AUSTRALIAN INSTITUTE OF CRIMINOLOGY

trends & issues

in crime and criminal justice

No.106

Industrial Espionage: Criminal or Civil Remedies

Gillian Dempsey

Should theft of tvade secrets be regarded as a civil or a criminal matter? This is a question of growing significance since the importance of Australia remaining a competitive player in the global economy requires that Australian enterprise take every advantage of business opportunities, at home and abroad. However, Australian companies should be mindful that competitors, and nations which might be hosts to Australian investment, may have a strong interest in Australian trade secrets and other economic intelligence.

Although its incidence and prevalence are unknowable, industrial espionage by governments and private sector institutions is a fact of contemporary commercial life. Recent developments in the technology of intercepting communications make such activities easier to undertake and more difficult to detect than in the past.

This essay discusses whether existing Australian legal safeguards against industrial espionage are adequate, or whether the greater use of criminal sanctions, such as those recently introduced in the United States, might be appropriate. It balances a number of considerations, including deterrence, compensation and incentives to innovation, and cautions against uncritical adoption of overseas innovations.

Adam Graycar
Director

Since the demise of the Cold War, the battle lines have been redrawn firmly in terms of economic competition between nations. Tariffs and trading blocs may have replaced bullets and bombs, but accurate data and information remain the most essential weapons in any war. The US President's Annual Report to Congress (1996), *Foreign Economic Collection and Industrial Espionage,* observed that:

> *The increasing value of proprietary economic information in the global and domestic marketplaces, greater access to the "information superhighway", and the proliferation of new technology demands combine to increase both the opportunities and motives for conducting economic collection and industrial espionage.*

In response to several committee recommendations the US Congress enacted the Economic Espionage Act 1996. The US is the only Western nation with a legal system similar to Australia's to pass such legislation. This issues paper considers whether Australia should follow suit.

March 1999

ISSN 0817-8542
ISBN 0 642 24091 4

Australian Institute
of Criminology
GPO Box 2944
Canberra ACT 2601
Australia

Tel: 02 6260 9200
Fax: 02 6260 9201

For subscription information together with a complete list of the papers in the Trends and Issues in Crime and Criminal Justice series, visit the AIC web site at:

http://www.aic.gov.au

or call AusInfo toll free on 13 24 47

What is Industrial Espionage?

Firstly, the arena of war must be defined. A US information security specialist, Robert D. Steele (1997), has developed a taxonomy dividing intelligence into four categories:

> a. ***Open source or public information***; *within intelligence communities, this is known as open source intelligence or OSCINT. "Grey literature", literature which is unclassified and not proprietary, but produced in limited quantities for limited purposes, is included as an element of OSCINT. Open (unclassified) electronic information, such as that available through the Internet and related file servers and newsgroups, is also included in OSCINT. The vast majority of scientific and technical intelligence is available through OSCINT, to include 600 scientific and technical journals that appear only in electronic form.*
>
> b. ***Open proprietary information***; *discernible through open source investigation. This includes the reverse engineering of legitimately acquired products, and legally conducted "competitor intelligence". (Note: competitor intelligence is the globally accepted term for legal research efforts by businesses studying their competitor's products, organizations, and related matters.)*
>
> c. ***Closed proprietary information***; *[trade secrets] available only through industrial espionage or clandestine and technical penetrations of regulatory agencies.*
>
> d. ***Classified information***; *[military and national secrets] available only through clandestine human intelligence or technical (imagery or signals) intelligence.*

Industrial espionage, which Steele classes as "closed proprietary information", is synonymous with "economic espionage", "foreign economic collections" and "commercial intelligence". It refers only to the unlawful acquisition of trade secret data and information. Trade secrets are typically misappropriated through:

- employees (with or without deliberate collaboration);
- telecommunications interceptions (such as wire tapping, use of directional microphones and monitoring of emissions); and
- reverse engineering.

The competitive demand for information has inspired people to expend significant amounts of money on collecting open source information. *Wired* magazine (1998, p. 87) cites a report by The Futures Group that 82 per cent of US companies with $10 billion or more in annual revenues have a formal competitive intelligence network. The challenge for legislators is to forbid one form of information gathering without affecting the other.

Recent US Laws Criminalising Industrial Espionage

Having defined industrial espionage, it is useful to analyse the manner in which the US addressed the issue, particularly the main points raised in debate and the structure and content of their response.

On 1 February 1996, Senators Kohl and Specter introduced the Economic Espionage Act 1996 to the US Congress. In the Statements on Introduced Bills and Joint Resolutions (Senate Bill 1557), the senators claimed that the Bill addressed the:

> *… systematic pilfering of our country's economic secrets by our trading partners which undermines our economic security. It would not be unfair to say that America has become a full-service shopping mall for foreign governments and companies who want to jump start their businesses with stolen trade secrets.*

The primary justification for the Bill was the suggestion that existing laws inadequately protected the money spent in acquiring and creating proprietary information. It was argued that:

- civil trade secrets laws possessed insufficient deterrent power;
- the National Stolen Property Act (18 U.S.C. s.2314.31) failed due to some courts having held "purely intellectual property" to not constitute "goods, wares or merchandise";
- the Federal mail and wire fraud statutes prohibiting obtaining property by false pretences or representations were relatively unsuccessful due to the evidentiary difficulties posed by the need to connect a "scheme to defraud" with the use of the mail or wire transmissions to perpetrate the trade secret theft.

To overcome such alleged deficiencies, the provisions contained within the Economic Espionage Act are cast quite broadly and have two effects: to make theft of trade secrets a crime; and to make economic espionage a separate crime.

Trade secrets are defined in s.1839 as including all forms of information (regardless of the form in which it is stored) which *might* have economic value from "not being generally known" to "not being readily ascertainable through proper means", provided that the owner had taken "reasonable measures" to keep the information secret. Theft, attempted theft, and conspiracy to commit theft of proprietary information from a US owner for the benefit of a foreign government or a corporation, institution, instrumentality, or agent are criminalised under s.1831.

The definition of theft under s.1831 effectively has two broadly cast limbs. The first prevents traditional types of theft: "steals, or without authorisation appropriates, takes, carries away, or conceals, or by fraud, artifice, or deception obtains such information". Limb two reflects copyright-like protection without reflecting the corresponding public interest: "without authorisation copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information". Other subsections relate to dealing in stolen goods, conspiracy and attempt.

Disposal of trade secrets is exhaustively defined, including the alteration, destruction, replication and communication of the purloined trade secret. The provision relating to receiving stolen information is broad, outlawing receiving, buying or possessing a trade secret whilst knowing it to have been stolen or appropriated, obtained, or converted without authorisation.

The actual economic espionage provision, s.1831, mirrors the trade secrets provisions but has a requirement of proving that the defendant intended or knew that the offence would benefit any foreign government, foreign instrumentality, or foreign agent. This definition appears deliberately broadly cast. By saying "any" foreign government instead of "a" foreign government, the burden on the prosecution is somewhat alleviated as the causal nexus between the theft and the benefit need not be as direct. To reflect the increased severity of the crime, it has higher penalties: 15 years maximum term as opposed to 10 years.

In both cases there is also provision for the victims to receive restitution from funds recovered, and the potential for import bans against goods created by the stolen technology. In addition to this, the Act provides the court with power to issue protective orders and to take appropriate measures including interlocutory appeals against decisions or orders authorising disclosure of the information.

The US's decision to criminalise economic espionage rather than relying on civil remedies was, in part, prompted because a private suit against a foreign company or government "often just goes nowhere". The Economic Espionage Act 1996 provides for extraterritorial jurisdiction where:

- the offender is a US citizen; or
- the victim is a US citizen; and
- the offence was intended to have, or had, a direct or substantial effect in the US.

Referring back to Steele's distinction, the definitions in both the trade secrets provision and the industrial espionage provision will certainly catch "closed proprietary information" but may also catch "open proprietary information" in the form of reverse engineering, due to the conjunction of "not being readily ascertainable through proper means" and "appropriates".

Australia's Current Laws

The enactment of industrial espionage legislation would constitute a shift from traditional counterintelligence efforts largely directed at military threats to national security. Prior to making such an important decision, Australia should consider whether and to what degree:

- Australia's current laws address industrial espionage; and
- criminalisation of industrial espionage per se would result in a desirable long-run economic outcome.

To determine whether Australia's current legal responses are satisfactory, it is useful to consider whether Australia's laws suffer from the same deficiencies which led the US to legislate.

Criminal actions

In most jurisdictions in Australia (as in the US) information will not fall under the definition of "property" as it is not "capable of physical possession and removal", nor will it comprise "theft", as in most cases there will be no intention to permanently deprive the owner of the information. The definitional problems relating to information are largely mitigated in Australia by all jurisdictions having criminalised unlawful access to, alteration of, or destruction of data. Furthermore, s.7 of Part II of the *Telecommunications (Interception) Act 1979* renders it unlawful for an individual to intercept or to allow another to intercept a communication passing over a telecommunications system. This would include espionage activities such as wire taps and ethernet collars. Breaking, entering or any misappropriation of physical goods is covered by laws in all Australia. The only actions not covered by these crimes are where:

- an individual with permission to access the information disseminates the information;
- the information is reverse engineered.

This raises two questions: do Australia's civil laws cover these areas adequately, and is it economically sensible to criminalise the areas?

Civil actions

Part of the US's reason for criminalising industrial espionage was the perceived inadequacy of civil laws. Unlike the US, which has state-based statutory protection for trade secrets, Australia's contractual and equitable intervention for the protection of trade secrets is grounded in the enforcement of relationships of trust and confidence. Whereas the law relating to contractual measures (non-

disclosure agreements and their ilk) is well settled, the foundation of "breach of confidence" is uncertain. This uncertainty will ultimately have an effect on what information will be protected and the degree to which it will be protected. Currently, the leading case in this area is *Ansell* where Gowan J elucidated some common characteristics of secrets that could be protected. The secret:

- may not be a process in common use, or something which is in the public domain;
- does not need to be novel or inventive (since the rationale is breach of faith);
- is more likely to be protectable if others would have to go through the same process to produce the same material;
- must be in a form that it would be difficult to acquire except by "improper" means.

To which actions will breach of confidence apply?
Equity is the jurisdiction that binds the conscience. For this reason, information can be inferred to be secret where a person is given reasonable grounds to suspect that information is being given to them in confidence or for a limited purpose. In contrast to this, the issue as to what extent protectable private information can be used where there is a mixture of public and private information remains unsettled in Australia. Historically, this "springboard" problem has been resolved by a total restriction upon using private information, even where that information becomes public. More recently, cases have suggested that the confidee may use the information once it has become public if they offer to pay a reasonable sum for use.

To which actions will breach of confidence not apply?
Whereas the scope of the restrictions initially appears to be similar to the US's definition in the Economic Espionage Act, the effect is narrower because the underlying rationale for the protection differs. States in the US statutorily protect information as property. Australia, however, still leans towards equitable actions relating to the treatment of confidential information. This theoretical divergence gives rise to some differences in the scope of the law between the US and Australia.

The situation where an employee or a former employee possesses proprietary information is typically covered by covenants. Express or implied contractual obligations not to use information are read down to apply only to information which was not part of the general stock of an employee's knowledge. Courts in the US construe such agreements far more strictly.

In the US, at civil law, innocent third parties can be bound by the confidentiality despite not being in a fiduciary or other relationship of confidence. Under the Economic Espionage Act 1996 this treatment of innocent third parties is statutorily enacted. In contrast to this, Australia will not provide a remedy against an innocent acquirer of confidential information, as equity will not bind an innocent party in such a way. This means that innocent third party acquirers cannot be injuncted not to make use of, or reveal, the information. Merely accessing the information through reverse engineering will not constitute a breach of confidence, as no relationship of confidence could have arisen. This differs from the situation where a company hires a spy to acquire information and subsequently makes use of the misappropriated information. If evidence of a link sufficient to set up an equitable duty can be found, then the action can proceed.

Remedies for breach of confidence are compensation, account of profits, and delivery up of goods. The objective of equitable remedies such as this is to put the plaintiff in the position in which they would have been, had the wrong not occurred. Civil remedies in Australia are not as generous as those in the US: damages are calculated more conservatively and exemplary damages are rare.

Should Australia Criminalise Industrial Espionage Laws?

If one were to follow the US's logic, the deterrent effect of Australian civil laws would be significantly lower than that of US laws. Therefore, Australia should criminalise industrial espionage. Whilst it is true that, compared to US law, Australian law affords relatively little protection to trade secrets, it does not necessarily mean that Australia's regulation is deficient. Before criminalising industrial espionage, one must consider the economic effect of such legislation on the existing incentive structures established by intellectual property laws. Furthermore, one must consider who should bear the cost of enforcement.

Interaction with intellectual property laws

Envisaging the misappropriation of confidential information as a threat to Australia's economy requires a set of implicit assumptions to be made about the nature of information, as well as the nature of technological change and economic progress. Industrial espionage must be viewed in the context of other economic regulation. It is important to move from an *a priori* assumption that the current regulatory framework is sufficient, because independently criminalising industrial espionage would have an effect on long standing intellectual property regimes which currently hold the majority of intangible property.

Part of the rationale for offering patent and copyright

protection is to encourage the dissemination of information throughout an economy by providing an incentive to disclose trade secrets. If, as in the US, more protection of trade secrets is enacted, a move away from patent and copyright protection for intellectual objects must be the result. Stronger trade secrets laws hinder dissemination of innovation. Gurry (1984), in a random survey of the chemical industry in Britain, discovered that 22.2 per cent of firms kept innovations secret which they would have patented if the law did not protect confidences. The British law relating to breach of confidence was, at that time, less accommodating than Australia's laws are currently. Nevertheless, the attitude of some policy makers will be that valuable information, like valuable physical commodities, should be "protected" by criminalisation, in the interests of facilitating trade.

Effect on innovation of criminalising industrial espionage

One important assumption implicit in the US's understanding of the regulation of trade secrets is that innovations are largely produced through the effort of a single firm. This assumption is derived from Neo-classical economic theory which holds that, as both firms and individuals derive returns from proprietary knowledge, they have little incentive to share such knowledge, particularly with competitors. Empirical evidence, however, runs contrary to this argument: in the context of information, the recurring theme is the benefits of the division of labour (Leijonhufvud 1989).

In a modern economy, production tends to be characterised by alliances between firms. Indeed, economic literature is rife with examples of the incentive to combine structures in relation to search and research costs. As an example of sharing behaviour, Rosegger (1989, 1991) observed a rapid growth of bilateral, cooperative arrangements and the generation of institutionalised informational exchange on a widening range of topics. These alliances are often for the term of particular projects, where each firm can bring its particular (yet complementary) specialist knowledge to bear on the resolution of a particular problem.

This model explains why cooperation can be a beneficial strategy for the solution of problems and the development of new technologies – it is this very complementarity which provides the incentive to cooperate. The paradox here is that the best way to keep a secret is not to share it – yet the most rapid and efficient manner of solving a problem involving specialist knowledge is to form an alliance with a firm already possessing the requisite complementary knowledge. The obvious problem here is that, under the current intellectual property regimes, alliances in industry are often fluid, with firms constantly seeking out partners or suppliers for new projects. As a consequence of this, by accident or design, undesired dissemination of confidential information is, to a degree, inevitable. If this information is protected by patent or copyright, the damage done to a firm by dissemination is mitigated by the provision of the right; however, where the damage is protected by confidentiality, once the information escapes beyond the originator and any contracting parties, remedy is unavailable.

The question that must be posed is: if it is important to impose criminal restrictions to cover works unprotectable under current intellectual property regimes, would one risk the current structure of innovation? Regardless of the existence of other intellectual property laws, the imposition of criminal restrictions would be in the short-term self-interest of a firm at the commercial level. Once trade secrets are covered by criminal remedy, the incentive to cooperate and share information in the manner already outlined may decrease (Oakley and Owen 1989) due to concern over possible liability. Whilst this might not be contrary to the interests of the firm in the short run, the question arises as to whether it would be contrary on the whole to Australia's current economic interests.

Effective subsidy and incentive structures.

Criminalisation would effectively constitute a subsidy to the production of information in the form of legal costs (and possibly security expenditure). The difference between a civil and a criminal regulatory framework is in relation to the party who bears the costs. Under civil law, firms have a strong incentive to protect their information by constantly investing in, and maintaining, security arrangements. If these arrangements are violated, the cost of litigation is divided between the plaintiff and the defendant in the action.

Provided that the firms were already engaging in sensible management accounting practices, some of these costs would already be factored into the price of the goods or services sold. Additional to this, d'Aspremont and Jacquemin (1988) suggested that losses due to imitation by competitors can be mitigated where firms are able to internalise the research and development spillovers from other firms. To achieve this, further expenditure on research and development is necessary to appropriate the spillovers from other firms and to keep informed about the technological advances of competitors.

To put this another way, if the firm plans and budgets in a sufficiently careful manner, the costs of protecting against industrial espionage (on average over the long run) can be minimal. This is the most sensible economic solution. The firm should be in the best position to recognise its particular security weaknesses and to act to protect

its own economic interests. Looking at the current levels of sophistication in encryption techniques, organisational structures within corporations and other security measures, companies who are cognisant of the problem should be well placed to establish counter-intelligence measures.

In contrast, to argue for criminalisation would involve an implicit assumption that the interest of the firm is concurrent with the interest of society as a whole. The costs of detection and policing are likely to be relatively higher in a criminal arena than in a civil arena due to unfamiliarity with the particular firm. And the policing agency would have to acquire sufficient experience and knowledge in information security and evidence gathering techniques in a market where such knowledge is at a premium. For this argument to hold, criminalisation would have to cause welfare effects to pass from the firm on to society as a whole. This runs contrary to evidence which suggests that, where firms attain such a benefit, the bulk of the benefit remains within the firm and the remainder of the economy suffers due to disastrous effects on innovation and competitiveness (Macdonald and Mandeville 1987).

Conclusion

Criminalisation of industrial espionage per se in Australia is unlikely to prove a significantly greater deterrent than civil law and would constitute an expensive exercise, both in terms of establishing incorrect incentives, and of requiring specialist detection and enforcement measures. Further, one of the US's main complaints in relation to the current state of its own civil trade secrets protections was that it failed to exert extra-territorial jurisdiction. Australia generally has avoided extra-territorial application of its laws other than in exceptional situations such as war crimes and child sex tourism.

A sensible compromise for Australia would be to combine an education program to create awareness of the potential for harm or loss with a federal codification and simplification of trade secrets protection. Federal codification would provide greater consistency as all other intellectual property measures (with the exception of passing off) are enacted under s.51(xviii) of the Constitution.

References

Annual Report to Congress 1996, *Foreign Economic Collection and Industrial Espionage*, May, US Government Printing Service, also at:

http://www.nacic.gov/ECON96.htm

Ansell Rubber Co Pty Ltd v. Allied Rubber Industries Pty Ltd [1967] VR37

d'Aspremont, C. & Jacquemin, A. 1988, "Cooperative and Noncooperative R & D in Duopoly with Spillovers", *American Economic Review*, vol. 78, no. 5, pp. 1133-7.

The Futures Group report at:

http://www.tfg.com/pubs/docs/cs-sumry.html

Gurry, F. 1984, *Breach of Confidence*, Oxford University Press, Oxford.

Leijonhufvud, A. 1989, "Information Costs and the Division of Labour", *International Social Science Journal*, vol. 41, no. 2.

Macdonald, S. & Mandeville, T. 1987, "Innovation Protection Viewed from an Information Perspective" in *Direct Protection of Innovation*, ed. W. Kingston, Kluwer Academic, Dordrecht, pp. 157-70.

Oakley, B. and Owen, K. 1989, *Alvey: Britain's Strategic Computing Initiative*, MIT Press, Cambridge, Mass., p. 28.

Rosegger, G. 1989, "Cooperative Research in the Automobile Industry: a Multinational Perspective" in *Cooperative Research and Development: The Industry, University, Government Relationship*, eds A.N. Link & G. Tassey, Kluwer Academic, Boston, pp. 167-86.

Rosegger, G. 1991, "Advances in Information Technology and the Innovation Strategies of Firms", *Prometheus*, vol. 9, pp. 5-20 at pp. 9-10.

Senate Bill 1557, 104th Congress, Second Session, 1 February 1996 (p. S737 of the *Congressional Record*).

Steele, R.D. 1997, *Theory and Practice of Intelligence in the Age of Information*, Open Source Solutions Inc. at:

http://www.oss.net/Proceedings/ossaaa/aaa2/aaa2an.htm

Wired 1998, June, p. 87 (citing The Futures Group).

Dr Gillian Dempsey is a Lecturer in the Department of Commerce at the Australian National University.

General Editor, Trends and Issues in Crime and Criminal Justice series:
Dr Adam Graycar, Director
Australian Institute of Criminology
GPO Box 2944
Canberra ACT 2601 Australia

Note: Trends and Issues in Crime and Criminal Justice are refereed papers.