Industrial Espionage: What Can the Law Do?

*Victor Tunkel**

The NCP case

On March 12 1993 there ended what *The Times* [1] described as Britain's biggest industrial espionage trial, *R* v. *Layton & Others*. The case was heard over a period of eight weeks at the Old Bailey. What this must have cost the parties and the taxpayer can only be guessed. The bill for the police investigation alone was estimated to be £4 million. Since the case ended in acquittals for all concerned it will not get into the law reports or the annals of crime and any lessons which might be learned from it are likely to be forgotten.

The allegations in the case, which were not disputed at the trial, are a useful illustration of some of the machinations currently practised by business spies and saboteurs. The defendant, Mr. Layton, was the chief executive of National Car Parks (NCP). His co-defendant, Mr. Hewitt, was the manager of KAS, described as a security agency. Their target was a rival car park company, Europarks. It appears that Europarks, a newcomer to the car parking scene, were scooping the most lucrative concessions, *e.g.* Heathrow Terminal 4 and the South Bank Centre, which until then NCP would have been able to command. Mr. Layton, disconcerted by this competition, thought that there might be a mole in his own company who was leaking information to Europarks. He therefore called in KAS. KAS was set up by the late Sir David Stirling, founder of the SAS, to be a sort of civilian equivalent. Many of its "operatives" were ex-SAS. Indeed, some were recalled to the colours for Desert Storm.

KAS were unable to detect any mole in NCP. Mr. Layton therefore asked them to investigate Europarks. They went to work in military style. They managed to install one of their operatives as a car park manager wth Europarks for 3 months. He passed information, 36 reports in all, to NCP; obtained information about Europarks' customers and their cars; obtained the number of a safe; rifled the briefcase and wallet of a Europark executive; took files from their office which were copied and returned. He also tried to whip up unrest among Europark staff. Europark dustbins were searched and useful waste extracted. Europark directors were shadowed, their homes watched and their families photographed. By means of a false *c.v.*, KAS got Jane Turpin,

* Queen Mary & Westfield College, University of London.

1. *The Times* March 13, 1993. Also *The Independent, Guardian, Financial Times.*

a former Captain in the Royal Signals, the job of personal assistant to the managing director of Europarks. She thus gained access to the company's most confidential documents of which she took copies, and to financial information, all relevant to KAS.

The end of the affair was something of an anti-climax. The intelligence which finally emerged from all this spying was simply that Europarks had been successful through undercutting NCP. As for the stalking of Europarks, this came to light when Mr. Hewitt, aggrieved at being dismissed by KAS when the agency fell on hard times, went and blew the whistle to the *Sunday Times*. This led to a civil action by Europarks against NCP which was settled by NCP in effect buying out their competitor for £5 million.

A prosecution then began. The main charges were against Layton and Hewitt for conspiracy to defraud Europarks by dishonestly acquiring information about its business affairs. (A charge against Miss Turpin of obtaining pecuniary advantage, namely the job, by deception, was for medical reasons not proceeded with, and so Mr. Hewitt was formally acquitted of abetting her.) Neither Layton nor Hewitt gave evidence. Their lawyers argued that neither defendant believed he was breaking the law or was dishonest; that Mr. Layton in employing KAS had been assured that only legal means would be used. In particular he specifically ruled out any electronic surveillance.

Thereafter he was unaware of KAS's methods, save that he knew of Miss Turpin's infiltration. Presumably if he expressly stipulated KAS should act only legally, he must have meant non-criminally; it would not be hard to establish breaches of contract and various torts by KAS operatives. However even if such civil wrongs were foreseen and acquiesced in by Mr. Layton, there would be no statutory criminal conspiracy since the Criminal Law Act 1977 abolished the common law crime of conspiracy to commit a tort.

The Crown therefore resorted to charging conspiracy to defraud. However that crime remains shrouded in all its unreformed common law uncertainty. We know that "defrauding" clearly extends to conduct not in itself criminal, including some inflictions of economic harm, and that it does not require deception. In the leading case, *Scott* v. *Comr. of Police for the Metropolis,* [2] the House of Lords specified dishonestly depriving a person of something which is his; or dishonestly injuring some proprietary right of his. It is conceivable that Mr. Layton, in employing KAS to find out by "only legal means" all they could about Europarks, intended in so doing neither to deprive, nor to injure any proprietary right. The Crown agreed that there was no evidence that Europarks had suffered any loss. It is true that in *Wai Yu-tsang* v. *R* [3] the Privy Council upheld a direction that "If . . . the economic or proprietary interests of some other person are imperilled, that is sufficient to constitute fraud even though no loss is actually suffered and even though the fraudsman himself did not desire to bring about any loss", following the case of *R* v. *Allsop*.[4] However

2. [1975] A.C. 819.
3. [1991] 4 All E.R. 664.
4. (1976) 64 Cr. App.R.29 (C.A.)

these remarks have to be seen in context. The two cases were conspiracies to defraud involving the deceiving of the victim into adopting a course of conduct which put him at financial risk; and the question was whether recklessness as to prejudicing the victim would suffice. Mr. Layton could say that he foresaw no peril from the act of getting information itself; that he might not find out anything of use; and that if he did, and if he then chose to use it subsequently in giving NPC a competitive edge over Europarks, that was no part of the conspiracy charged. Finally, there is the overriding requirement of "dishonesty" which has been much debated in Theft Act cases. The Privy Council in *Wai Yu-tsang* felt it necessary to add: "Of course, if the conspirators were not acting dishonestly, there will have been no conspiracy to defraud . . ."[5] Whatever this may amount to in practice, it of course follows that if as in this case there are only two alleged conspirators, a finding of non-dishonesty in one puts an end to the guilt of both.

The use of conspiracy

Whatever the moral merits of the arguments, it must be clear that the crime of conspiracy to defraud is too ill-defined and imprecise to deal with industrial espionage. The acquittal of the accused after their eight-week trial speaks for itself. The Law Commission have been labouring for years to create a new specific offence of defrauding, so that any conspiring to do it would become normal statutory conspiracy under the 1977 Act. Whether they will come up with something which catches industrial espionage in all its present and foreseeable manifestations may be doubted. A different solution is offered in conclusion below. However, before leaving the present law we should inquire whether sufficient other crimes exist such as may be effective against at least some aspects of this activity.

The use of theft

The layman might well call it theft. But as every law student would tell him, in the NCP case there was neither the *actus reus* nor the *mens rea* for theft. Firstly, there was no "property belonging to another" appropriated. The true gravamen, dishonestly obtaining information, is not touched by the Theft Acts: one cannot steal facts. The law was settled in *Oxford* v. *Moss*[6] where a sneak preview by a university student of a forthcoming exam paper was held not to be theft. However valuable know-how may be as a matter of everyday commerce, it is not for theft purposes "property". Secondly, even if it were so regarded, the KAS spies had no intention of depriving but only of sharing it. There was no intention of keeping e.g. the contents of files or brief-cases, if for no other reason because this would lead to discovery. One could say that the spy's intention is to permanently deprive the owner (and any other authorised users) of exclusivity. So far no one in England appears to have argued that the right of exclusivity could be "intangible property" within Theft Act s.4 and it is very doubtful if any court would now entertain that proposition. Moreover to make

5. [1991] 4 All E.R. at 672c.
6. (1978) 68 Cr. App.R.183.

information stealable would raise a further crop of problems in relation, for example, to what might constitute subsequent "handling" of such information by others, or to the retention and use of the information by ex-employees.

Other crimes

Against some business spying, one might have thought that that old warrior the Wireless Telegraphy Act 1949 could be invoked. Since unlicensed radio transmission and receiving of unauthorised signals are offences, it is strange that the manufacture, sale and use of bugging devices is not more tightly controlled. Suffice it to say that such devices are on public sale and widely advertised. More specifically, the Interception of Communications Act 1985 s.1 creates the crime of unlawful interception of communications either through the post or through any public telecommunications system. So bugging the victim's phone or Fax machine would be an offence but not bugging his office or boardroom. The real point of the Act was to preserve some degree of civil liberty by controlling official bugging by police and intelligence services, not to deal with private eavesdroppers.

The Computer Misuse Act 1990 looks more promising. Section 1 makes unauthorisedly accessing a computer an offence. Largely aimed at the nuisance of hackers, it extends to intruders with more sinister motives. However the accused must be shown to have "caused the computer to perform a function". The in-house spy who reads the screen over the authorised operator's shoulder is therefore not caught. Moreover the s.1 offence is summary only, not much of a threat; and the aggravated s.2 offence, by requiring an ulterior serious criminal intent, begs the fundamental question and is unlikely to be satisfied in the case of the typical industrial spy. The overt shadowing of people or watching and besetting their premises for purposes of harassment or sabotage could be caught by s.7 Conspiracy and Protection of Property Act 1875. However, this old Act, hardly ever used even against the brazen paparazzi who besiege the homes of the famous, has no application to covert operations. Obtaining pecuniary advantage by deception under Theft Act 1968 s.16(2)(c) may have a limited part to play where, e.g. moles are planted in a rival organisation; but of course it may not have been necessary to make any untrue statement in achieving a plant. As for invasions of privacy, the public debate generated by recent press intrusions looks like resulting in legislation. But this may be based in civil law only, and anyway may be couched in terms of private lives rather than businesses. Some proposals have been published and more are expected. These are mentioned below.

It seems clear that these miscellaneous weapons that the criminal law offers against industrial espionage are at best effective only against some methods optional to its perpetrators. Against the activity as such there is no general prohibition. Victims must have recourse to their civil remedies, mainly through actions for breach of confidence. The scope of such actions, though still capable of development, has been described by the Law Commission as "glaringly inadequate".[7]

7. Law Com. 110 (1981). This is considered further below.

The need for legislation

Do we want more specific and rigorous legal control? Does industrial espionage pose a sufficient economic or social threat to warrant it? We frequently read of huge losses caused to legitimate businesses by successful espionage. How accurate some of these figures are and how much is mere journalistic guesswork is impossible to say. One difficulty in arriving at a reliable estimate is that espionage, unless it extends to blatant sabotage, may often go undetected; not merely as to the identity of the spymaster, the mole or their ultimate instigator, but even that it has occurred. Enterprises fail because someone else does it cheaper or better, and there may be no way of knowing exactly how or why their competitor prevailed. Another common difficulty is the reluctance of the target business to admit their security has been breached and their know-how filched, either from embarrassment or through not wanting the intruders to know that they know.

Moreover industrial espionage may provoke undesirable yet understandable reactions: counter-espionage in both the defensive and the retaliatory sense. While the security industry may be seen as generating some useful employment and technical innovation, the social or economic benefit of these is surely outweighed by the extra costs of businesses having to protect themselves, which are ultimately borne by customers and consumers. Besides which, it should be a matter of concern that so many former members of the SAS, intelligence services, customs and police are now being snapped up for "civilian" employment.[8] Beyond all these economic and social considerations is the decent and reputable trader's sense of helplessness and lack of protection in the face of dishonest and unfair competition. That sense of helplessness has always been one of the mainsprings of the motivation to criminalise rather than leave individuals to pursue their civil remedy or to resort to self-help. I suggest that taken together these make a strong case for specific prohibition.

Other countries' experience

One might have thought that since industrial espionage is a world-wide activity, other countries might have found more effective ways of dealing with it. However recent cases and legislative efforts from the common law world do not seem to provide us with much of a lead.

Australia: the case of *Warman International* v. *Envirotech Australia*[9] is instructive. The plaintiffs manufactured and supplied slurry pumps and had 90% of the Australian market. They produced and supplied to their employees technical manuals, data and drawings. Two long-serving employees, S and W, left the plaintiffs and went to work for the defendants, an American subsidiary beginning to compete with the plaintiffs

8. Personnel at all levels are recruited. The former deputy head of MI6 retired aged 57 to join Group 4: *The Times* May 26, 1993. The ex-Commissioner of the Metropolitan Police, Sir Peter Imbert, joined another SAS-inspired organisation, Integrated Security Systems: *The Independent* May 31, 1993.
9. (1986) 67 A.L.R. 253 (Australian Federal Court, Wilcox J).

in the Australian market. A third employee, M, subsequently also left the plaintiffs for the defendants, where he saw copies of the plaintiffs' manuals and drawings in the possession of S and W. When issuing these to customers, M was instructed to block out the plaintiffs' name. M (a counter-mole?) reported these happenings to the plaintiffs. Their general manager then did some counter-espionage by prospecting on Sundays in the defendants' dust-bins. He removed three bag-loads of refuse, in which were found pages from the plaintiffs' manuals and drawings which could be proved to have been supplied to S.

Warman brought civil proceedings, alleging breach of copyright, breach of confidentiality and also invoking various Australian statutes. Much of the argument in the Federal Court concerned the availability of the privilege against self-incrimination in resistance to the Anton Piller order in the case.[10] Wilcox J found S and W in breach of their duty of confidence to Warmans in making the documents available to Eurotech, and that company liable with them as a joint tortfeasor for knowingly using the documents. Saying "the term 'commercial theft' is not too harsh a description" of their activities, he issued injunctions and restraining orders against them. Apart from showing how readily espionage provokes counter-measures, and the necessity of the victim to have to do all the detective work and to pursue multifarious causes of action with no guarantees of success, the case indicates a further type of espionage activity which is difficult, perhaps impossible, to outlaw: the headhunting of competitors' employees in order to gain their confidential knowledge. If W and S had restricted themselves to passing on their knowledge and expertise, however confidentially acquired, it would have been impossible to bring the case home to their instigator.[11]

United States: A different but just as narrow approach was taken by the American prosecuting authorities in *Carpenter* v. *US.*[12] Winans and Carpenter were responsible for a daily column "Heard on the Street" in the *Wall Street Journal.* This was based on information obtained by talking to well-placed and knowledgeable people in the business world. The column was very influential and readers tended to invest in reliance on it. Winans and Carpenter entered into a scheme with two stockbrokers to give them advance information of the column's content, so that they were able to anticipate the market movement which would follow publication, making a profit which they shared with the columnists. The prosecution relied on what might be thought to be

10. In England this privilege, successfully raised against an Anton Piller order in *Rank Film Distributors* v. *Video Information Centre* [1982] A.C. 380 (H.L.), was promptly removed in any such future confrontations by Supreme Court Act 1981 s.72.

11. Allegations of conduct similar to those in the *Warman* case (note 9, above) were made against the production chief of Volkswagen when he joined that company shortly after leaving General Motors. A team of 40 prosecution officials raided VW's offices in 11 different locations to look for GM documents: *The Times* August 27, 1993.

12. (1987) 484 U.S. 19; 98 L.Ed. 2d. 275.

a wholly peripheral fact, that the conspirators had communicated by post, wire, radio or television. This was necessary to bring them within the federal mail and wire fraud statutes which prohibit the use of these media for any scheme to defraud of money or property.[13] The US Supreme Court accepted the argument that the information was confidential to the newspaper prior to publication; that defrauding simply meant wronging someone in his property rights by dishonest methods or schemes; and that it had therefore been defrauded even though it had suffered no monetary loss because it had been deprived of a property right, namely the right to make exclusive use of the information prior to publication.

To the English reader at least, the grounds and the reasoning will seem equally strained. Apart from the irrelevant underlying requirement of the media of communication, there was the artificiality of the supposed "defrauding" of some "property" when in reality there was no quantifiable loss to or wronging of the newspaper, save perhaps temporarily in its reputation. The real gravamen lay in the dishonest profiting from manipulation of the market caused by the defendants' self-fulfilling prophecies. In the UK this would perhaps be an offence under the Financial Services Act 1986 s.47, or the new insider dealing provisions of the Criminal Justice Act 1993. That is not to say, however, that it should be beyond the reach of an effective law to protect such confidential price-sensitive information from selective disclosure. The mistake here (and in some of the reform proposals: see later) is the law's result-approach rather than a conduct-approach.

Canada: The information in the *NCP* and *Warman* cases was intrinsically of commercial value. The need to protect a still wider range of business information is shown by the case of *Stewart* v. *The Queen.*[14] The Constellation Hotel, Toronto, had about 600 employees. A trade union wanted to organise them but was unable to get their names and addresses because the management's policy was to keep this information confidential. Stewart was therefore hired to obtain the information. He approached one of the hotel's security guards, H, offering him a bribe to obtain the hotel's staff list. H reported this to the security chief and to the police. Stewart was charged with counselling theft and counselling fraud, as defined in the Canadian Criminal Code. The Supreme Court of Canada held that for theft there must be something capable of proprietary right and capable of being taken so as to amount to deprivation; and that confidential information does not satisfy these requirements. For fraud, the Code calls for prejudice to "property, money or valuable security".[15] Since the hotel had no intention to deal with this confidential information in a commercial way, Stewart's incitement of H was not counselling fraud.

Again, it would be possible in England to find an existing crime to deal with this sort of activity: the Prevention of Corruption Act 1906 would apply, irrespective

13. 18 U.S.C.S. 1341, 1343.
14. (1988) 50 D.L.R. (4th.) 1.
15. S.338.

of what the subject-matter was and of success or failure. This only reinforces my suggestion that a new and unfettered conduct-crime is called for, which will cover the whole field.

Existing reform suggestions

Having seen in these recent cases some of the forms which industrial espionage can take and the inadequacy of the law to deal with it, we now need to look at prevalent reform ideas.

Attempts to reform the law have been rather tentative. Some US jurisdictions[16] have simply extended the definition of "property", leaving it to their existing theft-related offences to do the rest. For reasons given earlier, I suspect that prosecutions on this basis will either fail for lack of theftuous *mens rea*, or if they succeed will raise a whole new crop of problems.

J T Cross[17] commends with reservations the more specific approach of the Alberta Law Institute. They have proposed making it a crime for any person who ". . . fraudulently and without colour or right acquires, discloses or uses the trade secret of another person" with intent to deprive of either control or of "economic advantage associated with the trade secret". A second proposed offence would criminalise fraudulently inducing an owner to disclose a trade secret; and there would be a lesser punishment where in either offence the defendant was negligently unaware that it was a trade secret. One could have hoped that the *Stewart* case would have shown "trade secret" to be too limited a category of what requires protection; and anyway, the narrowness of the range of activity caught by this proposal must be obvious. Attempts and other preliminary crimes should be built-in, not left to be grafted on uncertainly by the common law. And with all this, the likelihood is that all sorts of associated conduct would still escape: surveillance, planting moles, etc. The use of "fraudulently" is not very helpful.

In the UK there have been various law reform proposals over the years. The Younger Committee[18] recommended in 1972 that there be a new offence of "surreptitious surveillance". The Scottish Law Commission[19] in 1977 proposed criminal offences of (1) entry of premises, or searching or examining property, without consent or authority to obtain confidential information or information of value; and (2) the use of certain surveillance devices. These offences, though still too narrow, show a tendency towards the more appropriate emphasis on conduct rather than results.

The English Law Commission in 1979 were asked "to consider the law relating to the disclosure or use of information in breach of confidentiality and to advise what

16. For a fuller survey, especially of US and Canadian developments, see articles by JT Cross: "Trade Secrets, Confidential Information and the Criminal Law" 36 McGill LawJo.524; and "Protecting Confidential Information under the Criminal Law of Fraud and Theft" 11 O.J.L.S. 264 (1991).
17. In McGill LawJo. article (previous note).
18. Report of the Committee on Privacy, Cmnd.5012 (1972).
19. Memorandum 40.

statutory provisions are required to clarify or improve it." They were also asked to propose remedies for loss caused by such breaches. Despite these seemingly wide and general terms of reference, they appear to have assumed that they were confined to civil law matters. Their Report[20] proposed a new statutory tort to replace the present inadequate common law. They appended a draft Breach of Confidence Bill dealing with improperly acquiring information not in the public domain, and the methods of acquisition include unauthorised taking, handling, copying, deception, surveillance, or just being somewhere without authority. The subject-matter protected is wide, going well beyond commercial information. But the range of activities is limited as in previous examples of reform; and in leaving all the initiatives and expense to be undertaken by the aggrieved target, whether corporate or individual, one of the essential shortcomings of the present law remains. The report has not been adopted, though the government is now considering implementation of some parts of it.

Most recently, the Lord Chancellor's Department has issued a consultation paper, *Infringement of Privacy.*[21] The paper presents a useful survey of all the previous efforts to protect confidentiality by creating new torts of crimes. However it is only concerned with the protection of personal privacy, and only by means of a proposed new civil action. At the time of writing a further government white paper from the Department of the National Heritage is awaited. This will be in response to the Fourth Report of the National Heritage Select Committee,[22] and therefore may be expected to contain some at least of the criminal offences proposed by the Calcutt Report.[23] These however are about media intrusions into private lives. Calcutt recommended three new crimes: for the purpose of obtaining personal information with a view to publication, either entering private property, or placing a surveillance device there, or photographing or recording there, without the appropriate consent. It is likely that some legislation along these lines will be enacted before long. If not requiring the intent to publish, it could be of some marginal use against some industrial espionage. However in view of its original motivation to curb the excesses of the tabloids and the protection of individuals in their private capacity ("private property" is defined in residential terms), the legislation is unlikely to offer protection to business and industrial information.

A proposal for an Industrial Espionage Act

It seems to me that in the light of the recent cases and such reform proposals as have so far emerged, the only way to deal with industrial espionage is by specific legislation. This would have to encompass the types of activity now known to be practised and all further ones so far as they can be foreseen. For reasons we have seen, such legislation

20. Law Co. 110, Cmnd.8388 (1981).
21. July 1993.
22. Privacy and Media Intrusion 294-1 (March 1993).
23. Report of the Committee on Privacy and Related Matters' Cm. 1102 (1990).

will fail if it is framed so as to create result-crimes. It is the activity and its intent, irrespective of success or failure, that must be proscribed. At present business spies may calculate that they will achieve their purpose long before the law's intervention, if any. To deter them, and to counterbalance this gamble on success, the criminal law should be effective at a very early stage. The words of the Calcutt Report in relation to prying on privacy are surely just as applicable to prying into businesses.

"The main desire of a victim . . . is for the intrusion to be stopped immediately. . . . While, in some cases, the civil law can be brought quickly to bear by obtaining an injunction, this remedy cannot realistically be described as instant. . . . Only the criminal law can guarantee prompt relief for the victim and provide a sufficient deterrent to the intruder."[24]

What needs to be criminalised is the essential espionage activity, the attempt to gain confidential information; and this should include attempts to get such information from third parties who happen to hold it, for example the tax authorities, police or customs.

At the same time some consideration should be given to outlawing the related activity of industrial sabotage. The type of "dirty-tricks" campaign, for example as alleged in the current Virgin Atlantic and British Airways dispute,[25] may also involve information-gathering, surveillance, etc. But it need not do so, and anyway requires to be dealt with separately. In order, however, not to hinder what may perhaps be sharp but still permissible competition, the interference proscribed would be such as was directed against existing legal relationships and obligations and not, for example, towards potential customers or potential employees of a competitor. Similarly headhunting the employees of a rival for the sake of their knowledge would not without more be an offence unless it involved their breaking their existing contracts. Pretended headhunting, where a rival's employee is interviewed for a job merely to gain information, and where no job is really on offer, should be caught, but proof might be difficult.

As with all criminalising legislation, the choice lies between a wide-ranging general prohibition which is left to prosecutorial discretion and to the courts to flesh out; and a more precisely categorised provision. Each approach has its drawbacks, but the need for certainty in proscribing business activity previously considered lawful calls for precise targeting, not a catch-all in generalities easily holed by defence lawyers. I therefore offer the draft clauses set out in the Annex below, with a list-approach which indicates both the genera and species and which is not exhaustive.

Three legitimate activities which may foreseeably overlap the prohibitions are

24. *Ibid.*, paragraph 6.30.

25. Although characterised as the villain in the Virgin affair, British Airways have themselves more recently been a victim. Its rights issue of May 1993 was leaked, leading to a Stock Exchange inquiry. The Chairman, Sir Colin Marshall, is reported as saying: "I wish we could explain it. We do not know how it happened. Our board has asked for an inquiry." *The Times* May 26, 1993.

specifically excluded: industrial disputes, investigative journalism, and "knocking-copy" advertising. Press diggings into private lives have already been mentioned. In so far as they may be legitimate, legislation now in contemplation may be expected to provide for defences. But it is important that the media's probings of the business world should not be inhibited, either under the guise of privacy protection or the stigma of industrial espionage. This is avoided by clause 4(b). Hostile advertising is best left to self-regulation. In so far as it might be caught by clause 3(b), it likewise is put outside the Bill by 4(b).

Generally excluded are any activities which are not "dishonest". That word has survived a quarter of a century of probing by criminal lawyers and although its interpretations have not pleased everyone, I suggest that it has attained a plateau of acceptability which makes it the most useful word available. There will always be a grey area on which opinions may differ as to what is a legitimate (if disreputable) competitive tactic and what is intolerable. Such uncertain and shifting boundaries in commercial ethics are inevitable and no better way of judging these in the criminal context has been found than by recourse to the reasonable informed juror's concept of dishonesty. Having said that, it needs to be made clear that once espionage is outlawed, there must be no recourse to self-help of the sort we have seen in some of the cases. A defendant who pleads "defensive" espionage may nevertheless be found to be dishonest, depending on the circumstances. This is provided for in clause 5. Extra-territorial activity would be included by virtue of the Criminal Justice Act 1993. Finally, there is the overriding safeguard of the DPP's consent.