No. 15-2003 ICCSR Research Paper Series - ISSN 1479-5124

In the company of spies: The ethics of industrial espionage

Andrew Crane

Research Paper Series
International Centre for Corporate Social Responsibility
ISSN 1479-5124

Editor: Dirk Matten

International Centre for Corporate Social Responsibility
Nottingham University Business School
Nottingham University
Jubilee Campus
Wollaton Road
Nottingham NG8 1BB
United Kingdom
Phone +44 (0)115 95 15261
Fax +44 (0)115 84 66667
Email dirk.matten@nottingham.ac.uk
www.nottingham.ac.uk/business/ICCSR

In the company of spies: The ethics of industrial espionage

Andrew Crane

Abstract

This paper takes a critical look at the practice of industrial espionage. By focusing on three recent cases of industrial espionage, involving major multinationals such as Proctor & Gamble, Unilever, Canal Plus, and Ericsson, light is shed on current developments in the competitive intelligence gathering 'industry' and the ethical problems that are typically surfaced. The argument is made that, from an ethical point of view, industrial espionage can be assessed according to three main considerations: the tactics used in the acquisition of information; the privacy of the information concerned; and the consequences for the public interest as a result of the deployment of the information by the intelligence gatherer. These issues are examined in the context of the three cases, and their implications for the overall definition and assessment of industrial espionage are considered.

The author:

Andrew Crane is a Senior Lecturer in Business Ethics at the International Centre for Corporate Social Responsibility (ICCSR) at the University of Nottingham, UK. He has a PhD from the University of Nottingham and a BSc from the University of Warwick. His current research interests include business ethics and organization, theoretical approaches to corporate citizenship, stakeholder communication, and organizational greening. He has published widely on these subjects in journals such as Academy of Management Review, European Journal of Marketing, Journal of Business Research, Journal of Business Ethics, and Organization Studies.

Address for correspondence:

Dr Andrew Crane, International Centre for Corporate Social Responsibility, Nottingham University Business School, Nottingham University, Jubilee Campus, Wollaton Road, Nottingham NG8 1BB, United Kingdom, Email andrew.crane@nottingham.ac.uk.

Introduction

Espionage is a word that brings to mind James Bond movies, or the spy stories of John Le Carre. But in recent years, espionage has also become widely associated with business practice too. Industrial espionage is essentially a form of commercial intelligence gathering, usually, but not exclusively, on the part of industry competitors. With global competition intensifying, finding out about rivals' products and processes has become big business – and competitive intelligence gathering is increasingly seen as an important and largely acceptable form of market research. Although industry representatives, such as the society for Competitive Intelligence Professionals argue that industrial espionage, or spying, is both unethical and illegal, there is sometimes a fine line between the 'legitimate' tactics of competitive intelligence gathering and the 'illegitimate' practice of industrial espionage (Shing and Spence 2002).

In this paper, we shall look at some high profile cases where allegations of industrial espionage involving some of the world's top companies have hit the headlines, and in so doing, explore some of these grey areas between acceptable and unacceptable intelligence gathering practices. In order to do so, we shall begin with a brief outline of the nature of industrial espionage and competitive intelligence gathering. We shall then proceed to outline our three cases, before discussing the cases in terms of a set of ethical tests that should throw light on how to determine the acceptability or otherwise of the practices concerned. We shall conclude with a discussion of the nature and boundaries of industrial espionage in the contemporary business environment.

Industrial espionage and competitive intelligence gathering

All organizations collect and make use of some kind of information about their competitors and other organizations. Just as a university will typically investigate which courses are offered by other universities, or may ask a new member of staff about comparative practices at their previous employer, so too will companies take a keen interest in the products, policies, and processes undertaken by their rivals. Indeed, such intelligence gathering activities are very much a standard aspect of conventional market research and competitor benchmarking, and make for effective

competitive behaviour (Shing and Spence 2002). It could be argued, therefore, that any means of gathering information is acceptable in a competitive context. After all, competitors are typically seen as being in an on-going, zero-sum battle with each other for customers, resources, and other rewards. Why should organizations accord their competitors any specific ethical claim when these are the very businesses that they are vying with for such rewards? What rights could, say, Volkswagen possibly have in its competition for car customers with Volvo?

This is not actually as simple, or as redundant, a question as it might at first seem. Volkswagen certainly has a number of *legal rights* that are more or less protected by national and international trade agreements, and which Volvo must respect. These include the right to freely enter and leave the market, the right to set their own prices free from influence or coercion, and the right to inform potential customers about their products. In 2001, for example, over-the-counter drugs manufacturers in the UK finally capitulated to demands to remove retail price agreements that had prevented retailers from setting their own prices rather than those set by manufacturers (Meikle 2001).

It is a relatively short step from these legal rights to claim that a competitor also has some form of *moral claims* on an organization that go beyond those codified in law – for example some form of right to privacy, or a right to 'fair play'. Certainly, it is open to debate whether the mere fact of a competitive situation bestows upon an organization carte blanche to act in whatever way is necessary to beat their competitors, including lying, deception, providing false information about competitors to consumers, poaching staff, and other such questionable practices.

In addition to this arguments, it can also be contended that competitors and other organizations are, in some sense, *stakeholders* of a company (Spence, Coles, and Harris 2001). Looking to Freeman's (1984)'s now classic definition of a stakeholder, the first condition of being a stakeholder is that the constituency can be *harmed by* or *benefit from* the organization – a criterion clearly possessed by competitors (Spence et al. 2001). Competitors can experience a loss or gain of market share as a result of the actions of their rivals, they can experience a change in trading conditions (for example, their suppliers might switch to a competitor offering higher prices), or they

can face changes in the perception of their industry by customers, regulators, or other stakeholders as a result of the behaviour of their competitors.

Therefore, whichever way we look at it, there seems to be a reasonable case for suggesting that there are limits to acceptable forms of intelligence gathering, beyond which the practice might be considered unethical. Ordinarily we might expect the law to determine the boundary between acceptable and unacceptable practice, but with the rapid advancement in information and communication technologies, as well as the increasing professionalisation of the competitive intelligence industry, legal limits are not always as clear-cut as one might hope (Hallaq and Steinhorst 1994; Skapinker and Edgecliffe-Johnson 2001). Indeed, ethical issues in business typically come into play when the law is unable or unwilling to set such limits (Treviño and Nelson 1999). For this reason, we shall refrain from adopting Shing and Spence's (2002) somewhat simplistic distinction between *legal* 'competitive intelligence gathering' and *illegal* 'industrial espionage' – although this is not to deny that the lines of illegality may well at times be crossed.

Despite the redundancy of a legalistic definition, it is clear that industry professionals and commentators certainly do ascribe a pejorative meaning to the term 'industrial espionage', preferring instead the more neutral competitive or corporate intelligence (Edgecliffe-Johnson 2001b; Shing and Spence 2002). This suggests that there is (or there is seen to be) a normative difference between the two types of practices, regardless of whether they are actually legal or not. Therefore, it would seem to be reasonable to distinguish espionage as intelligence practices of *questionable ethics*.
Our task then is to determine at what point does industrial espionage constitute a potential ethical transgression? In order to answer this question, let us now look at some examples where accusations of industrial espionage have been levelled against intelligence gatherers.

Three cases of industrial espionage

Perhaps unsurprisingly, the world of industrial espionage only rarely seems to make it into the public eye, and there is little incentive either for errant companies, or those that have been the victim of intelligence breaches, to make their problems public.

Perhaps the most well known, and most widely publicised, incident of all is that of British Airways against Virgin Atlantic during the early part of the 1990s. The 'dirty tricks' campaign, which ultimately resulted in BA chairman Lord King issuing a public apology to Virgin in court, was alleged to have involved the accessing of confidential Virgin passenger information, impersonating Virgin staff, poaching of customers as they queued for Virgin tickets, theft of documents, a hostile smear campaign in the press, as well as aggressive predatory pricing aimed at putting Virgin out of business (Economist 1993). Such events though are now more than a decade old. Let us look at some more recent examples to see how the practices of competitive intelligence gathering and industrial espionage have developed.

1. Unilever falls victim to 'dumpster diving'

Probably the most well known incident of industrial espionage in recent years involved the archrival branded-goods companies Proctor & Gamble and Unilever. Known for their often fierce competition, the espionage scandal exploded in 2001 when it came to light that private investigators hired by Proctor & Gamble in the US to find out more about its competitor's hair care business, had sifted through rubbish bins outside Unilever's offices.

The investigators succeeded in gathering piles of unshredded documents relating to Unilever's plans for the shampoo market. Although not necessarily illegal – different countries, and even different states, have differing rules on the legal status of rubbish (Burns 2002; Skapinker and Edgecliffe-Johnson 2001) – the practice commonly known as 'dumpster diving' broke Proctor & Gamble's own internal guidelines on intelligence gathering. Alerted to the breach, Proctor & Gamble bosses decided to come clean to Unilever about the supposedly 'rogue operators' who had apparently overstepped the mark in their eagerness to provide high level intelligence.

Although the public details of the case remain sketchy, it has been suggested that it was the timing of the covert operations that would have been of particular concern to Unilever, coming as they did when the two companies were involved in an auction for the Clairol hair care brand – a competition which Proctor & Gamble ultimately won (Edgecliffe-Johnson 2001a). Moreover, some industry insiders have expressed

scepticism at the 'rogue operator' explanation offered by Proctor & Gamble (see Skapinker and Edgecliffe-Johnson 2001). For instance, it can be argued that companies who want to engage in dubious practices simply contract the work out to independent operators to 'do the dirty work' whilst providing 'plausible deniability' for the company in case the operation is exposed or goes wrong.

Following their own internal review of the breach, Unilever responded by threatening legal action against their rivals, seeking a reported 'tens of millions of dollars' in restitution (Edgecliffe-Johnson 2001a). The case was finally resolved when Proctor & Gamble made an out of court settlement of some $10m.

2. Canal Plus claims 'piracy' by rival

Another case of alleged espionage between bitter rivals, that this time did end up with a massive lawsuit (around $1bn), concerned the two huge media corporations, News Corporation and Vivendi Universal, and their combative chief executives, Rupert Murdoch and Jean-Marie Messier. Although the two media tycoons were not named in the suit itself, the dispute centred on allegations made in March 2002 by a Vivendi subsidiary, the French pay-TV company Canal Plus Technologies, against NDS, a UK based technology firm eighty per cent owned by News Corporation (Snoddy 2002).

NDS is responsible for providing the encryption services used by satellite television companies to prevent people viewing programmes they have not paid for. Canal Plus used a rival security technology, which, it claimed, NDS employees deliberately cracked, and then sent to hackers on the west coast of the US, to be published on a website used by software pirates. According to Canal Plus, NDS employed a 'sophisticated and well-funded' team of scientists to crack the codes on smart cards that protected the company's pay TV systems (Cassey 2002). Following the publication of its smart card codes on the web, pirates were able to watch pay channels for free, depriving the French company of millions in lost revenues. The failed UK company ITV Digital, a user of Canal Plus cards, also blamed such piracy for the loss of some £100m revenue, which ultimately contributed to the firm's collapse in 2002 (Cassey 2002).

The case, one among many suits and counter-suits in the ultra-competitive digital TV industry, also underlines the murky world of anti-piracy. NDS, for example, is known to have financially supported a UK hackers' website, supposedly to attract illegal counterfeiters in order to prosecute them (Snoddy 2002). Similarly, 'reverse engineering' of competitors' products in order to unravel the technology behind them, is common practice in this and other high tech industries. However, NDS vehemently refuted the allegation that it was involved in any way in actually sending the codes to pirates or placing them on hackers' websites. As the company's chief executive claimed, the allegations were 'outrageous and baseless' and merely served to cover up Canal Plus' 'inferior' technology and 'poor performance' (Cassey 2002).

At the time of writing, the case hadn't actually reached the courts – and increasingly looked like it might not. Whilst NDS revealed that it had spent over €2m in legal costs fighting the lawsuit in the first three months alone, it had also subsequently been presented with a lawsuit by another rival, Echostar Communications, based on similar allegations (Anon 2002a). However, in a surprise twist, in June 2002 Canal Plus suspended, and looked set to completely drop, the 'piracy' lawsuit. The move came as part of a deal between the two parent companies Vivendi and News Corporation, that was set to see the latter take over an Italian pay television company from Canal Plus for €1bn (Godson 2002).

3. Ericsson involved in spy scandal

If the two previous cases illustrated the tensions caused by intense competition between rivals, our final example shows that industrial espionage can also escalate to national security concerns.

Ericsson, the Swedish telecommunications company best known for its mobile phones, was the surprise subject of a major diplomatic incident in 2002. What many people probably don't know about Ericsson is that in addition to being one of the leading suppliers of mobile phones, it is also involved in developing highly sophisticated radar and missile guidance systems for Sweden's Gripen fighter plane, the country's main strike aircraft.

The events of the industrial espionage case centred on the alleged leaking of company information from Ericsson to a foreign intelligence service. Two Ericsson employees, and one former employee, were taken into custody suspected of passing on secret documents, and two further employees were suspended on suspicion of breaking company security rules. However, the employees were not particularly senior, and the company was quick to suggest that they had been caught quickly before a serious security breach could have occurred (Anon 2002b).

Nonetheless, the implications certainly became more serious when Sweden expelled two Russian diplomats who were said to be 'directly linked' to the industrial espionage case at Ericsson. Although the Swedish authorities and Ericsson were reluctant to disclose too many details, such developments gave clear indication that they believed that the Ericsson employees had been passing sensitive information to the Russians. Incensed at the expulsions, the Russians subsequently announced tit-for-tat expulsions of two Swedish diplomats, drawing accusations from Stockholm that they were returning to 'Soviet-era foreign policy' (Osborn 2002). Whichever way you look at it then, Ericsson had clearly got itself embroiled in a case of industrial espionage that not only threatened its own reputation for information security, but even had major implications for diplomatic relations in its home country and in the rest of Europe.

Discussion

Are these three cases really examples of industrial espionage? Have they crossed the boundaries of acceptable practice? What do they tell us about the nature of contemporary intelligence gathering and industrial espionage?

In order to begin answering such questions, we need to develop some kind of framework for assessing the types of practices outlined in the cases. To this end, we would like to suggest the following criteria to determine whether ethical problems could be said to have arisen in intelligence gathering. Specifically, one might suggest that ethical problems occur when one or more of the following are deemed to have occurred:

a) The *tactics* used to secure information are questionable since they appear to go beyond what might be deemed acceptable, ethical, or legal business practice;
b) The *nature* of the information sought can itself be regarded as in some way private or confidential;
c) The *purposes* for which the information is to be used are against the public interest.

These three issues, or 'tests' if one prefers, are not mutually exclusive, and indeed, it is often difficult to disentangle one from another. Nonetheless, they represent important first steps in assessing the ethics of industrial espionage. Let us look at them in a little more detail.

Questionable tactics may take many forms, from the clearly illegal, such as breaking and entering a competitors' offices to steal information or installing tapping devices, to rather more grey areas. This includes searching through a competitors rubbish, hiring private detectives, infiltrating competitor organizations with industrial 'spies', covert surveillance through spy cameras, contacting competitors in a fake guise such as a potential customer or supplier, interviewing competitors' employees for a bogus job vacancy, and pressuring the customers or suppliers of competitors to reveal sensitive information about their operations (Hallaq and Steinhorst 1994). These are all tactics that have been, and indeed continue to be used, by intelligence gatherers in industry.

Such tactics are of dubious ethicality primarily because they violate a duty to be honest and truthful in business dealings (Boatright 2000: 141). They might therefore be criticised from the perspective of what are called *deontological* precepts such as the 'golden rule' – do unto others as you would have them do unto you – or Kant's categorical imperative. This basically states that actions are only acceptable if one is willing to allow the rule or maxim underlying the action to be universalised for all. Such a test poses problems for certain forms of intelligence gathering because, once they become accepted into business practice – or to use Kant's words, they become 'universal law' – all firms tend to lose out. This might be because: a) the industry

starts to suffer from a surfeit of trust; and/or b) it becomes necessary for all industry players to commit resources to institute procedures guarding against the loss of trade secrets to unscrupulous competitors (Boatright 2000: 141).

Such issues of questionable tactics were primarily the problems raised by the Unilever case, since the intelligence agents hired by their rivals overstepped the mark in the way in which they sought to obtain data. The fact that the data might be deemed 'private' is really a secondary issue since even if the agents had only uncovered publicly available material their 'dumpster diving' practices would still have raised concerns, and would still have breached Proctor & Gamble's ethical guidelines on information gathering. This case illustrates well the limitations of the law in determining acceptable practice, especially given the variable and indeterminate property status of discarded waste. Of course, determining where exactly 'questionable' practices become 'unethical' ones is not exactly clear cut either, but application of the golden rule and other deontological principles can help to clarify this position.

Private or confidential information may refer to any kind of information which the organization feels should not be freely available to outsiders and which therefore should be some kind of moral or legal protection. Whilst in principle this seems quite reasonable, it is rather more difficult to establish a corporation's right to privacy than it is an individual's – and certainly, the enforcement of privacy is considerably trickier. Specifically:

- Corporations are to some extent 'boundary-less' – they have fewer clear boundaries to define the private 'corporate space' compared with private individuals.
- Corporations consist of, and deal with, multiple individuals and this makes the control of information difficult.
- Much corporate activity takes place in public and quasi-public spaces such as shops, offices, hospitals, colleges etc, and via shared infrastructure such as roads, railways, seas, telephone lines, fibre optic cables, etc. These are easily and usually quite legitimately observed, infiltrated, or tracked.

However, even if it is difficult to fully ascribe a right to privacy upon corporations, it is relatively more straightforward to suggest that certain information that corporations have is a form of property and is thus subject to *property rights* (Boatright 2000: 132). This particularly tends to apply to trade secrets, patents, copyrights, and trademarks – all of which are to some extent legally enforceable intellectual property that is said to belong to the organization. Intellectual property rights can be assigned to many intangible forms of property, including product formulations, theories, inventions, software, music, formulae, recipes, processing techniques, designs, and so on. The development of such 'information' frequently involves organizations in millions of Euros investment in R&D costs. Unsurprisingly then, corporations often go to great lengths and invest substantial resources in trying to keep this information secret from their competitors so that they may reap the rewards of their investment.

With improvements in information and communication technologies, the ease of replication of digital information, as well as the refinement of 'reverse engineering' techniques (where competitors' products are stripped down and analysed in order to copy them), the unauthorised accessing and exploitation of intellectual property has been on the rise (Shapiro 1998). Moreover, the emergence of new technologies will continue to spark new ethical debates about what constitutes intellectual property and what restrictions can and should be put on different forms of property, including human and plant genes, and digital information.

This latter form of property, digital information, is what was primarily at stake in the Canal Plus case, and illustrates well the problems of ascribing ownership to non-tangible assets. The 'theft' or 'hacking' of sensitive digital information has become a major risk for high tech companies of various sorts, and intellectual property infringements on digital information have been the subject of numerous recent cases, including the record industry's battle against Napster, the internet music-swapping service (see Grimes 2002). For Canal Plus, as with the record industry, protection of this information is crucial to their survival, and whether it is targeted by rival companies (such as NDS) or even individuals or 'hackers' seeking to embarrass the company or to make the information freely available to themselves or others, the consequences can be devastating.

Issues of property rights and 'theft' of proprietary information typically are left to the courts, although statute is often slow to catch up with these new forms of 'property'. Moreover, contexts such as the internet are located in a transnational space that is difficult if not impossible to police. And then there are some cultures, most notably in Asia, where different notions of property rights prevail. Muskin (2000) suggests that whilst European, and even more so US, companies might expect the granting of exclusive rights to any novel technologies they develop, in Asia innovation is often seen as a public good to be used for the advance of technology by all.

Overall then, it would still seem to be incumbent upon corporations, at least to some extent, to define their own limits of acceptable practice regarding the derivation and use of potentially private or confidential information. Whilst it may seem that there will always be substantial rewards for firms willing and able to seek out such data, one can again also make the argument that there are also rewards for the industry as a whole if firms collaborate to ensure greater security for all. Thus, just as firms in the finance industry and in record industry have worked together to try and fight against security breaches, so too might digital TV companies derive benefits from collaboration. As we have argued earlier in the article, competition does not always have to be seen as a zero-sum game.

Finally, **public interest** issues can arise when the information gleaned through intelligence gathering is put to purposes such as anti-competitive behaviour, including the deliberate removal or ruin of competitors, price inflation, or entrenchment of a monopoly position. Public interest issues may also arise when corporate intelligence germane to national or international security or domestic economic performance is secured. With corporations involved in designing, producing, and servicing military hardware and software, governmental data storage, and other security-related products and services, the accessing of company data by competitors (especially from overseas), or even foreign governmental agencies can lead to threats to the public interest.

Unsurprisingly, public interest issues usually rest on consequentialist reasoning, namely that the action can be said to cause an overall aggregate reduction in happiness for affected members of society. Should competition be reduced as a

result of industrial espionage then the public may suffer because of increased prices and lower innovation over the long term. Spying related to military or other sensitive information may harm the public through increased exposure to risks of various kinds. Clearly, these were the main concerns raised by the Ericsson case. Whilst private or confidential information was certainly involved, it was the use to which the information may have been applied that was of particular concern here, not the fact that it was private in the first place.

Public interest concerns add an extra dimension to issues of privacy and commercial confidentiality. The issue is not so much that certain information is 'owned' by a corporation, but whether the ability to use that ownership to restrict access to others is ultimately in the best interests of the public. This can work both ways for corporations. In the case of Ericsson, the argument would be that protection of information about the company's products was necessary to promote Sweden's security interests, and any violations would have been ethically undesirable. It is notable that even in the Canal Plus case discussed above, investigations were not only made by the French company's own lawyers, but also by the French secret service. The service's industrial espionage division was thought to have started enquiries into case because it affected French industrial policy – again, a public interest issue (see Doward 2002). Similarly, arguments for copyright, patents, and other forms of intellectual property sometimes rest less on rights and more on the benefits that such protections bring in terms of encouraging innovation and ultimately improving economic performance.

Others though have made the case that intellectual property and commercial confidentiality can act *against* the public interest. For instance, the debate over the supply of cheap, generic, anti-retroviral AIDS treatments for less developed countries focused attention on the social benefits that a relaxation of patent protections could bring (Brennan and Baines 2002). Similarly, Nike and other apparel manufacturers have long been chastised by workers rights campaigners for claiming that the location of their supplier factories was 'commercially confidential', thus preventing campaigners from independently auditing conditions in the factories.

As with all consequentialist-based reasoning then, the question of whether an act of intelligence gathering is in the public interest will depend upon what assumptions and parameters are applied. In the Ericsson case, the situation might seem to be reasonably clearly doubtful on ethical grounds, but at the same time one would imagine that the so-called 'spies' involved would also claim to be acting in the (Russian) public's interest by revealing the company's confidential data. Without going into the political situation present at the time, such issues therefore remain surprisingly cloudy. However, one has to wonder what intelligence Ericsson might have possessed that should rightly have been beyond the purview of a country that is not only not in conflict with Sweden, but might even be considered its ally. It remains to be seen whether there were actually security issues at stake here as opposed to simply protection of domestic competitors from overseas rivals.

Conclusions

As the examples and the discussion above attest, industrial espionage has become a significant, and in many ways troubling, aspect of contemporary business practice. It would seem that even companies with an ethical policy on intelligence gathering might accidentally encourage, or even tacitly endorse, questionable behaviours on the part of employees or contracted agents. In an increasingly knowledge-based competitive environment, the incentives to overstep the mark in intelligence gathering have increased significantly, and with advances in information and communication technologies, the opportunities for doing so have multiplied accordingly. Moreover, the boundaries for defining acceptable practice have also become increasingly muddied, especially now that surveillance technologies and other 'spying' tools and gadgets have become so easily available to companies.

What we have also seen here is a blurring of boundaries between state and industrial espionage. On the one hand, companies are now intrinsically involved in the affairs of government (including defence, anti-terrorism, tax collection and investigation, welfare distribution, etc) meaning that much 'state' espionage is carried out through commercial entities. On the other hand, governments rely substantially on the success of domestic companies to further their own economic goals, meaning that

governments often have a major role to play in facilitating or preventing so-called 'industrial' espionage.

In assessing the three recent cases involving allegations of industrial espionage, we have set out three main ways in which we might determine the acceptability or otherwise of the actions involved. We have not done so in order to make definitive judgements on the three cases (or on other incidences of potential espionage), but rather to examine and illustrate the types of issues that might be at stake, and to give guidance on how to assess them. Industrial espionage is always going to remain in the grey areas of questionable business practice, and so the more we are able to make sense of the problems involved, the more able we will be to deal with them competently and rationally.

Ultimately though, perhaps the greatest lesson to learn here is that it is all too easy to think about and rationalize industrial espionage simply in the context of two fiercely competitive rivals such as Proctor & Gamble and Unilever, or News Corporation and Vivendi. Looking at it this way, it might seem that there will always be an overwhelming incentive to cross the ethical threshold of acceptable intelligence gathering in order to outdo one's enemy. However, if instead of thinking about businesses as one-to-one combatants, we consider them as mutual stakeholders operating within a web of other businesses, we might more easily recognise their mutual interests and interlinked flows of resources and rewards (see for example Easton 1992). As such, it is clear that industrial espionage has major implications for *all* industry players, whether they are directly involved in espionage activities or not. Businesses need to maintain confidence in their data integrity and security; they need to offer reliance in their attitude towards privacy; and perhaps most of all, they need to establish strong relationships of trust with their key stakeholders. An industry saddled with a reputation for spying and secrecy is unlikely to be a supportive context for any business to develop such capabilities. If employees, customers, suppliers, competitors, or even regulators believe they are in the company of spies, the challenge to maintain long-term business success will be all the more testing.

References

Anon. 2002a. Echstar begins piracy lawsuit against NDS. The Independent, 1 October 2002: 22.

Anon. 2002b. Two Ericsson spy case suspects freed from custody. www.reuters.com, 5 December 2002.

Boatright, J.R. 2000. Ethics and the Conduct of Business, (3rd ed.). Upper Saddle River, NJ: Prentice Hall.

Brennan, R. and Baines, P. 2002. Ethical aspects of drug pricing: GlaxoSmithKline and anti-retroviral drugs in South Africa. Paper presented at the 2002 Academy of Marketing Annual Conference, Nottingham.

Burns, J. 2002. Bribes and trash archaeology. Financial Times, 11 April 2002: 5.

Cassey, J. 2002. Top Murdoch lawyer to fight hacking claim. The Guardian, 18 March 2002: 7.

Doward, J. 2002. French agents probe Murdoch firm. The Observer, Business, 17 March 2002: 1.

Easton, G. 1992. Industrial networks: a review. In B. Axelsson and G. Easton (eds.), Industrial networks: a new view of reality: 3-27. London: Routledge.

Economist. 1993. Tactics and dirty tricks. Economist, 16 January 1993: 21-22.

Edgecliffe-Johnson, A. 2001a. P&G admits spying on Unilever. Financial Times, 31 August 2001: 17.

Edgecliffe-Johnson, A. 2001b. 'Trash archaeologists' hunt for meaning in a can of garbage. Financial Times, 3 September 2001: 12.

Freeman, R.E. 1984. Strategic management. A stakeholder approach. Boston: Pitman.

Godson, R. 2002. TV deal to end piracy action. Sunday Times, 9 June 2002.

Grimes, C. 2002. Napster sell-off is quiet finale. Financial Times, 5 September 2002: 23.

Hallaq, J.H. and Steinhorst, K. 1994. Business intelligence methods - how ethical. Journal of Business Ethics, 13: 787-794.

Meikle, J. 2001. £300m slashed off drugs as price fixing abandoned: chemists warn of closures as supermarkets cut costs of medicines. The Guardian, 16 May 2001: 3.

Muskin, J.B. 2000. Interorganizational ethics: standards of behavior. Journal of Business Ethics, 24: 283-297.

Osborn, A. 2002. Sweden expels Russian jet 'spies'. The Guardian, 12 November 2002.

Shapiro, B.R. 1998. Economic espionage. Marketing Management, 7 (1): 56-58.

Shing, M.N.K. and Spence, L.J. 2002. Investigating the limits of competitive intelligence gathering: is mystery shopping ethical? Business Ethics: A European Review, 11 (4): 343-353.

Skapinker, M. and Edgecliffe-Johnson, A. 2001. Tricks of the corporate spying game. Financial Times, 1 September 2001: 9.

Snoddy, R. 2002. Personal friction at heart of media battle. The Times, 20 March 2002.

Spence, L.J., Coles, A.-M., and Harris, L. 2001. The forgotten stakeholder? Ethics and social responsibility in relation to competitors. Business and Society Review, 106 (4): 331-352.

Treviño, L.K. and Nelson, K.A. 1999. Managing business ethics: straight talk about how to do it right. New York: John Wiley.

Research Paper Series
International Centre for Corporate Social Responsibility
ISSN 1479-5124

Editor: Dirk Matten

The ICCSR Research Papers Series is intended as a first-hand outlet for research output of ICCSR. These include papers presented at symposiums and seminars, first drafts of papers intended for submission in journals and other reports on ongoing or completed research projects.

The objective of the ICCSR Research Papers Series is twofold: First, there is a time goal: Given the quality of ICCSR publication, the targeted journals normally require large time spans between submission and publication. Consequently, the ICCSR Research Papers Series serves as a preliminary airing to working papers of ICCSR staff and affiliates which are intended for subsequent publication. By this, research output can be made available for a selected public which will not only establish ICCSR's lead in advancing and developing innovative research in CSR but will also open the opportunity to expose ideas to debate and peer scrutiny prior to submission and/or subsequent publication. Second, the ICCSR Research Papers Series offers the opportunity of publishing more extensive works of research than the usual space constraints of journals would normally allow. In particular, these papers will include research reports, data analysis, literature reviews, work by postgraduate students etc. which could serve as a primary data resource for further publications. Publication in the ICCSR Research Paper Series does not preclude publication in refereed journals.

The ICCSR Research Papers Series consequently is interested in assuring high quality and broad visibility in the field. The quality aspect will be assured by establishing a process of peer review, which will normally include the Editor of the ICCSR Research Papers Series and one further academic in the field. In order to achieve a reasonable visibility the ICCSR Research Papers Series has full ISSN recognition and is listed in major library catalogues worldwide. All papers can also be downloaded at the ICCSR website.

Published Papers

No. 01-2003 *Wendy Chapple & Richard Harris*
Accounting for solid waste generation in measures of regional productivity growth

No. 02-2003 *Christine Coupland*
Corporate identities on the web: An exercise in the construction and deployment of 'morality'

No. 03-2003 *David L. Owen*
Recent developments in European social and environmental reporting and auditing practice – A critical evaluation and tentative prognosis

No. 04-2003 *Dirk Matten & Andrew Crane*
Corporate Citizenship: Towards an extended theoretical conceptualization

No. 05-2003 *Karen Williams, Mike Geppert & Dirk Matten*
Challenges for the German model of employee relations in the era of globalization

No. 06-2003 *Iain A. Davies & Andrew Crane*
Ethical Decision Making in Fair Trade Companies

No. 07-2003 *Robert J. Caruana*
Morality in consumption: Towards a sociological perspective

No. 08-2003 *Edd de Coverly, Lisa O'Malley & Maurice Patterson*
Hidden mountain: The social avoidance of waste

No. 09-2003 *Eleanor Chambers, Wendy Chapple, Jeremy Moon & Michael Sullivan*
CSR in Asia: A seven country study of CSR website reporting

No. 10-2003 *Anita Fernandez Young & Robert Young*
Corporate Social Responsibility: the effects of the Federal Corporate Sentencing Guidelines on a representative self-interested corporation

No. 11-2003 *Simon Ashby, Swee Hoon Chuah & Robert Hoffmann*
Industry self-regulation: A game-theoretic typology of strategic voluntary compliance

No. 12-2003 *David A. Waldman, Donald Siegel & Mansour Javidan*
Transformational leadership and CSR: A meso level approach

No. 13-2003 *Jeremy Moon, Andrew Crane & Dirk Matten*
Can corporations be citizens? Corporate citizenship as a metaphor for business participation in society (2nd Edition)

No. 14-2003 *Anita Fernandez Young, Jeremy Moon & Robert Young*
The UK Corporate Social Responsibility consultancy industry: a phenomenological approach

No. 15-2003 *Andrew Crane*
In the company of spies: The ethics of industrial espionage