Loyalty or betrayal? Information for innovation in the organisation

Stuart Macdonald

Management School
University of Sheffield
Sheffield S1 4DT, England
Fax: 44–1993–772871
E-mail: s.macdonald@sheffield.ac.uk

Abstract: Established wisdom is that the organisation benefits from retaining information, and loses if any of this information escapes. The employee who helps guard this information fortress is seen as loyal to the organisation: the employee who leaks information to the outside world as having betrayed it. Each is rewarded accordingly. This paper argues that organisations are dependent on external information for the innovation – the change – critical to their survival. But to receive information, they must first give information. The nature of organisation and the nature of information make this information transaction difficult. Organisations are forced to rely on key employees, trading in information, including the organisation's information, on their own account. A real test of managers is allowing these transactions without interfering in them, and realising that what is currently seen as betrayal of the organisation may actually be loyalty.

Keywords: innovation; information flow; information networks; espionage.

Reference to this paper should be made as follows: Macdonald, S. (2006) 'Loyalty or betrayal? Information for innovation in the organisation', *Int. J. Technology Intelligence and Planning*, Vol. 2, No. 1, pp.22–32.

Biographical notes: Stuart Macdonald is Professor of Information and Organisation at the University of Sheffield. Research has long been concerned with the role that information plays in innovation and in change more generally. Most of the research is strongly empirical, generally involving long-term investigation within organisations. An approach that makes information central to enquiry does not fit comfortably within the boundaries of a single discipline and has necessarily been pursued in several. Inevitably, the research has become inter-disciplinary and multi-disciplinary. Always the aim of the research is to contribute to understanding and thereby, perhaps, to corporate strategy and government policy.

An early version of this paper was published as Macdonald, S. (1996) 'Industrial espionage and innovation', *Interdisciplinary Science Reviews*, Vol. 21, No. 3, pp.209–214.

1 Introduction

> "Many businessmen fail to appreciate the extremely wide range of corporate data that could be useful to a competitor and thus harmful to their own company." (Edwards, 1987)
>
> "[Many managers] fail to appreciate the wide range of corporate data that could be useful to a competitor and, thus, harmful to their own companies." (Carter, 1989)

The quotations are early extracts from a burgeoning literature on the organisation's need to prevent the theft of information. In that the second was published two years after the first, from which it seems to have been stolen, heavy irony helps press home the point. It is understandable that this should be the argument of those who sell electronic eavesdropping equipment to acquire information from competitors or to detect competitors' attempts to acquire information from them. Problems arise, however, when the competitive intelligence lobby is all too convincing, when managers begin to disregard the cost to innovation of attempts to prevent industrial espionage.

Both the quotations exude crude information mercantilism. Both insist that the benefit to a competitor of any information acquired must be a cost to the organisation whence the information came: someone's gain must be someone else's loss. It follows that precautions should be taken to avoid this loss. Of course, information cannot be lost in the normal sense; even when information is gained by others, it is still retained. And whatever benefit accrues to a competitor comes not from information itself, but from using the information gained. There is, then, no direct relationship between gain and loss. Indeed, it could be argued – and it will be argued – that the organisation's loss of information leads directly to its gain of information, that competing organisations are actually interdependent, reliant on each other for the information required for innovation. Innovation is much more fundamental to their competitiveness than stolen scraps of information. In this sense, information from competitors is indeed important for competitiveness (von Hippel, 1988), but this sense entails getting information to competitors as much as getting it from them.

Is this obsession with retaining information likely to disrupt the flow of information among organisations? In particular, is informal flow of information through personal networks likely to be confused with industrial espionage? These personal networks cope well with tacit, uncodified information, totally different from the solid nuggets captured by miniature cameras, but it is still easy to confuse the mechanisms by which transfer takes place.

> "'There is no way to know who is listening.....' One experienced listener remarked about *The Lion and the Compass*, a popular Silicon Valley bar: 'If you really want to spy, just pull up a stool and listen.'" (Bronson, 1987)

Thus, does prescription for the guarding of information ignore decades of research on the link between ready information exchange (and even this particular bar) and rapid innovation in the high technology of Silicon Valley (Rogers, 1982; Braun and Macdonald, 1982).

This paper investigates not so much the role of the spy in technology transfer, for that is generally trivial, but the implications for technology transfer, and thus innovation and competitiveness, of attempts to prevent industrial espionage. It argues that actions to prevent spying may discourage innovation and hence reduce competitiveness (Macdonald, 1993). The paper goes further in suggesting that information must leave the organisation if the information required for innovation is to enter, and that this can best be effected by individual employees trading in information. It is bolder still, arguing that these employees must also trade in the organisation's information as well as their own, that they must act in their own interests rather than those of the organisation, and that such information transactions are largely beyond the organisation's control.

2 Information for innovation

Innovation is simply change in the way things are done. The world is sufficiently optimistic to assume that change is generally improvement, that there is some advantage for organisations in innovation, including competitive advantage. Essential for doing things in new ways is information (Macdonald, 1985). There are just two ways in which the organisation can acquire the information necessary for innovation: it can either look to its own information resources, or it can look outside to the information resources of others. Inside the organisation's boundaries are bits of information already in use which can perhaps be re-arranged into novel configurations. Bits that have long lain neglected may at last be exploited. There is also the internal option of creating new information through research, though inventing tends to entail as much information gathering as information creating. Alternatively, the organisation may search outside for information that might complement its own to yield innovation. Obvious information of the sort most readily available from the most likely sources, while easy to blend with the organisation's existing knowledge, tends to contribute to only minor, incremental innovation. Major, radical innovation requires the addition to existing stocks of information very different from what is already known. The more different this information, the more difficult it is to find, to transfer from external sources, and to blend with information already in the organisation (Robertson, 1975). The information required for innovation does not exist ready packaged, just waiting to be transferred – or stolen.

All sorts of problems arise when an organisation resorts to external information for innovation. The most obvious is that there is an awful lot of it about. How does the organisation find what it needs and then acquire this information? Though predictable sources may yield only predictable information, they do suggest where to search and how to acquire. Competitors are one very obvious source and collaboration has become a fashionable means of acquiring their information, one much encouraged by governments anxious to promote technology transfer (Dodgson, 1993). Yet, collaboration and other formal arrangements for the transfer of information do not always cope well with the characteristics of the good they are supposed to transfer. Just how is the organisation to reach a comprehensive, contractual agreement with its collaborators for the supply of what it does not know? Almost inevitably, the organisation seeks to cope with this fundamental uncertainty by forming committees to ensure that it receives as much information as possible and reveals as little as possible. Transaction costs mount, internal information channels become distorted (Teece, 1977), and other external sources of information, suspecting an exclusive agreement between the collaborators, become less

willing to supply information to the organisation (Macdonald, 1991). More difficulties arise when the information balance between the partners changes over time, as it often does. Such problems may help explain why a decade's enthusiasm for collaboration seems to be wearing just a little thin, with many organisations preferring either the total control they feel is provided by acquisition or merger, or looser network ties.

Informal means, as opposed to the formal means of the organisation, facilitate the acquisition of the external information required for innovation (von Hippel, 1987; Schrader, 1991; Conway, 1997). For instance, the importance of gatekeepers in exploiting their external contacts to bring information into their organisations is widely acknowledged. Their gatekeeping is totally informal. Much has been written about the role in innovation of the specialist information networks of key employees (see Davis and Wilkof, 1988). Such networks function through informal information exchange, with individuals giving information in order to receive it. Information exchange helps overcome one of the major obstacles to effecting information transactions – the problem of expressing demand for what is necessarily unknown. The exclusive network ensures that if a member finds value in information received through the network, he is likely to be able to supply information that other members will also find valuable. This is simply because information is required to use information; a member cannot find value in information unless he has other compatible information of his own, information which he is also able to supply in exchange for that received (Macdonald, 1992). Exchange need not be immediate or direct; eventual receipt through multilateral exchange is quite acceptable. For perpetual failure to supply, the penalty is ostracism from the network.

The gatekeeper may also exploit networks rather than simple contacts, but his primary distinction is that he passes on information to others in the organisation for them to use: the key employee exploits his networks for information for his own exclusive use (Macdonald and Williams, 1993). What they have in common is that both acquire external information for their own profit, with their employer benefiting only indirectly. Moreover, in order to acquire this information from external networks, both must proffer information. Those who exploit networks in this way cannot possibly distinguish between the organisation's information and their own; they contribute information they think will be valued to members of the network in order to receive valuable information in eventual and often indirect return, which they will also consider to be their own property. These personal networks are extremely likely to include employees of rival organisations. Not surprisingly, information exchange in personal networks is easily mistaken for industrial espionage. When steps are taken to curtail industrial espionage, intricate and delicate network mechanisms may be damaged. When this happens, the organisation's capacity to innovate, and hence to compete, may suffer.

> "It is correct, inevitable and regrettable that restriction of technology transfer must lead to restriction of technological information: technology is information. But we have some reason to be apprehensive about rules formulated in this area. So much technology lies in people's heads. Most foreseeable rules are going to ask them to put a fence down the middle of their minds and be careful at all times, know and remember to whom they are talking and just what they are supposed to know and not know. We have all had to do this in our time, but it is a mental burden. This is tolerable for limited numbers of people in limited circumstances. It becomes almost intolerable if spread over the vast range of people knowledgeable about dual-purpose technologies and it is an intolerable handicap to the kind of free-wheeling discussions over a beer which generate so many scientific and technical advances." (Appleyard, 1985, p.6)

3 National security export controls

Dual use technology – that which is considered to have both military and commercial applications – is subject to an array of export controls in the West and especially in the USA. During the Cold War, these controls were directed against the Soviet Bloc and, more pertinently, had come to be focussed on preventing the export of information. With some justification, it was argued that the core of new technology was not hardware, but rather the information required to make and operate the hardware.

> "..... control of design and manufacturing know how is absolutely vital for the maintenance of US technological superiority. Compared to this, all other considerations are secondary." (Department of Defense, 1976, p.iii)

> "..... there is unanimous agreement that the detail of how to do things is the essence of the technologies. This body of detail is hard earned and hard learned. It is not likely to be transferred inadvertently. But it can be taught and learned." (Department of Defense, 1976, p.3)

This emphasis on the importance of information was sound enough in theory, but difficulties were encountered when the theory was translated into practice. It is hard to know what someone else knows until this has been revealed, by which time it is obviously too late to prevent revelation. A solution to the problem was sought in establishing categories of information to be protected. Lists of the most precious information rapidly became far too cumbersome to be manageable.

> "The MCTL [Militarily Critical Technologies List] is the size of the New York phone book and worth a lot less. It's a bastardization of the concept of critical technology. The bureaucrats have taken a clear concept and turned it into a two inch document that's absolutely worthless." (Fred Bucy as quoted in Schatz, 1983)

Another response to this basic problem was to broaden the focus of regulations so that they encompassed not just specific bits of information, but whole subject areas. Thus, for example, export controls came to prohibit the unauthorised delivery of papers on certain subjects at conferences, not because the papers necessarily contained secrets, but because the whole discipline had been proscribed (Macdonald, 1990a; 1990b). While the authorities insisted that only a tiny proportion of information was actually declared secret, the impact on overall information flow may nevertheless have been considerable.

> "Now the technical societies are finding that scientists and engineers are bowing out of presentations at conferences just to avoid trouble, not because there is any real technology transfer problem." (Gregory, 1984, p.13)

A response with more fundamental implications was to shift attention from information itself to the means by which information might be transferred. Why struggle with the intangible when it was so much easier to control the tangible? Organisational systems could be designed to secure information and their security could be verified. It is an awkward characteristic of information that it can be passed on undiminished by use; systems had to be comprehensive if they were to be effective. There was no point preventing the transfer of information from the US to the Soviet Bloc if the Soviet Bloc could obtain the same information elsewhere. Nor could information be allowed to flow freely within the USA, being stopped only at the borders. If transfer of information to foreign countries was to be curtailed, then so had transfer to foreigners within the

USA and, naturally, transfer to US citizens who might talk to foreigners, and so on. Developed to absurdity – as it was – the argument insists that no information is secure as long as anyone talks about anything.

> "You have got to question about the validity of the firm you are dealing with, especially a foreign firm. Go to the FBI, ask questions. The FBI has recently sought to publicize their efforts in this problem in our particular area by putting up billboards similar to the World War II type of thing about the walls having ears." (D. Southard as quoted in Committee on Government Affairs, 1982, p.53)

> "Corporate executive and leaders of the business community must not only be understanding of the need for compliance and be supportive of the government's export control efforts, they must translate this state of mind into effective action by their company staff, managers and supervisors." (Wu, 1983)

As government itself could hardly prevent people talking to each other, responsibility was delegated. Organisations were to install compliance regimes sufficiently rigorous to satisfy the authorities that information could not flow freely. As penalties for failure to comply were both harsh and arbitrary, and it was never clear just how much compliance was required, organisations tended to over-comply rather than under-comply. They compiled huge manuals detailing where information was allowed to go within the organisation, installing virtual 'need to know' regimes in which employees were instructed to tell their colleagues nothing that was not absolutely necessary. External links were severed not only with blacklisted organisations, but also with suspect organisations, and with organisations that had any connection with suspect organisations.

Just how damaging to innovation has this period of espionage paranoia been? It is hard to say. Calculations of the cost of export controls to US industry were never encouraged, it being argued that they had to be weighed against the infinite value of national security (see Cahill, 1987). Whatever the costs to industry, they would always be swamped by the increase in defence expenditure which would be necessary should proscribed information reach the Soviet Bloc (Office of the Undersecretary of Defense for Policy, 1985). Such a conclusion was inevitable from a supposition that relaxation of controls on information in the West would lead to the acquisition of information by the Soviet Bloc which would be turned immediately into innovation that would pose an increased strategic threat to the USA. When calculations were eventually made, they concentrated on the advantage foreign competitors reaped through US controls being more stringent than controls elsewhere in the West (National Academy of Sciences, 1987; 1991).

If the problems the Soviet Bloc might encounter realising so much innovation were never raised, only occasionally was there any consideration of the problems export controls might pose for innovation in the West.

> "In theory, controlling the flow of 'know how' is a much more powerful defense than controlling product exports. But every time we make that decision, by classifying the knowledge, we pay a high price in slowed innovation rate." (L. Branscomb as quoted in Senate Judiciary Committee, 1988)

In part, this failure to consider the wider implications of restricting the flow of information was a product of a genuine confusion over the role of military strength in national security and that of commercial strength (Macdonald, 1990a; 1990b). Any diminution in US technological superiority was seen to threaten US national security, and

other Western nations, especially the Japanese, were eroding the technological lead of the US throughout the 1980s. Once it was accepted that measures to protect this lead enhanced national security, then it seemed to follow that measures to enhance national security could legitimately be directed at protecting the technological lead of the USA. But concentration on information as an instrument of policy also confused the issue. The vital contribution of know how to successful technology transfer had been appreciated in the Department of Defense long before that Department turned its attention to trying to control information. The inevitable inadequacy of its attempts to protect information always justified yet more drastic action, justification which was to prove invaluable in the Department's turf battle with the Department of Commerce to determine the legitimacy of Defense interests in industry and technology policy. Commerce survived as a combatant only by adopting the same weapon as Defense – the argument that, for the sake of national security, information must be protected.

4 Concluding thoughts

Few firms in the West protested about the debilitating effect of export controls on their capacity to innovate. No doubt they were discouraged by the severity of the penalties imposed on organisations thought to be uncooperative, but perhaps also by their own uncertainty about how information flows. It is hard to counter the argument that because information is essential to innovation, and hence to competitiveness, it should be carefully guarded. It is harder still to go further and argue that, for the sake of innovation and increased competitiveness, information should be given away, even to competitors. That the most effective means of doing this is to allow individual employees to operate on their own account, exchanging what may well be the firm's information for their own benefit and accountable to no one, is just about impossible for the organisation's senior management to swallow. Even in industries where such behaviour is rife and accepted as crucial to innovation, senior management is no more than tolerant of the situation.

If reason enough has not been presented for the attitude of senior managers, there is more. The use to which information is put in organisations extends well beyond innovation; its main use is in simply keeping the organisation operational, a use which often resists and resents incorporation of the new information required for innovation. In addition, the control systems of organisations are dependent on information channels which largely duplicate the organisation's hierarchical structure; information entering the organisation by informal means and flowing through non-organisational channels can easily be perceived as a threat to this structure. Information is also a source of power for individuals within the organisation, dispensed as much to those who will be pleased to know, and will pay for their pleasure, as to those who need to know (Pettigrew, 1972). And lastly, it is not the general perception of most managers that they are actually short of information. On the contrary, their typical complaint is that they already have far too much. Consequently, they feel little inclination to encourage dubious methods to acquire yet more. Anyway, there is perhaps little that senior management can do to encourage the informal flow of information for innovation (see Blois, 1999). Of its very nature, organisational involvement would rob this information flow of the very informality which allows it to make such a valuable contribution to innovation.

What, then, might be done? Senior managers may be powerless to encourage informal information flow, but this does not mean that they cannot discourage it. They can do so with great ease; almost by accident, in fact. So complex and sophisticated are informal information networks that any of a number of actions by the firm may disrupt information flow. For instance, the golden handcuffs that encourage an employee to remain with an employer may well constrain the human mobility which seems to be an important accompaniment to personal information networks. Most obvious of all, actions to prevent industrial espionage strike at the heart of informal information exchange. They need not. In practice, there is no confusion between industrial espionage and the exchange of information in personal networks. Such networks are extremely unlikely to be leaky; their members do not give away freely what is so valuable for use in exchange. Nor is there any reason at all why a network member wishing to sell proprietary information should do so via such a subtle, complex and on-going arrangement as an exchange network. A single, simple cash transaction is very much easier, and can be anonymous. Moreover, any reward received from industrial espionage would have to be sufficiently large to compensate the individual for permanent exclusion from the network; it would have to exceed the cost of impaired ability to function in existing employment, and to gain new employment. Implicit in industrial espionage is the devastating admission that the individual is less capable of making use of the information transferred than someone else (Cohen, 1983). Where mobility is high and it is practical to move to where information can be used, such an admission is ruinous to peer esteem and terminates network membership (see Cooper and Bruno, 1977). In the same way, using the network to transfer highly codified information is simply regarded by other network members as crass behaviour. Networks are inappropriate for transferring such information in much the same way that an academic publication is inappropriate for conveying details of a firm's balance sheet. Personal networks are an efficient means of transferring the tacit and uncodified information that is so hard to transfer by other means – and that is so essential for innovation.

Were senior managers to appreciate the distinction between information flow through industrial espionage and that through informal information networks, they would be better placed to defend the latter against efforts to prevent the former. They might even conclude that, so important are informal information networks for the organisation's innovation, it is worth tolerating a degree of industrial espionage so that they are not threatened. Then again, they might not (Oliver and Liebeskind, 1997). Perhaps a different argument altogether is required, one that starts from the proposition that it is actually rather hard to transfer information for innovation. With effort and understanding of the nature of the good, it can be done, and the innovation which contributes to competitiveness can result. From this perspective, the capacity of industrial espionage to transfer information is puny, and enormous efforts to prevent it pointless. Most managers in most organisations do not share this view. Their instinctive reaction to protect valuable information overwhelms the logic of innovation. In this intellectual climate, the primitive language of export controls is easily understood and readily adopted.

> "The future trend is to limit the amount of people with security clearance and restrict classified information on a 'need to know' basis. If there is no clear reason for an individual to know a secret, access to the secret will not be allowed." (Olney, 1988)

Most managers, of course, will not often confront industrial espionage, and efforts to prevent it will not occupy much of their working lives. But attitudes to industrial espionage are simply an extreme example of attitudes to information which are much more common. Information mercantilism is rife; managers see the organisation as an information fortress and themselves as guardians of the organisation's information property. They recognise the importance of information to the organisation's innovation in terms of intellectual property rights (Macdonald, 2004) and such notions as the learning organisation and knowledge management (von Krogh, 2003); they lack concomitant appreciation of the peculiar characteristics of information. This leads to acceptance of a profusion of new management methods which appear to address the problem of acquiring external information, but which ignore these basic characteristics (see Abrahamson, 1996; Sturdy, 1997; Collins, 2000). For instance, just in time may confine information flow to a few suppliers, and benchmarking encourages comparison with only the obvious competitors. Notions of getting close to the customer, of being customer-driven, seem only to increase the entitlement to information, and therefore the power, of marketing departments, and to isolate further other parts of the organisation from external information (Macdonald, 1995). The four opinions below are from managers in a large telecommunications company (see Macdonald, 1998):

> "Why should anyone but Marketing have contact with the customers? The customers are our business. We keep other parts of [the organisation] informed on a need to know basis."
>
> "R&D people are naive from a business point of view. They will tell you confidential stuff. I'm just amazed by the leakage that can occur."
>
> "We couldn't have our customers meeting an engineer with a cup of coffee and a fag hanging out of his mouth."
>
> "The old club atmosphere is going. There is a new gloss on what [the R&D Department] does. We used to get warts and all. Now [R&D] has commercial secrets to guard. Some time ago we stopped [R&D] giving papers externally."

The challenge for the manager, then, is to accept the consequences of information being fundamentally different from other goods. Information must come into the organisation for the innovation critical to its competitiveness, but is unlikely to do this unless information also goes out in exchange. These exchange transactions are much more efficient when they are carried out by employees rather than by the organisation itself, employees trading in the organisation's information as well as their own, and for their own benefit. The organisation cannot encourage these transactions without stripping them of the informality that allows them to work. The most that managers can do is tolerate them, but toleration requires justification in terms of the characteristics of information, a justification with which many managers are not familiar. Toleration also requires that managers surrender a degree of their control over the very resource which bestows authority and allows them to exert control. Managing with control and by method is easy: management by persuasion and instinct much more difficult. For managers, leaving the acquisition of external information to employees is very far from being the obvious option it might seem.

References

Abrahamson, E. (1996) 'Management fashion', *Academy of Management Review*, Vol. 21, No. 1, pp.254–285.

Appleyard, R. (1985) 'Intervention', *Papers Presented at the Workshop on International Technology Transfer: Promotion and Barriers*, Six Countries Programme on Aspects of Government Policies towards Technological Innovation in Industry, Ottawa, May, p.6.

Blois, K. (1999) 'Trust in business to business relationships: an evaluation of its status', *Journal of Management Studies*, Vol. 36, No. 2, pp.197–215.

Braun, E. and Macdonald, S (1982) *Revolution in Miniature. The History and Impact of Semiconductor Electronics*, Cambridge: Cambridge University Press.

Bronson, J. (1987) 'Unfriendly eyes', *IEEE Transactions on Professional Communication*, Vol. 30, No. 3, pp.173–178.

Cahill, K. (1987) *Trade Wars*, London: W.H. Allen.

Carter, R. (1989) 'Careless words cost business', *Accountancy*, Vol. 103, No. 1147, pp.158–160.

Cohen, D. (1983) *Labor Mobility and Trade Secrets in Knowledge-Intensive Industries*, paper presented to TIP workshop, Economics Department, Stanford University, June.

Collins, D. (2000) 'Management fads and buzzwords', *Critical-Practical Perspectives*, London: Routledge.

Conway, S. (1997) 'Strategic personal links in successful innovation: linch-pins, bridges and liaisons', *Creativity and Innovation Management*, Vol. 6, No. 4, pp.226–233.

Cooper, A. and Bruno, A. (1977) 'Success among high-technology firms', *Business Horizons*, Vol. 20, No. 2, pp.16–22.

Davis, P. and Wilkof, M. (1988) 'Scientific and technical information transfer for high technology: keeping the figure in its ground', *R&D Management*, Vol. 18, No. 1, pp.45–58.

Department of Defense (1976) 'Science board task force on export of US technology', *An Analysis of Export Control of US Technology – A DOD Perspective*, Office of the Director of Defense Research and Engineering, Washington, DC, February.

Dodgson, M. (1993) *Technological Collaboration in Industry*, London: Routledge.

Edwards, E. (1987) 'Corporate espionage: legal but usually dishonest', *Management Accounting*, Vol. 65, No. 10, pp.18–19.

Gregory, W. (1984) 'The technology transfer mess', *Aviation Week and Space Technology*, May, Vol. 14, p.13.

Macdonald, S. (1985) 'Technology beyond machines', in E. Rhodes and D. Wield (Eds.) *Manufacturing Innovation and the Implementation of New Technologies*, Oxford: Blackwell, pp.41–49.

Macdonald, S. (1990a) *Strategic Export Controls. Hurting the East or Weakening the West?*, London: Economist Intelligence Unit.

Macdonald, S. (1990b) *Technology and the Tyranny of Export Controls. Whisper Who Dares*, London: Macmillan.

Macdonald, S. (1991) 'Formal collaboration and informal information flow', *International Journal of Technology Management*, Vol. 7, Nos. 1/3, pp.49–60.

Macdonald, S. (1992) 'Information networks and the exchange of information', in C. Antonelli (Ed.) *The Economics of Information Networks*, North-Holland, Amsterdam, pp.51–69.

Macdonald, S. (1993) 'Nothing either good or bad: industrial espionage and technology transfer', *International Journal of Technology Management*, Vol. 8, Nos. 1/2, pp.95–105.

Macdonald, S. (1995) 'Too close for comfort? Implications for strategy and change arising from getting close to the customer', *California Management Review*, Vol. 37, No. 4, pp.8–27.

Macdonald, S. (1998) 'Notions of network: some implications for telecommunications of differences in perception' in S. Macdonald and G. Madden (Eds.) *Telecommunications and Socio-Economic Development*, North-Holland, Amsterdam, pp.295–312.

Macdonald, S. (2004) 'When means become ends. Considering the impact of patent strategy on innovation', *Information Economics and Policy*, Vol. 16, No. 1, pp.135–158.

Macdonald, S. and Williams, C. (1993) 'Beyond the boundary: an information perspective on the role of the gatekeeper in the organization', *Journal of Product Innovation Management*, Vol. 10, pp.417–427.

National Academy of Sciences (1987) *US National Security Export Controls and Global Economic Competition*, Washington, DC: National Academy Press.

National Academy of Sciences (1991) *Finding Common Ground. US Export Controls in a Changes Global Environment*, Washington, DC: National Academy Press.

Office of the Undersecretary of Defense for Policy (1985) *Assessing the Effect of Technology Transfer on US/Western Security – A Defense Perspective*, Department of Defense, Washington, DC, February.

Oliver, A. and Liebeskind, J. (1997) 'Three levels of networking for sourcing intellectual capital in biotechnology: implications for studying interorganisational networks', *International Studies of Management and Organisation*, Vol. 27, No. 4, pp.76–104.

Olney, C. (1988) 'The secret world of the industrial spy', *Business and Society Review*, Vol. 64, pp.28–32.

Pettigrew, A. (1972) 'Information control as a power resource', *Sociology*, Vol. 6, No. 2, pp.187–204.

Robertson, A. (1975) 'The effect on an organization of communication with the outside world: the relationship between free flow of information and an organization's effectiveness', *ASLIB Proceedings*, Vol. 27, No. 8, pp.339–345.

Rogers, E. (1982) 'Information exchange and technological innovation' in D. Sahal (Ed.) *The Transfer and Utilization of Technical Knowledge*, Lexington, MA: Lexington Books, pp.105–123.

Schatz, W. (1983) 'The hitch in high tech trade', *Datamation*, Vol. 29, No. 10, pp.148–159.

Schrader, S. (1991) 'Informal technology transfer between firms in cooperation through information trading', *Research Policy*, Vol. 20, pp.153–170.

Senate Hearings (1982) *Transfer of United States High Technology to the Soviet Union and Soviet Bloc Nations*, Permanent Subcommittee on Investigations, Committee on Government Affairs, Washington, DC: USGPO, p.53.

Senate Judiciary Committee (1988) *Testimony of L. Branscomb*, Subcommittee on Technology and Law, 16 March.

Sturdy, A. (1997) 'The dialectics of consultancy', *Critical Perspectives on Accounting*, Vol. 8, pp.511–535.

Teece, D. (1977) 'Technology transfer by multinational firms: the resource cost of transferring technological know-how', *Economic Journal*, Vol. 87, pp.242–261.

von Hippel, E. (1987) 'Cooperation between rivals: informal know-how trading', *Research Policy*, Vol. 16, pp.291–302.

von Hippel, E. (1988) *The Sources of Innovation*, New York: Oxford University Press.

von Krogh, G. (2003) 'Understanding the problem of knowledge sharing', *International Journal of Information Technology Management*, Vol. 2, No. 3, pp.173–183.

Wu, T. (1983) 'The citizen partner: a key force in effective strategic export control', *Signal*, August, pp.106–108.