DECEPTIVE AND MISLEADING ON-LINE ADVERTISING AND BUSINESS PRACTICES

Dr Russell G. Smith
Australian Institute of Criminology
Email: russell.smith@aic.gov.au
ABSTRACT

This paper considers the extent to which digital communications technologies are being used in misleading and deceptive ways to advertise goods and services, and how problems of this nature can best be dealt with. Four types of misleading and deceptive on-line practices are considered—pretending to sell something you don’t have whilst taking the money in advance; supplying goods or services which are of a lower quality than the goods or services paid for, or failing to supply the goods and services sought at all; persuading customers to buy something they do not really want through oppressive marketing techniques; and disguising one’s identity in order to perpetrate a fraud. A range of hard and soft regulatory responses are considered along with various on-line preventive strategies including the use of on-line surveillance, consumer warnings, and on-line authentication technologies. Although there remains a place for legal controls, it is concluded that the most effective strategies lie in making consumers aware of the risks they face and informed about the nature of misleading and deceptive practices which are present. In this regard, the use of certification and notification systems, which permit consumers to identify businesses which have been found to be trustworthy, seem to provide the best option. Steps need to be taken, however, to ensure that those with the necessary technological expertise are unable to manipulate such systems and thus undo the benefits which they seek to provide.
The Nature and Extent of On-Line Misleading and Deceptive Practices

Traditional misleading and deceptive practices, generally fall within four categories: pretending to sell something you don’t have whilst taking the money in advance; supplying goods or services which are of a lower quality than the goods or services paid for, or failing to supply the goods and services sought at all; persuading customers to buy something they do not really want through oppressive marketing techniques; and disguising one’s identity in order to perpetrate a fraud. These practices have always existed and the old adage that ‘fools and their money are easily parted’ remains as apt now as it did in less technologically-advanced times.

In the traditional market-place, many of these risks could be reduced by consumers being able to inspect the product they wanted to buy before parting with their money. Merchants were also able to receive cash in hand before parting with their goods. In the on-line world, however, the risks both to merchants and to consumers have increased greatly as goods and services are generally unable to be inspected prior to the transaction being concluded. Cash payments have also been replaced by electronic transfers of funds with the potential for transactions to be concluded instantaneously. These developments, whilst increasing the speed and efficiency of business transactions, also substantially increase the opportunities for fraud and illegality to take place.

Deceptive practices are easier to carry out electronically than using traditional practices because it is a relatively simple task to make one’s self appear legitimate on-line. Through the use of sophisticated Web page designs, it is much easier to disguise intent and to present a scheme in a positive light, and the pool of potential victims is greatly enhanced through the use of extensive electronic mailing techniques. In addition, the financial outlays required for on-line merchants to set-up business are much less than with traditional forms of marketing, as offices are not required and stationery and staff costs are reduced. In the electronic marketplace it is also easy for fraudulent businesses to disguise their true identities, to hide, to shut down or to move to a new location when the illegal nature of their activities starts to become apparent.

The Internet also enables the traditional boundaries between information, advertising and entertainment to blur. Consumers are able to be tricked into believing that the facts they have been supplied with are objective and reliable, when in fact they are merely advertising puffs. The use of such techniques when accompanied by exotic graphic and audio displays has proven to be an effective marketing strategy when directed at children. The use of hyperlinks embedded in information pages or search engine sites which direct users to advertising material can also be an insidious promotional technique in which readers are asked to believe that the linked material is of an objective, factual nature when in fact it is merely supportive of some specific advertised product. Hyperlinks have also been used to direct consumers to other sites which are covertly operated by the same business as the original site.

The extent to which deceptive and misleading practices take place on-line is difficult to quantify precisely, although some estimates have been attempted. One commentator has estimated that as much as ten per cent of on-line commerce may involve consumer fraud (Rothchild 1999, p. 897, n. 11). A worldwide clean-up operation, involving the Office of Fair Trading in Britain and its counterparts in twenty-two other countries, identified 1,159 potential ‘get rich quick’ schemes being advertised on Internet sites (Office of Fair Trading
In the United States, over 18,600 complaints were registered on the Federal Trade Commission’s fraud database ‘Consumer Sentinel’ in 1999, more than double the number in 1998 (United States, Department of Justice 2000).

In 1999, a survey was conducted at the University of Utah of Internet trading which was coordinated by Consumers International and funded by the European Union. Representatives of those groups bought more than 150 items from Web sites based in seventeen countries, and then tried to return them. It was found that eight percent of the items ordered never arrived; many Web sites did not give clear information about delivery charges; a minority disclosed whether the laws of the seller’s country or the buyer’s country would apply in the event of a dispute, and only fifty-three percent had a return policy. In addition, only about thirteen percent of the sites promised not to sell customers’ personal data to a third party and only thirty-two percent provided information on how to complain if there was a problem with a transaction (Clausing 1999). In Australia, the Australian Securities and Investments Commission (ASIC) and the Australian Competition and Consumer Commission (ACCC) have both found an increase in the extent to which the Internet is being used for deceptive practices in recent years.

What, then, is the nature of these misleading and deceptive practices, and how have they been adapted for use in the digital age?

**Types of Misleading and Deceptive On-Line Practices**

**Advance Fee Schemes**

The gist of so-called ‘advance fee schemes’ is to trick prospective victims into parting with funds by persuading them that they will receive a substantial benefit in return for providing some modest payment in advance. The characteristics of this type of fraudulent scheme usually entail enlisting the services of the prospective victim to assist in an activity of questionable legality, thus providing some assurance that the victim would be unlikely to report the matter to the police, once defrauded. Thus, the offender is able to carry out the scheme repeatedly, sometimes in respect of the same victim, whilst police are faced with difficulties in finding witnesses and securing evidence.

Examples of on-line advance fee schemes include pyramid schemes that have the primary purpose of enlisting individuals to earn money through recruiting other persons such as through the use of E-mail chain letters and electronic mailing lists. One recent example investigated by the ACCC involved the Canadian Global Interactive Investments Club which advertised the fact that offshore banks would issue low-interest Visa cards via the Internet with the promise of no credit checks or income verification. The scheme was actually an international pyramid scheme, in which applicants were encouraged to recruit others in return for $25 each (ACCC 1997b).

The Internet is also being used as a medium for Ponzi investment schemes and a variety of fraudulent business opportunity schemes as well as schemes that make use of on-line auctions and lotteries conducted electronically.

**Non-Delivery and Defective Products and Services**
Misleading advertising on the Internet may also involve the merchant failing to deliver the goods when and where requested, or at all. This problem is exacerbated in global commercial transactions where long-distance delivery of goods is involved, sometimes entailing customs clearance and the payment of importation taxes. Alternatively, defective goods may be delivered or the wrong ones supplied, in which case consumers need to arrange for return and the refund of the price paid and any expenses involved. Many of these problems arise out of the fact that the goods are unable to be physically examined on-line in the first place.

Problems are also created by reason of the immediacy of some transactions in which goods or services are obtained at exactly the same time as payment is authorised (e.g. the purchase of software downloaded after providing a credit card number). In such cases, the traditional methods of stopping payment on a cheque or withdrawing authorisation for a credit card purchase are unavailable.

As consumers continue to increase their use of the Internet so the number of complaints about Internet Service Providers has also increased. The ACCC, for example, has investigated allegations of overbilling, inadequate detail when billing, failure to supply technical support and other services as represented, failure to connect consumers to the Internet as agreed, not honouring requests to disconnect, the need to have a credit card to obtain services, attempts to avoid consumers’ legal rights, and misrepresentations about the speed of Internet access and the experience of the Service Provider (ACCC 1999).

The Internet is now being used to advertise cable television decryption kits which enable consumers to obtain cable television without paying contract fees. Not only do such kits seldom work but they also require consumers to break the law by stealing cable services.

In the digital age, it has also become possible to purchase a variety of digitised products by downloading them electronically. The Internet provides a comprehensive advertising medium for these products, often with on-line samples being provided free of charge. Once payment has been transmitted to the merchant, the purchaser is able to download the complete product along with appropriate licences for its use. If, however, the software has been illegally copied, or if it is defective in some way, the consumer is often disappointed having paid for a product which cannot legally be used.

One area of on-line commerce that has developed prolifically is that which concerns the provision of pornographic images and sexual services. Some of these involve misleading and deceptive conduct. One example involved a company which advertised ‘free’ erotic photographs on the Internet. In order to see the images, the user was required to download software which, once installed, took control of the user’s modem, cut off the local Internet Service Provider, and dialled a number in the former Soviet Republic of Moldova in Eastern Europe. The line remained open until the computer was turned off resulting in the user incurring large international telephone charges which were shared between the fraudster and the Moldovian telecommunications company. The fraud was detected through regular surveillance of customers’ telephone accounts and the FTC was able to obtain an order requiring the defendants to place US$1 million in an escrow account pending resolution of the case (Federal Trade Commission v Audiotex Connection Inc E.D.N.Y. Filed 13 February 1997).

Other on-line unlawful practices have included the advertising and sale of loan schemes, credit-repair kits, health and medicinal products such as cures for cancer and HIV, and
educational qualifications from on-line universities, some of which fail to provide recognised, or indeed, any, valid qualifications, or occasionally fail to deliver any educational programs at all.

**Unsolicited and Unwanted Goods and Services**

Traditionally, there were few controls on advertising conducted by mail and direct marketers inflicted a barrage of advertising material on unsuspecting, and often unwilling, recipients. The electronic equivalent, known as ‘spam’, entails the same idea carried out through the use of E:mail. Its future equivalents may be even more invasive with self-opening attachments which could carry viruses into the recipient’s computer hard drive causing damage and loss.

Bait advertising that involves the offer of a product or service for sale at an enticingly low price in order to sell some other more expensive product or service, or advertising a bargain which does not exist in order to attract customers to do business with the merchant is also able to be conducted electronically, as is inertia selling or sending unordered goods to consumers and billing them in the hope that they will accept the goods and pay the bill without question. Various statutes now make such practices illegal which would, arguably, apply where electronic goods or services are provided to on-line consumers without their request. One could imagine software being provided as a self-opening attachment to an E:mail message which would then be billed. Similarly, requiring payment for access to Internet sites could amount to a form of inertia selling of the service in question.

**Identification Deception**

The advent of on-line commerce has also created new forms of illegality which are less likely to occur in traditional marketplaces. Many consumers, for example, now have great difficulty in identifying those with whom they do business. Some merchants may intentionally disguise their identity through the use of remailing facilities in order later to defraud customers and avoid detection (see Rothchild 1999, p. 927). Others may simply be neglectful in providing accurate and verifiable information.

The technology of the Internet makes it relatively simple for users to disguise their identities. Electronic mail and Internet addresses may be manipulated by including details which are misleading or the source of a message may be made anonymous or changed so that it appears to be coming from another user. Similarly, there is no way of knowing the commercial affiliations of those on the Internet. Referees for businesses or products might, in fact, be individuals employed specifically to indicate their approval of the venture or product in question.

Businesses might also choose legitimate-sounding names in order to improve their credibility or include domain names which are misleading. There has recently developed a practice in the United States and Canada of some businesses adopting domain names containing the names of Australian cities in order to improve their marketability and credibility, despite the fact that they have no connection at all with Australia.

In one case investigated by the ACCC (1997b), an Internet trader used the same domain name as another trader (the original bearer of the name), but with a <.com> suffix, as opposed to the <.net> suffix of the original site. The confusion created as to the identity of the actual proprietor of the site allowed consumers to be misled or deceived. The <.com> site did,
however, include an inconspicuous notice stating that the site should not be confused with the <.net> site of the same name, although this could easily have been overlooked by those visiting the site.

**Hard Regulation**

The regulation of advertising and marketing is a relatively new phenomenon which was gradually introduced as the twentieth century progressed. Consumer advocacy groups, which emerged in the 1970s, tended to demand strict legal prohibition of unethical practices (the so-called hard regulation approach) whilst those within the business community felt that self-regulation through the use of codes of practice was just as effective (soft regulation). With the introduction of new communications media, which included the telephone, radio, television and later the Internet, the debate as to the appropriate form which regulation should take has continued unabated.

Most of the advertising content which appears on the Internet is, legally, in the nature of an invitation to treat, or mere puffery. Only if interested consumers respond by disclosing their personal details, which may include a name, address and credit card account numbers, will a formal offer to purchase be transmitted which, if accepted and supported by consideration, will give rise to a legally binding agreement (*Carlill v Carbolic Smoke Ball Co* [1892] 2 QB 484—see Davies 1997).

Those who display misleading or deceptive advertisements on the Internet will generally only be held liable if the objectionable content forms part of the terms of the agreement. This may then give rise to a right to rescind the contract or sue for damages. In this sense, the use of the Internet raises legal issues which are substantively the same as those which arise out of paper-based advertisements and contracts. There are, however, particular evidentiary and forensic difficulties associated with establishing what transpired between the parties to an electronic transaction.

In Australia, one of the first consumer protection statutes to be enacted was the *Book Purchasers Protection Act 1899* (NSW) which sought to regulate the conduct of itinerant merchants who engaged in door-to-door sales. Since then, more restrictive legislative regimes have been devised to control marketing and advertising practices. These laws now help to ensure that consumers are not coerced into buying products which they do not want and are not otherwise deceived by sellers. Statutory cooling-off periods, for example, are an example of a legislative means of empowering consumers who are subjected to high-pressure sales techniques in their homes (see Goldring, Maher, McKeough, and Pearson, G. 1998, pp. 270-306).

Both federal and state consumer protection laws apply to transactions in which Australian citizens or corporations are involved (see Goldring *et al.* 1998). The *Trade Practices Act 1974* (Cth) has provisions concerning consumer protection in Part V which proscribe various unfair practices and specify product safety standards and the operation of conditions and warranties in contracts.

The *Trade Practices Act 1974* (Cth) is, however, generally silent as to whether its provisions apply to conduct carried out electronically, although the breadth of its controls would, arguably, apply to all on-line activities carried out between corporations and consumers. Most of the consumer protection provisions of the Act specifically apply to conduct which
‘involves the use of postal, telegraphic or telephonic services’ (s. 6(3)) which would seem to exclude the Internet and E:mail which are not specifically ‘telephonic’). This question has yet to be judicially determined in Australia although the ACCC takes the view that advertising on the Internet comes within the provisions of the *Trade Practices Act 1974* (Cth) (ACCC 1997a).

Although Australia’s consumer protection laws would apply to contracts for the purchase of goods and services entered into with merchants who have advertised on the Internet, the imposition of liability may be difficult and costly where overseas corporations are involved. Most laws apply only to transactions carried out between Australian citizens and corporations within Australia. The cost, inconvenience, and logistics of cross-border legal proceedings make the imposition of liability on manufacturers, distributors, and merchants outside Australia unviable for most consumers.

**Soft Regulation**

In view of the practical difficulties associated with relying upon legislative regulatory approaches to control misleading and deceptive on-line conduct, a number of industry groups have established self-regulatory groups which have devised their own standards and codes of practice. These were originally created to deal with non-electronic forms of advertising and marketing, but are now being extended to deal with conduct in the digital world.

**Content Regulation**

One of the primary strategies which seeks to prevent misleading and deceptive material from being disseminated electronically relates to the regulation of on-line content. This can be done through the use of screening software or through measures which require Internet Service Providers to monitor the material being publicised on their networks. Recent proposals have also entailed an element of hard regulation through the criminalisation of content deemed to be unsuitable which has been publicly disseminated.

Although the use of screening software has been widely advocated to control access to obscene and objectionable materials, its use in the control of misleading and deceptive advertising may be more difficult. Often the deception would not be discernible from an image or description of the product in question, and it might be impossible to differentiate between a legitimate advertisement and one which contains some misleading content, merely on the basis of the words or images used.

Instead, various industry groups have developed guidelines for Internet Service providers to follow when regulating the content of material which appears on their networks. The Internet Industry Association, for example, recognises that the Internet should provide a means to enable control of access to content while acknowledging it is impractical to filter all Internet content. Accordingly, the Association endorses methods by which content can be recognised and possibly excluded by content filter technologies as the most practical means of empowering responsible adults to control access to the Internet to determine appropriate controls on content.

As with the regulation of sexually explicit, racist, or other illegal content, questions of freedom of speech and the practicality of regulating content are the major areas of concern in adopting content regulatory approaches.
Certification and Endorsement Services

As an alternative to the use of prohibitory schemes which seek to identify objectionable content and to prevent users from gaining access to it, a number of certification and endorsement services have been established which provide users with information as to the reliability and acceptability of on-line material. Users are then free to decide whether or not they wish to make use of the material in question.

The Platform for Internet Content Selection (PICS), for example, is a voluntary content rating system which helps users identify material which complies with specified standards. Although this has primarily been used to deal with obscene and objectionable content, it could be adapted to deal with misleading and deceptive content as well.

In the United States, the Council of Better Business Bureaus carries out a certification service in which Internet business sites are given a form of approval. Sites which display the authorised and encrypted seal of approval agree to abide by the Council’s truth-in-advertising standards and to adopt its dispute resolution procedures. Members of approved Internet Associations are able to display the fact of their membership and consumers are able to check to see if organisations do, in fact, have membership.

Certification and endorsement services have two primary benefits. First, consumers are able to rely upon the fact of a merchant being certified in order to have some measure of confidence in the trustworthiness of that merchant and in the availability of redress mechanisms if problems arise. Secondly, financial institutions involved in providing payment facilities could be encouraged to deal only with certified merchants who have agreed to comply with a code of conduct which meets certain minimum standards. This would provide a powerful industry-based inducement for merchants to undergo certification and to act responsibly and in conformity with established codes of practice.

One of the main problems with endorsement and certification, is the proliferation of services and the determination of appropriate standards. Already, some twenty so-called ‘Webseals’ are in circulation in Australia with the government providing a comparative table which sets out their various attributes (http://www.dcita.gov.au/nsapigraphics/?Mlval=dca_dspdodc&pathid=%2fshoponline%2fsealtable%2fhtml visited 4 July 2000)(see Cook 1999). Determining acceptable standards and publicising these will represent a major challenge for the future.

Information Intermediaries

In Australia, the ACCC (1997b) has also raised the idea of using information intermediaries to provide information about on-line merchants and the procedures involved in conducting business on-line, similar to the kinds of information which insurance or mortgage brokers provide. Several private enterprises, including the Australian Consumers Association, have set up an independent advice service on loans and mortgages offered on-line by financial institutions whilst various consumer subscription services publish independently conducted evaluations of products offered on-line.

Preventive Strategies
In addition to the use of both hard and soft-regulatory approaches, much can be achieved by way of self-help strategies which aim to alert users to the presence of misleading and deceptive practices in order that they can avoid victimisation. Such preventive action may take the form of regular surveillance of the Internet in order to locate objectionable and illegal practices, providing educational material warning users of dangerous schemes and the use of authentication technologies to permit individuals to know with certainty with whom they are dealing in the on-line world.

Most regulatory agencies throughout the world provide information in paper form and electronically through Websites which alert consumers to misleading and deceptive practices. One of the most comprehensive booklets directed at Australian consumers is *The Little Black Book of Scams* published by the Ministerial Council on Consumer Affairs (1999). In electronic form, the ACCC’s Website gives advice on pyramid selling schemes, business opportunity schemes, and phoney prizes and lotteries. Examples of popular deceptive practices are listed along with the legal penalties which apply to those who run or participate in such activities. In addition, and in order to enhance consumer confidence in the Internet, the Australian government has produced a series of fact sheets which provide information to consumers about the risks of shopping on-line, and certain other issues such as paying tax and duty and privacy issues (<http://www.dcita.gov.au/shoponline> visited 4 July 2000).

Consumer groups also represent a good source of trusted information for consumers. Groups, such as the Australian Consumers Association, conduct their own testing of products and services and publicise the results through subscriber based magazines such as *Choice* (Australia). Although consumer organisations already provide consumer information by various means, including the Internet, perhaps the role of consumer groups in providing information services could be increased.

Finally, in order to solve the problem of consumers and merchants adopting false identities for fraudulent purposes when carrying out on-line transactions, the use of electronic user authentication systems is starting to be employed. Public key systems which make use of encrypted data transmissions are one way of helping to ensure that both consumers and merchants are confident of the identity of the person with whom they are dealing. Such technologies would not, however, prevent individuals from illegally obtaining access to private cryptographic keys by stealing tokens which hold keys or by presenting fabricated documentation in order to obtain key pairs fraudulently (see Office of Government Information Technology 1998). They do, however, represent a much more secure way on conducting on-line transactions than simply by trusting material that is displayed on the Internet and hoping that it will be secure.

**Conclusions**

Although some may question their effectiveness, on-line advertising is already subject to a variety of laws and other regulatory controls. Those who engage in misleading and deceptive practices invariably infringe local laws in the jurisdiction in which they reside or the jurisdiction in which their material is read; or sometimes both. This often provides sufficient jurisdictional basis for the commencement of legal proceedings. The last thirty years has seen continual improvements in consumer protection legislation and dispute resolution procedures and many on-line activities fall within the scope of these initiatives.
Unfortunately, the remedies which are available to those who have been deceived electronically are often practically unavailable as they would require offenders to be extradited from other places or victims to take cross-border legal proceedings. Such action is invariably beyond the means of most individuals and costs far in excess of the amount lost in most consumer frauds.

Legal enforcement proceedings can, however, sometimes be taken on behalf of groups of consumers who have suffered loss in the form of class actions against large corporations. Although these are sometimes slow and costly, victims are empowered through the weight of numbers and compensation is occasionally able to be made.

The perpetrators of many on-line scams, however, are often not large corporations. They are able to close-down their operations quickly and easily, move assets to secure locations and use digital technologies to conceal their identities and disguise evidence. In such cases there is little likelihood of success whether civil or criminal proceedings are taken.

Consumers who transact business on-line need to be made aware of the risks they face and informed about the nature of misleading and deceptive practices which are present. Already there are substantial amounts of information of this nature available. The challenge lies in ensuring that consumers are made aware of its existence. In this regard, certification and notification systems, which permit consumers to identify readily businesses which have been found to be trustworthy, seem to provide the best option. Technology needs to be developed, however, to ensure that certification services are, themselves, unable to be manipulated. There could, for example, develop a trade in fraudulently acquired certificates of propriety which illegitimate businesses could attach to their Website. Fraud relating to the process of certification might also develop in the future as might the use of ‘phoenix businesses’ which re-establish themselves immediately they have been closed down because of improper practices.
References


