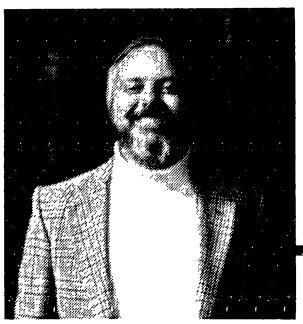
support therefore comes from informed individuals, commercial and industrial undertakings whom we have convinced that donations to NICRO should more correctly be regarded as environmental investments made for reasons of enlightened self interest. We believe that by placing greater emphasis on the prevention of crime, while not reducing our rehabilitative services to offenders, we in fact enhance our ability to compete in the "donations market". Certainly our ability to have initiated and financed 6 community work posts in two years gives this statement credance. Nevertheless this response and our general financial position remains precarious and a serious problem, which severely restricts the role that our national crime problem demands we fulfill.

This overview of NICRO as an African Organisation and the response it has made to better serve the rapidly developing nation within which it operates is for us an exciting development. It is a development, a beginning, and as such it has raised our expectations of being more successful in grappling with the complexities of crime in a nation of extraordinary diversity. Through the broader approach we have initiated we hope to recover an aspect of our functioning which was a feature of our service until 40 years ago. From our foundation in 1910 and until 1937, when we appointed our first social worker, all the work of the organisation was undertaken by committed volunteers. Since 1937 our pace in appointing professionals to do the job quickened and has resulted, undoubtedly in an improved quality and content of service, but it has also resulted in the volunteer taking a behind the scenes role. As such his numbers have declined and his interest has waned. It is this which we must now rectify. We must recover the volunteer not only to bridge the gap between the public and the criminal justice system, but because he has skills to offer and because he is the key to bridging the professional manpower problem we face. In the modern agency the volunteer has a valuable role to play in all three methods of the social work profession but it is in community work that we see him reaching a pinnacle of constructive achievement. Community work is a process which can be summarised as a matter of building linkages between identified needs and those who have the skills and resources to alleviate them. Not only does the volunteer in such a role perform a constructive task but in the process he grows in human awareness, an awareness he will convey to others. This expansion of our educative role through volunteer participation is surely a vital tool in the containment of crime.



# INDUSTRIAL ESPIONAGE

*DETECTIVE SGT. PERC CARTER

## INTRODUCTION AND DEFINITION

We generally think of espionage as an intrigue set on a rain swept side street of a large European city, but there is also a type of espionage that takes place in the offices, factories and laboratories of Australian businesses. Industrial espionage ranges from intelligence provided to a company by a newly hired employee who had worked for a competitor, to elaborate electronic eavesdropping devices and professional thieves who steal various types of proprietory information.

Corporations, no less than countries, have been gathering information about one another for years. Among nations it is called spying and may involve sophisticated techniques, huge sums of money, especially trained personnel and covert methods. Companies are more likely to call it market research or commercial analysis. It is often difficult for the executive whose business practices are ethical to realise that there are unethical individuals who will take advantage of a situation in which intellectual information can be stolen or misused.

In ancient times the most valuable possessions of merchants were jewels and precious metals which were secured in strong locked chests. Today the most valuable assets are no longer that concrete. Nor is their protection that simple. Intellectual information has evolved into an important business asset and concurrently, a fundamental problem has developed. The risk of loss through industrial espionage.

What is industrial espionage? The word espionage is derived from the French verb 'espionner' which means to see or discover something intended to be concealed. For practical purposes, industrial espionage can be defined as:

> **'The illiegal obtaining and disclosure or use of confidential, secret, or proprietory information, method, blueprints, equipment and prototypes of an enterprise; either by stealth, electronic devices, deceit, subterfuge, blackmail, bribery or theft.' (B)**

Like sex, industrial espionage seems to be one of those activities that has been going on for a long time, that everyone knows is going on, but which nobody knows very much about. No one is quite sure who is doing it, how frequently, to whom, or how. (C)

## EXAMPLES OF INDUSTRIAL ESPIONAGE

Industrial espionage is by no means a recent phenomena. William F. Legget in his book, "The Story of Silk", gives a perfect example. Silk originated in China at least 5000 years ago. Its production and processing were maintained as jealously guarded secrets for many centuries. The Roman Emporer, Justinian, AD 529–565, was aware that his subjects were importing raw silk from the east at enormous cost. The silk was manufactured into garments in Constantinople, his capital. Justinian decided, because of the cost of the raw silk, to obtain the silk secrets from China so that both the fibre and

*Detective SGT. Perc Carter of the N.S.W. Police Department Criminal Investigation Branch Fraud Squad, is the author of this paper which has previously been published in the Australian Police Journal. He has kindly consented to our re-publishing the article. Detective SGT Carter is also the N.S.W. Branch State Representative on the National Executive of the Australian Crime Prevention Council.*

fabric could be processed locally and additionally, that his silk industry would be independent from the rest of the world. About AD 550 Justinian sent two monks to China to obtain employment in the silk industry and remain there until they had obtained the secret of raw silk production. Justinian's industrial spies remained in China for two years and learned as much as they could about the silk secrets. About AD 552 the monks returned to Constantinople with the secrets and also some silkworm eggs that they had stolen and smuggled out of China in their bamboo walking sticks. Justinian set up his silk industry using the eggs and Constantinople became a famous producer of silk for the markets of the Middle East. It enjoyed that distinction for about 600 years. Here we have a perfect example of industrial espionage as an important factor in the economic success of a whole country.

The theft of knowledge today is a business as multi-national in its drive and structure as any corporate entity. (D) The extent of the activities of the industrial spy can be determined by a short review of some recent cases.

Encyclopaedia Brittanica in the U.S.A., recently sued three of the computer operators on the night shift for $4 million for copying three million names from tapes of the company's most valued customer lists and then selling them to a direct mail advertiser.

British Airways had the programmes and details of its $100 million computer system stolen and offered for sale to its rival airlines.

In 1965 two employees of Kodak were tried at the Old Bailey for corruptly accepting money in exchange for information on emulsions, wetting agents, anti-static and anti-halo materials and secret processes of Kodak. They were aquitted when evidence was given that Kodak had paid the costs of the trial witnesses.

Italian Police recently uncovered a network of illegal organisations tapping the telephones of Shell and Chevron Oil, the Bank of Italy, newspapers and leading politicians and peddling the intelligence gained to any interested party. Subsequently, an Industrial Espionage seminar in Paris was told that there was good reason to believe that similar agencies existed in Britian, France, Germany and Switzerland.

According to the Australian Businessmans's Security Manual, recent surveys show that many Australian companies are being bugged for industrial secrets. One major construction company lost a multi- million contract to a rival tenderer. It was discovered later that the premises had been bugged. Similarly, a clothing manufacturer placed bugs in the board room of a rival company and learned its marketing secrets. The spying company got to the public first with a new range of clothing thus costing the competitor almost $500,000.00 in lost sales.

In July, 1977 Fraud Squad Detectives from the Sydney C.I.B. attended the offices of . . . . . a subsiduary of the giant . . . . . group of companies. An employee had been observed photocopying confidential information relating to freight rates. Inquiries showed that the suspect was leaving . . . . . where he worked as an accounts clerk to take up a similar position with a rival company. Management of . . . . . believed that the suspect was going to sell or otherwise dispose of the photocopies to his prospective employer. The documents contained information which would have allowed competitors of . . . . . .to undercut and gain contracts in preference to . . . . . .The suspect, however, never removed the photostats from the office of . . . . . but threw them away into a waste-paper basket in the office. When questioned, he admitted that it had been his intention to supply the documents to his prospective employer to gain their favour. However, he had a change of heart before he could do so. His actions were not the result of an approach by his prospective employer, but as a result of his own thought for aggrandisement, no secret commission was paid and no offence was committed.

The use of an aeroplane to obtain photographs for industrial espionage was reported in the Wall Street Journal of August 8, 1970, following the case of E.I. DuPont de Nemours & Co. –v– Christopher. The case was heard in New Orleans, U.S.A. and promises to become a landmark in the annals of industrial espionage.

Judge Irving Goldberg of the U.S. Circuit Court of Appeals ordered a Texas photography concern to divulge in a lower court the name of the party to which it sold aerial pictures of a Du Pont plant that uses a secret process to produce methanol. The chemical is used to make anti-freeze and industrial plastics.

In March 1969, construction workers at Du Pont's new multi-million dollar plant in Beaumont, noticed a low-flying plane circling over the still unfinished construction site and acting in a 'generally suspicious manner', according to a Du Pont spokesman. After some detective work of its own, the company discovered that the plane contained a photographer who snapped 16 pictures of the plant. The pictures would enable competitors to duplicate the Du Pont process. The photography company involved in the alleged aerial spying, Rolph and Gary Christopher, refused to divulge who had hired them. Du Pont brought suit in the Federal District Court that also asked for damages and an injunction to prevent further circulation of the photographs and additional photographing of the plant. The court ruled in Du Pont's favour and the photography firm appealed.

In upholding the decision, Judge Goldberg noted that aerial photography was an unusual form of industrial espionage that did not involve fraud or other direct violations of the law. "However", he said, "our devotion to free wheeling industrial competition must not force us into accepting the law of the jungle as the standard of morality excepted in our commercial relations". The case is interesting because it shows the lengths to which industrial spies are prepared to go to obtain their information.

## HOW INDUSTRIAL ESPIONAGE IS CARRIED OUT AND INDUSTRIAL SECRETS LOST

Industrial espionage relies heavily on gathering information which is freely available to the diligent information gatherers. When this method fails, the industrial spy reaches for his tools of trade. Everyone who has ever seen a spy film is familiar with the electronic bugs, miniature cameras, telephone scramblers, and sensors. These tools of trade are probably far more widely used by agents trying to steal the details of a new detergent than a new destroyer.

The practice of head-hunting, i.e. hiring away competitors key staff and picking their brains for useful unformation is always being practised. Basically, methods used in industrial espionage may be classified broadly as:

(a) Subterfuge
(b) Fraud
(c) Trespass
(d) Bribery
(e) Theft; and
(f) Eavesdropping and wire tapping (E)

## SUBTERFUGE

Most common, passing oneself off as another, i.e. visitor, employee, fire inspector, council inspector, publicity agent or a photographer after a story. The list is endless but the result is the same. Entry to a plant or an office often unescorted.

## FRAUD

A party may indicate to the owner of a trade secret that

they would be interested in a licence to use the secret. During the negotiations, question after question, finally leads to an indication of the general element of the secret. Finally, the false negotiator says, "Well, now the general terms have been worked out, but of course we can't buy a pig in a bag, let's see how the process works before we sign." After the disclosure, the fraudulent negotiator finds some excuse for breaking off the talks and proceeds to profit from the owners secret process.

### TRESPASS

Frequently an espionage agent may be so determined and so expectant of a high reward that he will risk actual trespass without subterfuge to gain access to an office, laboratory or plant.

### BRIBERY

Either by money or by kind,The old adage, "When the wine is in the secret is out" applies here.

### THEFT

This needs no explanation, the agent actually removes the confidential papers from the subject and supplies them or the information from them to his principals.

In the catergory of theft of course, the use of the office photostat machine finds a place. Photocopy machines have become a boom to the corporate espionage agent. Copying of confidential documents can be controlled by limiting employees access to all photocopy machines and duplicating machines.

### EAVESDROPPING AND WIRE TAPPING

Electronic eavesdropping devices are part of the tools of trade of the industrial spy. These 'Big Brother' devices are readily available and in most instances, no technical skill is required to be able to operate them. The list of available devices is lengthy and runs from the simple telephone bug to sophisticated laser beam instruments. Micro-circuitry and minature electronics techniques are now in use to produce smaller and more efficient instruments. Many security executives in business and in industry discount the use of electronic listening devices and say they are stretched out of proportion. They point out the many other ways of gathering information. The point remains, however, that these devices are being produced and there is a market for them. In its report, *The Law and Private Police,* The Rand Corporation of America notes that between 1958 and 1968 sales of electronic detection and surveillance equipment grew from $27 million to $83 million annually. Prevention on the part of management is the key to the problem of electronic eavesdropping.

The old wartime expression, "Loose lips lose ships" and "Carless talk costs lives" still have great meaning in the area of industrial espionage. Hotels and restauants are ideal targets where over a drink or a meal people can be expected to talk more freely than usual, and if an affable stanger joins a group of employees and buys a round of drinks, who worries. Workers go to the local 'water-hole' and in no time at all they feel it is not a public place but a club and practically an extension of the office. Even major policy decisions can be made in the hotel, within the hearing of all and sundry, usually with no notable caution. Such cocktail hours are a treasure trove of information. (F)

### HOW INDUSTRIAL SECRETS ARE LOST

There is a fine line of demarcation between obtaining competitive intelligence through legitimate and moral means and engaging in nefarious industrial espionage. Robert Farr in "The Technological Spy" believes that about 60% of all company leaks are the result of carelessness. Carelessness or not, such leaks and nefariously obtained information are estimated to cost United States industry about $2 billion annually. (G)

People are the best source of information about anything. The following classes of persons contribute to the industrial espionage scene:

(a) The disloyal employee

(b) The moonlighting employee

(c) The mobile employee, i.e. leaving one company for another and taking secrets in his head

(d) The marketing employee, i.e. salesman entrusted with confidential information to help him sell the product

(e) Purchasing employees, i.e. giving too much information to suppliers

(f) Consultants — assist one company by scuttling another; and

(g) Cleaners

In addition to the above list, souces such as:

(a) Seminars

(b) Conventions

(c) Trade shows; and

(d) Trade Publications

provide valuable information to rival companies.

How can then, the company executive, protect his company secrets? There are a number of techniques for protection. He can:

(a) Screen job applicants thoroughly, particularly with reference to why last position vacated

(b) Educate employees, ideally every employee should be convinced that his job, his sucess and his growth within the organisation depends on the success of the enterprise for which he works

(c) Physical control — Prevent employees from moving into areas of the operation which do not concern them

(d) External control — Prevent non-employees (visitors) having access to the plant and have them under supervision

(e) Internal control — Don't leave confidential papers and information about desks after hours; and

(f) Control disseminations of information. Censor entries in trade journals

### THE COMPUTER AND INDUSTRIAL ESPIONAGE

As computers emerge from their years of infancy, they are taking on increasingly responsible work. We do not know how far this process will go or how responsible the computer will eventually become in society. We can only observe its prodigious growth in capability and potential. The more vital the work of the computer, the more important it is to protect it from failure, catastrophe; and from criminals, vandals, incompetence and people who misuse its power. Put simply, the data processing function shall not lose vital data, introduce errors into them or permit data to be read or modified without authorisation. (H)

Computer technology has opened whole new areas of security vulnerability because of the simultaneous operation of three factors. First, data that formerly would have been dispersed into many different locales are now brought together — sometimes kept together — in the computer. Second, to optimise remote operations of industrial enterprise, computer facilites are being widely designed for remote-terminal access. That has the effect of exposing the information newly con-

centrated in the computer centre, perhaps thousands of miles away. The only requirement in many cases is access to a suitable terminal, or perhaps only a telephone instrument. Third, the economics inherent in broad computer use by small enterprises has created the computer service bureau. (L)

The perils of information loss are so great that many managers have chosen, perhaps unconsciously, to ignore them. Ignore does not mean to take absolutely no precautions, although there are cases in which this is literally true: it means .to rely on established security ritual that is not even responsive to the nature of the threats. (L)

Obviously, all one needs is the capacity to 'plug' into a computer installation with the necessary keys which make possible the making of duplicates from the information stores in the computer. Blank data cards and paper tape are given minimal accountability attention in most facilities because of their very low cost. The use of several hundred, or thousand, cards or of one or more paper tapes to make unauthorised copies would probably never be noticed. When the medium is as small and as easily transported as magnetic tape and physical theft, possibility becomes a probability.

Data in a computer as a captive facility is vulnerable to compromise in two ways:

(a) They can be duplicated during normal operations either by a change in programme instructions or by computer operations personnel making unauthorised use of facilities at unauthorised times.

(b) They can be intercepted from outside the computer centre. Clandestine interception can be either by attack on the electromagnetic envelope surrounding the computer, or by coupling in some way to the tele-communication links that bind several compuer units or their users together.

The subject of computer security and vulnerability to industrial espionage is a vast field. Suffice to say that with the present state of the criminal law, sanctions against the unauthorised uplifting of information from a computer that did not directly involve larceny of the tangible data, i.e. tapes, print-outs, etc., would be almost impossible to implement. The mere technological information necessary to understand the uplifting of portion of a computer programme would severely limit the availabillity of Police personnel who could be assigned to investigate such a case.

Martin Prentice-Hall in *'Secutiry, Accuracy and Privacy in Computer Systems'* says that five per cent of the total data processing budget should be set aside and represents a reasonable security budget for a computer installation.

## THE ROLE OF MANAGEMENT IN INDUSTRIAL COUNTER ESPIONAGE

The role of management in prevention of industrial espionage is the most important aspect. (J)

By observing the simple rules set out in the previous paragraph (How can then, the company executive, protect his company secrets?), management can minimise the possibility of loss through espionage.

Investigation of suspected cases of corporate spying is generally left to independent security experts who offer counter espionage services or to the increasing number of private inquiry agents who are undertaking such work. (K)

In 1973 for example, some 500 cases of industrial espionage were investigated by members of the Association of British Investigators.

Companies who have taken the espionage threat seriously have not surrounded themselves with security guards or barbed wire fences. They have tackled the problem through their personnel. Employees are indoctrinated with the security message via posters, stickers and talks. Thus everyone in the comapny is on guard against security leaks or at least aware of how easily they may occur.

Few companies, however, outside those on government work are as security conscious as they might be when it comes to defence against industrial espionage. If most companies are awaiting a lead, it has been provided by Imperial Chemical Industries, Brittians's biggest complex and one of the world's biggest chemical companies. It recently appointed as its security adviser Sir Martin Furnival-Jones, a career M15 man for 17 years and Director General of the Security Service for seven years until his retirement in 1972. An I.C.I. spokesman said, "I.C.I. decided to bring Sir Martin in to review company security to ensure we don't suffer any leakages."

## THE ROLE OF THE POLICE IN INDUSTRIAL ESPIONAGE

Scotland Yard in England is keeping an eye on the problem of industrial espionage and it is becoming increasingly involved in looking into suspected cases where the criminal law may have been infringed. Generally, there is little the Police can do since industrial espionage as such is not a crime. Only where bribery, theft or conspiracy can be proved does Scotland Yard submit a brief to the Director of Public Prosecutions. (K)

In New South Wales, a similar situation exists. The role of the Police in this State can best be explained by examining the law in relation to industrial espionage.

## INDUSTRIAL ESPIONAGE AND THE LAW

Laws relating to protection of trade secrets vary from jurisdiction to jurisdiction, however, they are developed from the common law which forms the foundation for the modern rule.

One of the earliest industrial espionage cases is an English case, Yovatt —v— Wingard, decided in 1820. The case involved a veterinarians's journeyman who began selling medicines after leaving the employ of the master from whom he had learned the secret medical formula. The court granted injunctive relief based on breach of confidence. In a later English case, Morison —v— Moat, decided in 1851, the court held that a civil cause of action was clearly established based upon a wrongful disclosure of a secret. The first case in the United States gave judicial protection to trade secrets was Peabody —v— Norfold, decided in 1868, in Massachusetts. In Australia, Rheem Australia Limited —v— American Flange Corporation, a case revolving about a 15 cent plastic bung and its use by Rheem Australia Limited, became a celebrated case, partially because it was the longest running civil litigation in our history. These are all civil cases.

The criminal law has had great difficulty coming to grips with the concept of industrial espionage and the laws of larceny, secret commissions and conspiracy must be looked to as having the most bearing on the subject. The difficulty arises with the basic concept of larceny which involves the wrongful taking of property. The English case, R —v— Poynton in 1862, established that the charge against the accused must have reference to some specific thing. That thing which is stolen must be the subject of larceny at common law. It must be tangible. It is essential that the thing alleged to have been stolen possesses physical characteristics or existence. The lack of perception by the sense of touch renders a thing not larcenable at common law.

A chose in action is not tangible. Because of their lack of substance, there cannot be larceny at common law of debts, copyrights, patents, trade marks, trade names or trade secrets. It would not be possible for example, to have a person found guilty of larceny at common law for the theft of an idea or a trade secret or the patented invention of another person. These actions would of course be actionable in the civil jurisdiction. Consequently where an idea or a concept, that intangible thing, is misappropriated the criminal law cannot come to grips with the problem. Obviously if the offence involves the actual theft of company documents containing

written details of maps, diagrams, models, blueprints or equation formula, then a charge of larceny could be substantiated because the property is tangible and is of some value, even although it may be only the value of the piece of paper.

The New South Wales Companies Act, No. 71 of 1961 provides protections. Section 124 of the Companies Act states:

(1) A director shall at all times act honestly and use reasonable diligence in the discharge of his office.

(2) An officer of a corporation shall not make improper use of information aquired by virtue of his position as such an officer to gain directly or indirectly an advantage for himself or for any other person or to cause detriment to the corporation.

(3) An officer of a corporation who commits a breach of a provision of this section is:

(a) liable to the corporation for –

(i) profit by him; and

(ii) damage suffered by the corporation, as a result of the breach; and

(b) guilty of an offence against this Act.

PENALTY: Two thousand dollars.

Note that the offender must be an officer of the company.

In addition, the New South Wales Secret Commissions Prohibition Act of 1919 provides penalties which are relative to industrial espionage by virute of Section 3 which states, inter alia:

If any agent corruptly receives or solicits from any person for himself or for any other person any valuable consideration:

(a) as an inducement or reward for or otherwise on account of doing or forbearing to do, or having done or forborn to do, any act in relation to his principal's affairs or business; or

(b) the receipt or any expectation of which would in anyway tend to influence him to show, or to forbear to show favour or disfavour to any person in relation to his principal's affairs or business; or

If any person corruptly gives or offers to any agent any valuable consideration:

(a) as an inducement or reward for or otherwise on account of the agent doing, or forbearing to do or having done or forborn to do any act in relation to his principal's affairs; or

(b) the receipt or any expectation of which would in any way tend to influence the agent to show or to forbear to show favour or disfavour to any person in relation to his principal's affairs or business.

shall be guilty of an offence under this Act.

The New South Wales Listening Devices Act of 1969 prohibits the use of listening devices to hear, record or listen to private conversations except where they are used by parties to the conversation or in authorised circumstances. The Act defines a listening device as:

> Any instrument, apparatus, equipment or device capable of being used to hear, record or listen to a private conversation simultaneously with its taking place.

Private conversation is defined as:

> Any words spoken by one person to another person in circumstances that indicate that those persons desire the words to be listened to or heard only by themselves or that indicate that either of those persons desire the words to be heard or listened to only by themselves and by some other person, but does not include words spoken by one person to another in circumstances in which either of those persons ought reasonably to expect the words to be heard, recorded or listened to by some other person, not being a person who has the consent, express or implied, of either of those persons to do so.

Use of the listening device is covered by section 4(1) of the Act which states:

> A person is guilty of an offence against this Act if he uses a listening device to hear, record or listen to a private conversation.

The Commonwealth Trade Marks Act of 1955–1966 creates offences of forging trade marks, applying falsely for a registered trade mark, disposing of or having in possession instruments used for forging trade marks.

The Commonwealth Telephonic Communications (Interception) Act 1960-66 prohibits the interception of telephonic communications except where especially authorised in the interests of the security of the Commonwealth.

Part VIII of the Commonwealth Crimes Act, 1914–66, deals specifically with espionage. section 78 of the Act states:

(1) If a person for a purpose intended to be prejudicial to the safety or defence of the Commonwealth or a part of the Queen's dominions –

(a) makes a sketch, plan, photograph, model, cipher, note, document or article that is likely to be, might be or is intended to be directly or indirectly useful to an enemy or a foreign power;

(b) obtains, collects, records, uses, has in his possession or communicated to another person a sketch, plan, photograph, model, cipher, note, document, article or information that is likely to be or is intended to be directly or indirectly useful to an enemy or foreign power;

shall be guilty of in indictable offence.

## SOME EXAMPLES OF OVERSEAS LEGISLATION –

### UNITED STATES OF AMERICA

**Federal Trade Commission Act** – Section 5 states, "Unfair methods of competition in commerce, and unfair or deceptive acts or practices in commerce are declared unlawful." However the law was designed to protect the public from one manufacturer passing off his goods as that of another and the Courts of Appeal have held that the Act is of little value in remedies against industrial espionage.

**Trade Practice Conference Rules** – Section 46.10 makes it unlawful to entice willfully employees to hamper or injure competitors.

**The Tarrif Act of 1930** – Designed to protect U.S. patents. This Act has been found to be substantially ineffective to protect American industry from 'pirated' know how.

**The Federal Food and Drug and Cosmetic Act** – Section 301 of this Act makes it an offence for any one using to his own advantage or revealing any method or process which is a trade secret.

California and New Jersey both provide penalties in their State statutes for 'pirating' of inventions, designs. New Jersey also has criminal penalties for acts detrimental to an employer. New Jersey Title 2A, Section 170–88 covers intangible proprietory information. The penalty is up to one year imprisonment or $1,000.00 fine or both.

Foreign nations, in particular the industrialised European nations have much stronger laws than the United States of America or Australia in the matter of theft and misuse of industrial secrets.

**In Sweden,** the Swedish Act of May, 1951, makes it an offence to "unlawfully use or disclose a manufacturing process." Penalty fine and imprisonment for up to one year.

**In France,** the French Penal Code, Article 418, punishes delivery to third parties of Industrial secrets by un-authorised

persons by fine and imprisonment up to five years. If the disclosure is to foreigners, the penalty is loss of civil rights for up to ten years at the end of the sentence of five years.

**In Yugoslavia,** the Criminal Code of 1951, Article 213 provides for imprisonment of up to three months for divulging business secrets. However, if a bribe is involved for the delivery, the penalty increases to ten years.

**In Germany,** the Unfair Competition Statute, Sections 17, 18 and 20 provide fines and imprisonment for offenders misusing trade secrets.

**In Belgium,** the law prohibits the fraudulent disclosure of trade secrets with imprisonment from three months to three years plus a fine.

**In Italy,** the Penal Code, Sections 622 and 623 make disclosure of confidential information for a person's advantage subject to imprisonment for up to two years.

**In Canada,** the Canadian statutes provide many avenues for action both under Criminal Code and the Theft Act, Section 269. If ex-employee is involved, action lies under the Criminal Breach of Trust section of the Criminal Code, Section 282. If stolen information is utilised by a competitor, action is possible under the Unfair Competition Act 1–2, Elizabeth 11, Chapter 49.

**In Norway,** the Act of July 7, 1922, Section 1, prohibits improper competition as by an ex-employee or another to whom he has conveyed trade secrets.

**In Argentina,** Section 156 of the Criminal Code, penalises theft of trade secrets with a fine and loss of the right to work.

**In Austria,** the Law Against Unfair Competition of 1923, penalises the unauthorised use of trade secrets or abuses of documents entrusted to a person, with a fine and imprisonment.

**In Brazil,** the Penal Code, Sections 163 and 154, penalises disclosure of confidential information which damages the owner by fine or imprisonment.

**In Columbia,** Article 280 of the Criminal Code penalises unauthorised disclosure of trade secrets by an employee by fine and imprisonment.

**In Japan,** Criminal Code, Article 235 provides penalties of up to ten years imprisonment for employees who accept salary with intent to defraud the employer of trade secrets.

**In Mexico,** Penal Code, Section 210 provides fines and imprisonment for unauthorised disclosure of trade secrets by an employee.

**In Spain,** Penal Code, Article 499, specifically deals with disclosures by employees.

**New South Wales,** has no criminal sanctions available to compare with those listed.

## THE K.G.B. (SOVIET SECRET SERVICE)

No paper on industrial espionage would be complete without mention of the Russian Secret Service or K.G.B. and their activities in the field.

International espionage used to concentrate mainly on government and military secrets. Today large sums of money are being spent to obtain industrial secrets. To quote Newsweek of October 5, 1971, "Increasingly, the K.G.B. is turning its attention to a new kind of spying; technological, commercial and industrial espionage. The field is less glamorous than traditional undercover pursuits but it is probably more vital to the Soviet Union. . . One of the K.G.B.'s new assignments is to help close the technological gap between the Soviet Union and more advanced nations, and to prevent even less developed nations from catching up. Sometimes this calls for extreme measures. In September, 1971, 105 Soviet spies were expelled from England in one coup and most were engaged in ferreting out industrial secrets. One of their main methods was to bribe or blackmail citizens into obtaining industrial information, particularly on electronics and computers."

The London Observer of October 3, 1971, commented, "The factory and the laboratory have become major priority areas for modern spies. Nor is it difficult to see why a country like Russia is still technologically so far behind Britian, should invest so much money in this kind of spying, and court the kind of risks that exploded with such impact in their face. The cost of initiating and developing new technological process is immensely expensive, and it is quite obviously quicker and cheaper to steal what knowledge one can from those who have made the initial investment in capital and knowledge. Russia would obviously be better off it, instead of having to import expensive computers and scientific instruments if it could gain access to information that would enable it to produce the goods for itself."

It should be kept in mind that in his book "Espionage and Subversion", Peter Hamilton states that schools for industrial spies exist in Switzerland and Japan, the Japanese being the more important of the two.

In closing, pause a while and consider those breaking and entering offences of factories, laboratories and offices where nothing is reported stolen. Industrial espionage?

## BIBLIOGRAPHY


(A) "Protecting Your Business Against Espionage." Walsh HEALY'
(B) Iron Age, Volumn 211, April–June, 1973.
(C) "From Du Pont With Love", Edward ENGBERG, Commonwealth, July, 1972.
(D) "I Spy", Howe MARTIN, Columbia Journal of World Business, May–June, 1969.
(E) Industrial Espionage and Misuse of Trade Secrets, Worth Wade.
(F) "Office and Office Building Security", Sam LEWIS.
(G) "The Industrial Spy", American Management Association.
(H) "Security, Accuracy and Privacy in Computer Systems", Martin PRENTICE-HALL.
(J) "Practical Security in Commerce and Industry", Oliver & Wilson.
(K) Industrial Management, July–August, 1974.
(L) "Prevention and Detection of Fraud in Industry", Steven North.

In addition to the above texts, reference was also made to:
Business Administration, May, 1974; Business Week, August 4, 1975; Business Management, October, 1965; Handbook of Business Administration and Industrial Safety and Protection by Mel Handell; Harvard Business Review, November-December, 1974; The Bulletin; Duns Gazette; and, the New South Wales Police Academy Detectives' Course notes.