Appeal deleted the part of an order which required the defendant to give details of the value of his overseas assets because there was a real risk that that information would provide a link in the chain of proof on charges of conspiracy to defraud.

8.19 The consultation paper proposed that the present privilege against self-incrimination should no longer apply in any civil proceedings, but should be replaced by a secondary privilege under which any self-incriminating statements or admissions given in evidence by a party or witness in civil proceedings could not be used against the witness in criminal proceedings. It was envisaged that this privilege would not need to be claimed until the prosecution sought to use the relevant information, in which case it would be for the court hearing the criminal proceedings to decide the issue of admissibility if the claim was disputed.[432] An alternative proposal was that section 72 of the Supreme Court Act 1981,[433] section 31 of the Theft Act 1968[434] and section 9 of the Criminal Damage Act 1971[435] should be consolidated so that they would be in the same form as section 72, and that this form of protection should extend to all proceedings involving an allegation of dishonesty.[436]

8.20 In December 1992, the Parliamentary Secretary for the Lord Chancellor's Department[437] announced that a large majority of respondents had supported the proposal that the privilege against self-incrimination should be abolished in civil proceedings, provided that appropriate provision was made to protect the witness in any subsequent criminal proceedings.[438] He stated that the Government intended to introduce legislation on this matter when a suitable opportunity arose, taking into account any related recommendations which might be made by the Royal Commission on Criminal Justice. When that Commission reported,[439] it did not deal with the privilege against self-incrimination, perhaps because it was only dealing with criminal justice and not civil proceedings. No legislation has as yet been introduced, but the matter has taken on a European dimension.

[432] The Privilege Against Self-Incrimination in Civil Proceedings: A Consultation Paper (Lord Chancellor's Department, 1992) para 30.

[433] See n 31 above.

[434] See n 20 above.

[435] The section provides:

> A person shall not be excused, by reason that to do so may incriminate that person or the wife or husband of that person of an offence under this Act –
>
> (a) from answering any question put to that person in proceedings for the recovery or administration of any property, for the execution of any trust or for an account of any property or dealings with property; or
>
> (b) from complying with any order made in any such proceedings;
>
> but no statement or admission made by a person in answering a question put or complying with an order made as aforesaid shall, in proceedings for an offence under this Act, be admissible in evidence against that person or (unless they married after the making of the statement or admission) against the wife or husband of that person.

[436] The Privilege Against Self-Incrimination in Civil Proceedings: A Consultation Paper (Lord Chancellor's Department, 1992) para 32.

[437] Mr John M Taylor MP.

[438] Written Answer, *Hansard* (HC) 17 December 1992, vol 216, col 350.

[439] (1993) Cm 2263.

### Developments in European law

8.21 Recent developments suggest that the privilege against self-incrimination is recognised both by the law of the European Union and by the European law of human rights. In *Orkem SA v The Commission*,[440] a limited company brought an action for the annulment of a decision of the European Commission requiring replies to questions set out in a request for information with which the applicant had failed to comply. The decision stated that the Commission was entitled to impose fines upon undertakings which provided incorrect information or failed to furnish information within the prescribed time limit. It was submitted that the Commission had used the decision to compel the applicant to incriminate itself by confessing to an infringement of the competition rules.

8.22 The European Court of Justice held that, since there was no right to remain silent expressly embodied in the relevant Regulation, it was appropriate to consider the general principles of Community law. The Court concluded that in general, the laws of the member states granted the right not to give evidence against oneself only to a *natural* person charged with an offence in *criminal* proceedings, as opposed to *legal* persons in relation to infringements in the *economic* sphere. However, the rights of the defence were a fundamental principle of the Community legal order,[441] and the Commission could not, by means of a decision calling for information, undermine the rights of defence of the undertaking concerned. Thus, the Commission could not compel an undertaking to provide it with answers which could involve an admission on its part of an infringement which it was incumbent upon the Commission to prove.

8.23 A similar conclusion has been reached on the basis of Article 6 of the European Convention on Human Rights ("the Convention"). The United Kingdom has an obligation in international law to conform its domestic law to the requirements of the Convention.[442] Article 6(1) provides, in part:

> In the determination of … any criminal charge against him, everyone is entitled to a fair and public hearing … by an independent and impartial tribunal … .

8.24 In *Funke v France*[443] the European Court of Human Rights held that Article 6 had been infringed where the applicant's conviction, secured by the French customs authorities in order to obtain certain documents which they believed to exist, was an attempt to compel the applicant himself to provide evidence of other offences he had allegedly committed. Furthermore, anyone "charged with a criminal

[440] Case 374/87 *Orkem v Commission of the European Communities* [1989] ECR 3283.

[441] Case 322/81 *NV Nederlandsche Banden-Industrie Michelin v Commission of the European Communities* [1983] ECR 3461, para 7.

[442] "The contracting parties have undertaken to ensure that their domestic legislation is compatible with the Convention and, if need be, to make any necessary adjustments to this end": European Convention on Human Rights, *Yearbook*, vol 2, p 234. In *Ireland v United Kingdom* (1978) 2 EHRR 25, the Court said at p 103, para 239: "By substituting the words 'shall secure' for the words 'undertake to secure' in the text of Article 1, the drafters of the Convention also intended to make it clear that the rights and freedoms set out in section 1 would be directly secured to anyone within the jurisdiction of the contracting States."

[443] (1993) 16 EHRR 297.

offence" within the meaning of Article 6 had the right to remain silent and not to incriminate himself. The applicant's conviction was an infringement of this right which the special features of French customs law did not justify.

8.25 More recently, the European Court of Human Rights has held in *Ernest Saunders v United Kingdom*[444] that there was an infringement of Article 6 where the applicant was compelled under the threat of two years' imprisonment[445] to answer questions put by investigators of the Department of Trade and Industry, which were thereafter used as evidence against him at his criminal trial pursuant to section 434(5) of the Companies Act 1985.[446] The Court drew a distinction between the use in criminal proceedings of "material which may be obtained from the accused through the use of compulsory powers but which has an existence independent of the will of the suspect such as, inter alia, *documents acquired pursuant to a warrant*, breath, blood and urine samples and bodily tissue for the purpose of DNA testing"[447] and the use of the accused's answers to questions. The Court rejected the argument that the complexity of corporate fraud and the vital public interest in the investigation of such fraud, and the punishment of those responsible, could justify a marked departure from Article 6.[448]

## The options for the privilege against self-incrimination for the proposed offence

### *Option 1: Allow a claim to privilege based on the risk of prosecution for the proposed offence*

8.26 The existence of the privilege prevents a witness from being faced with an unenviable choice – providing a truthful answer, and risking being punished for a crime; refusing to answer, and being punished for contempt of court; or giving an untruthful answer, in the hope of escaping detection and punishment both for the original crime and for perjury.[449] So it is said that the privilege encourages witnesses to come forward and give truthful evidence in civil proceedings without the fear of difficult decisions.

[444] (1997) 23 EHRR 313.

[445] Contempt of Court Act 1981, s 14.

[446] Under the Companies Act 1985, s 434, it is the duty of all officers and agents of the company under an investigation, to answer questions, produce documents and provide other assistance to inspectors of the Department of Trade and Industry appointed by the Secretary of State under s 432 to investigate the affairs of a company. Subsection (5) enables an answer given by a person to a question asked by an inspector to be used in evidence against that person. In *Re London United Investments plc* [1992] Ch 578 the court held that the examinee may not rely on the privilege against self-incrimination so as to refuse to answer questions.

[447] (1997) 23 EHRR 313, 338, para 69.

[448] The Court considered that "the general requirements of fairness contained in Article 6, including the right not to incriminate oneself, apply to criminal proceedings in respect of all types of criminal offences without distinction, from the most simple to the most complex": *ibid*, at p 340, para 74.

[449] The Privilege Against Self-Incrimination in Civil Proceedings: A Consultation Paper (Lord Chancellor's Department, 1992) para 3.

8.27 However, granting the privilege to witnesses who fear prosecution for dishonesty is arguably unfair to their victims. As we have said,[450] the courts have evolved a series of remedies (such as Anton Piller and Mareva injunctions) to ensure that these victims can obtain documents and information to pursue their claims, and that defendants do not dissipate their assets. But these remedies may not be available if there is a real risk that the information would provide a link in the chain of proof on a charge of conspiracy to defraud.[451] The privilege might also preclude ordinary discovery being given in a civil case, or enable a party to a civil action to refuse to answer questions at trial. The victims of acts of dishonesty would be prejudiced by the choice of this option, and the courts would be unable to get to the truth. Wrongdoers would be given an unjustifiable advantage.

8.28 These arguments might have less force if the courts could restrict the operation of the privilege by imposing conditions so as to prevent a witness's self-incriminating disclosure from being used in criminal proceedings. But it seems that this can only be done with the consent of the prosecuting authority.[452] Moreover, the witness would not be fully protected unless the prosecuting authority agreed not only to refrain from using the disclosed material itself, but also to prevent its use for the purposes of a *private* prosecution.

8.29 We provisionally reject this option.

### *Option 2: Not allow a claim to privilege based on the risk of prosecution for the proposed offence*

8.30 Under this option, a witness could not withhold information on the ground that it might implicate him or her in an offence of trade secret misuse. This would have the merit that there would be no further argument on the extent of the privilege or the consequences of invoking it. On the other hand, witnesses would have the unenviable choice we have described,[453] between giving a truthful answer and being punished for their crime, refusing to answer and being punished for contempt of court, or giving an untruthful answer in the hope of escaping detection and punishment both for the original crime and for perjury. Our provisional view is that this is an unattractive feature of this option.

8.31 This option would also contravene Article 6(1) of the Convention, because the European Court of Human Rights has stated that "the right to silence and the right not to incriminate oneself, are generally recognised international standards which lie at the heart of the notion of a fair procedure under Article 6".[454] It would entail the loss of what Lord Browne-Wilkinson has described as "one of the basic freedoms secured by English law".[455]

[450] See para 8.7 above.

[451] *Sociedade Nacional de Combustiveis de Angola UEE v Lundqvist* [1991] 2 QB 310, 338. See para 8.9 above.

[452] *AT & T Istel Ltd v Tully* [1993] AC 45; see nn 39 and 40 above.

[453] See para 8.26 above.

[454] See *Ernest Saunders v United Kingdom* (1997) 23 EHRR 313, 337, para 68; para 8.25 above.

[455] See para 8.3 above.

8.32 For these reasons, we provisionally reject this option.

### *Option 3: Extend section 72 of the Supreme Court Act 1981 to our proposed offence*

8.33 As we have seen,[456] section 72 of the Supreme Court Act 1981 creates an exception to the privilege against self-incrimination in the case of "any offence committed in connection with infringement of rights pertaining to any intellectual property or passing off, being an offence involving fraud or dishonesty", but protects the witness against the use of the information in any criminal proceedings (except for perjury or contempt of court). At present, some trade secrets (for example, those protected by intellectual property law) fall within section 72, but others (for example, the details of confidential tenders) do not. This option would involve extending section 72 to cover our proposed offence of trade secret misuse, thus ensuring that defendants would have the same protection in relation to that offence as for intellectual property offences of the kind already covered by the section. As we have said,[457] our view is that section 72 in its present form might extend to some examples of our proposed offence. But the section does not apply where the witness has adequate grounds to fear prosecution for conspiracy to defraud,[458] and this would be so even if it were extended to our proposed offence of trade secret misuse.

8.34 For these reasons, we provisionally reject this option.

### *Option 4: Extend section 72 of the Supreme Court Act 1981 to our proposed offence and to any conspiracy offence*

8.35 This option meets the two main difficulties. First, section 72 in its present form might not cover every case of our proposed offence. An amendment of section 72 would make it clear that the section does apply to every such case. Secondly, even if section 72 is amended to take account of our proposed offence, the same set of facts may found a charge of conspiracy. If the section were also amended to take account of statutory conspiracy and conspiracy to defraud, defendants would be unable to refuse disclosure on the ground that to do so would involve the "grave danger" or "real possibility" of prosecution for *those* offences.

8.36 This is our preferred option. We are encouraged to make it by the suggestion of the Vice-Chancellor in *Sociedade Nacional de Combustiveis de Angola UEE v Lundqvist*[459] that Parliament should consider removing the privilege

> in relation to all civil claims relating to property (including claims for damages) but on the terms that the statements made in documents disclosed are not admissible in any criminal proceedings, *including conspiracy to defraud whether under statute or at common law*.[460]

[456] See paras 8.13 – 8.14 above.

[457] See para 8.15 above.

[458] See *Tate Access Floors Inc v Boswell* [1991] Ch 512.

[459] [1991] 2 QB 310, 338F–G.

[460] Italics supplied.

8.37 **We provisionally propose that the definition of a "related offence" in section 72 of the Supreme Court Act 1981 be extended to include**

**(1) our proposed offence;**

**(2) any offence of conspiracy to commit**

**(a) an offence already qualifying as a "related offence", or**

**(b) our proposed offence; and**

**(3) any offence of conspiracy to defraud, in so far as the course of conduct agreed upon would, if carried out in accordance with the parties' intentions, have amounted to or involved**

**(a) an offence already qualifying as a "related offence", or**

**(b) our proposed offence.**

### THE RELATIONSHIP BETWEEN CIVIL AND CRIMINAL PROCEEDINGS

8.38 We now turn to consider whether civil proceedings should be stayed when criminal proceedings in respect of the same matters are expected or have actually been commenced. Every court has the power to stay proceedings on the ground that they are an abuse of the process of the court.[461]

8.39 The courts recognise that the right of a party to bring litigation to trial is fundamental, and should be interfered with only in limited circumstances. Not surprisingly, this power is exercised with great care, and only where there is a real risk of serious prejudice which may lead to injustice.[462]

8.40 Where a party in a civil action might, in that action, have to disclose his or her defence, with the result that he or she could be indicating a likely defence in contemporaneous criminal proceedings, the courts will not regard this as a sufficient reason to justify a stay.[463] In these circumstances, the courts have been anxious to ensure that both proceedings can continue, whilst protecting the defendant. When Ernest Saunders faced concurrent civil and criminal proceedings, Sir Nicolas Browne-Wilkinson V-C refused to stay the civil action, or any interlocutory proceedings in it, but directed that it should not come on for trial until after the criminal proceedings had been concluded, and that all interlocutory proceedings should be held in camera.[464] Our provisional view is that this approach

[461] *Re Norton's Settlement* [1908] 1 Ch 471. The power stems from the inherent jurisdiction of the court preserved by section 49(3) of the Supreme Court Act 1981, which is distinct from the jurisdiction conferred by the Rules of the Supreme Court. The two sources of the power continue to exist side by side: *Re Wickham, Morony v Taylor* (1887) 35 Ch D 272 (CA), *Halsbury's Laws of England*, vol 37 (4th ed 1982) para 442.

[462] *R v Panel on Takeovers and Mergers, ex p Fayed* [1992] BCC 524, 531D, *per* Neill LJ.

[463] *Jefferson Ltd v Bhetcha* [1979] 1 WLR 898.

[464] *Guinness plc v Saunders, The Times* 18 October 1988; *The Independent* 18 October 1988. In *Re DPR Futures Ltd* [1989] 1 WLR 778 the respondents were charged with conspiracy to defraud, while in civil proceedings the joint liquidators obtained interlocutory relief requiring the respondents to swear affidavits setting out what had become of certain monies, which were the subject of the criminal action. When the respondents applied for an order staying the civil proceedings until after the trial of the criminal proceedings, Millett J held that, while there was a risk of prejudice to the right of the respondent to a fair criminal

achieves a fair balance between the conflicting interests of the defendant and plaintiff in the civil action.

8.41 There could, however, be limited circumstances in which the discretion to stay the civil proceedings might be exercised. Megaw LJ gave the illustration of a civil action which was likely to obtain such publicity as to come to the knowledge of, and influence, persons who could be jurors in criminal proceedings.[465]

8.42 We are not aware of any criticism of the way in which the present law operates, and we do not think that the existence of criminal proceedings would interfere with the right of the owner of a trade secret to obtain redress in the civil courts. We would be interested to receive comments from respondents who would disagree with this.

8.43 **We provisionally propose that the new offence should be subject to the present powers of the court to stay civil proceedings if criminal proceedings for the same matter are expected or have actually been commenced.**

trial if the civil proceedings were heard before the criminal proceedings, there was no sufficient reason to stay the civil proceedings because the interests of the respondents could be safeguarded in other ways. Those safeguards included undertakings by the joint liquidators not to disclose the contents of any affidavit or document disclosed (save with the prior written consent of the solicitors of the respondent or the leave of the court) and by directing that all future interlocutory proceedings should be held in camera, that the civil case should not be set down for hearing without the leave of the court, and that steps should be taken to ensure that the trial of the civil proceedings would not take place before the conclusion of the criminal proceedings.

[465] *Jefferson Ltd v Bhetcha* [1979] 1 WLR 898, 905.

# PART IX
# SUMMARY OF PROVISIONAL CONCLUSIONS, PROPOSALS AND CONSULTATION ISSUES

In this Part we summarise our provisional conclusions and proposals, and other issues on which we seek respondents' views. More generally, we invite comments on *any* of the matters contained in, or the issues raised by, this paper, and any other suggestions that consultees may wish to put forward. **For the purpose of analysing the responses it would be very helpful if, as far as possible, consultees could refer to the numbering of the paragraphs in this summary.**

### THE NEED FOR A NEW OFFENCE

9.1 We provisionally conclude that the main arguments in favour of criminalising trade secret misuse are as follows:

(1) that there is no distinction in principle between the harm caused by such misuse and the harm caused by theft;

(2) that the imposition of legal sanctions is necessary in order to protect investment in research;

(3) that civil remedies alone are insufficient to discourage trade secret misuse (and would continue to be insufficient even if exemplary damages were made more widely available), because many wrongdoers are unable to satisfy any judgment against them**;** infringement of copyright and registered trade marks but not the misuse of

(4) that it is inconsistent for the law to prohibit the trade secrets; and

(5) that criminalisation would help to preserve standards in business life.

(paragraph 3.60)

9.2 We provisionally propose that the unauthorised use or disclosure of a trade secret should, in certain circumstances, be an offence.

(paragraph 3.61)

### THE DEFINITION OF A TRADE SECRET

9.3 We provisionally conclude that, for the purpose of any new offence of trade secret misuse, it would be necessary to provide a definition of a trade secret.

(paragraph 4.5)

9.4 We provisionally propose that the definition of a trade secret should include a requirement that its owner has indicated, expressly or impliedly, a wish to keep it secret.

(paragraph 4.18)

9.5 We ask for views on whether the definition of a trade secret should include a requirement that its owner has taken steps to keep it secret.

(paragraph 4.22)

9.6 We invite views on

(1) whether the definition of a trade secret should make reference to the use of the information in a trade or business; and

(2) if so, whether the definition should extend to

(a) information used in a profession, or

(b) "pure" (non-commercial) research.

(paragraph 4.28)

9.7 We provisionally propose that it should be an element of the definition of a trade secret that the information is not generally known.

(paragraph 4.29)

9.8 We provisionally propose that, for the purpose of the requirement that the information is not generally known, the expression "generally known" should be (partially) defined in terms similar to the definition of "information in the public domain" in the draft Bill annexed to our Breach of Confidence report (Law Com No 110).

(paragraph 4.33)

9.9 We provisionally propose that the prosecution should not have to establish that the information was not generally known unless there is some evidence that it was.

(paragraph 4.34)

9.10 We provisionally propose that it should be an element of the definition of a trade secret that the information should have some economic value which derives from the fact that it is not generally known.

(paragraph 4.35)

9.11 We invite views on the extent, if any, to which the definition of a trade secret should include a reference to specific forms of information.

(paragraph 4.40)

## THE ELEMENTS OF THE PROPOSED OFFENCE

### Use or disclosure

9.12 We provisionally propose that the new offence should be committed by a person who uses or discloses a trade secret belonging to another without that other's consent.

(paragraph 5.3)

**To whom does a trade secret belong?**

9.13 We provisionally propose that a trade secret should be regarded as belonging to anyone entitled to the benefit of it.

(paragraph 5.4)

**Consent obtained by deception**

9.14 We provisionally propose that consent to the use or disclosure of a trade secret should not negative liability for the offence if it is obtained by deception.

(paragraph 5.7)

**The mental element**

9.15 We provisionally propose that it should be an element of the new offence that the defendant

(1) knows that the information in question is a trade secret belonging to another, and

(2) is aware that that other does not, or may not, consent to the use or disclosure in question.

(paragraph 5.8)

9.16 We provisionally propose that a person should not commit an offence by using or disclosing a trade secret in the belief that every person to whom the secret belongs would consent to that use or disclosure if he or she knew of it and the circumstances of it.

(paragraph 5.9)

**Mode of trial**

9.17 We provisionally propose that the new offence should be triable only on indictment.

(paragraph 5.11)

**Consent to prosecution**

9.18 We provisionally propose that prosecutions for the new offence should be brought only by or with the consent of the Director of Public Prosecutions.

(paragraph 5.15)

**Threats to prosecute**

9.19 We invite views on

(1) whether there should be a remedy for unjustified threats to prosecute for the proposed new offence;

(2) if so, whether the remedy should be civil or criminal;

(3) what conditions should be satisfied before proceedings can be brought; and

(4) what defences should be available.

(paragraph 5.17)

### Prospective effect

9.20 We provisionally propose that the offence should have prospective effect only.

(paragraph 5.18)

## EXCLUSIONS

### Employees

9.21 We provisionally propose that the new offence should not extend to the use or disclosure of information which, under the law of confidence, constitutes the enhancement of an employee's (or independent contractor's) personal knowledge, skill or experience.

(paragraph 6.6)

9.22 We provisionally conclude that employees should not be automatically excluded from the offence.

(paragraph 6.11)

### Acquisition by independent development

9.23 We provisionally propose that the new offence should not extend to the use or disclosure of information acquired by independent development.

(paragraph 6.12)

### Reverse engineering

9.24 We provisionally propose that the new offence should not extend to the use or disclosure of information acquired solely by reverse engineering.

(paragraph 6.15)

### Information available from another source

9.25 We provisionally conclude that, where information otherwise falls within the definition of a trade secret, the fact that it was available from another source at the material time should not exclude liability.

(paragraph 6.18)

### Innocent third parties

9.26 We provisionally propose that the new offence should not extend to the use or disclosure of information by a person who, at the time of acquiring the information (whether or not for value),

(1) did not know that it was a trade secret belonging to another, or

(2) was not aware that that other did not, or might not, consent to that acquisition (or believed that that other would consent to it if he or she knew of it and the circumstances of it),

unless that person was at that time aware that its acquisition by any other person from whom he or she (directly or indirectly) acquired it had (or may have) involved the commission by any person of

(a) an indictable offence, or

(b) an offence contrary to section 1 of the Computer Misuse Act 1990.

(paragraph 6.28)

**Public interest**

9.27 We provisionally propose that the new offence should not extend to

(1) the use, or the disclosure to an appropriate person, of information for the purpose of the prevention, detection or exposure of

(a) a crime, a fraud or a breach of statutory duty, whether committed or contemplated;

(b) conduct which is in the nature of a fraud on the general public; or

(c) matters constituting a present or future threat to the health or welfare of the community; or

(2) any use or disclosure of information which, under the law of confidence, would be justified on grounds of public interest.

(paragraph 6.54)

**Disclosure in accordance with a statutory obligation or power**

9.28 We provisionally propose that the new offence should not extend to any disclosure of information made by a person who, by statute or subordinate legislation, is obliged or permitted to make it.

(paragraph 6.56)

**Legal proceedings**

9.29 We provisionally propose that the new offence should not extend to the disclosure of information pursuant to a court order, or otherwise in, or for the purpose of, civil or criminal legal proceedings.

(paragraph 6.57)

**The police, security services and prosecuting authorities**

9.30 We provisionally propose that the new offence should not extend to the use or disclosure, in the lawful exercise of an official function in regard to national security or the prevention, investigation or prosecution of crime, of information obtained in the lawful exercise of any such function.

(paragraph 6.58)

**ACQUISITION OF A TRADE SECRET**

9.31 We invite views on

(1) whether the criminal law should be extended so as to cover the acquisition of a trade secret; and, if so,

(2) whether this should be done by creating

(a) an offence of acquiring a trade secret with the intention of using or disclosing it;

(b) an offence of acquiring a trade secret by wrongful methods; or

(c) an offence defined in some other way, and if so what.

(paragraph 7.31)

**THE RELATIONSHIP BETWEEN CIVIL AND CRIMINAL PROCEEDINGS FOR TRADE SECRET MISUSE**

9.32 We provisionally propose that the definition of a "related offence" in section 72 of the Supreme Court Act 1981 be extended to include

(1) our proposed offence;

(2) any offence of conspiracy to commit

(a) an offence already qualifying as a "related offence", or

(b) our proposed offence; and

(3) any offence of conspiracy to defraud, in so far as the course of conduct agreed upon would, if carried out in accordance with the parties' intentions, have amounted to or involved

(a) an offence already qualifying as a "related offence", or

(b) our proposed offence.

(paragraph 8.37)

9.33 We provisionally propose that the new offence should be subject to the present powers of the court to stay civil proceedings if criminal proceedings for the same matter are expected or have actually been commenced.

(paragraph 8.43)