Shopping on the Net: Legal Protection for Consumers

Kate Tokeley*

I Introduction

There are now more than 30 million users of the internet in over 135 countries.[1] New Zealanders, perhaps due to our geographical isolation, have been quick to accept this new technology and the growth rate over the 1994/1995 period for New Zealand use was estimated at 450%.[2] One survey has placed New Zealand as third equal for internet use, comparing users per thousand population.[3] Consumers can now purchase goods and services on the internet and pay by credit card or cheque[4] and it is likely that electronic internet payment systems will be developed in the future.[5] Most commentators agree that commerce over the internet can only increase.[6]

This electronic highway is transforming the business world and consideration needs to be given to the legal position of the consumer shopping on the internet. In the past few years there has been an upsurge of consumer protection legislation in New Zealand. There has been a move away from the principles of *caveat emptor* and sanctity of contract and it is now generally accepted that in the modern market place the consumer is in a significantly weaker bargaining position than the supplier and manufacturer and is therefore in need of special legal protection.[7]

---

* Lecturer in Law, Victoria University of Wellington, New Zealand. This article is based on a paper presented by the author at a Ministry of Consumer Affairs' conference on the electronic consumer in Wellington, December 1996.
[Accepted for publication June 1997]

1 See the *CommerceNet/Nielsen Internet Demographics Recontact Study March/April 1996: Executive Summary*, August 13, 1996 (available on the internet @http://www.commerce.net/work/pilot/Nielsen_96/ecec.html). For an introductory discussion of what the internet is and how it works, see I F Fletcher, "The Trouble with Bits -First Steps in Internet Law" [1996] JBL 416-420. For a more detailed description of the internet and its workings see Krol, *The Whole Internet User's Guide & Catalog* (O'Reilly & Associates, Sebastopol CA, 2nd ed, 1994).

2 C Brien, "Internet : The New Trade in Goods, Services and Ideas" (1996) 7 Journal of Law and Information Science 69 at 72.

3 C Anderson, "Accidental Superhighway-Paradise by the Modern Lights", *The Economist*, 1 July 1995.

4 New Zealand already has several on-line sites where consumers can purchase various goods. For example, The Warehouse site (http://thewarehouse.co.nz) and Whitcoulls (http://www.whitcoulls.co.nz) offer online shopping for their products with credit card facilities.

5 See L Morgan, "Cashing In: The Rush to Make Net Commerce Happen" http://pubs.iworld.com/iw-online/Feb95/feat48.htm (8th April 1996).

6 See Mary J Cronin, *Doing Business on the Internet: How the Electronic Highway is Transforming 'American Companies* (Van Nostrand Reinhold, New York, 1994) at 4.

7 For a good introductory discussion on the philosophy of consumer protection law see J Goldring, L W Maher & J McKeough, *Consumer Protection and the Law* (1993) at 1-14 and also I Ramsey, *Consumer Protection: Text and Materials* (1989) ch

The two main New Zealand consumer protection statutes are the Fair Trading Act 1986, one of the main aims of which is to protect consumers from misleading conduct and misrepresentations made in trade, and the Consumer Guarantees Act 1993 which provides consumers with minimum guarantees to which suppliers and manufacturers must conform.

One of the main problems for consumers shopping on the internet is that while New Zealand consumer protection legislation provides protection to consumers purchasing goods and services in the traditional way it does not provide adequate protection to cyber-shoppers. In this article I will outline some of the difficulties facing the cyber-shopper.[8] These include the practical difficulties of enforcement and redress which arise when a cyber-shopper purchases a defective product from an overseas supplier or when misleading information is placed on the internet by an overseas supplier. Cyber-shoppers may also have difficulties evidencing their contracts with computer records. In addition, because the issue of whether the postal acceptance rule applies to internet transactions has not yet been decided by the courts, often a consumer cannot ascertain for certain the time or place of contract formation, a matter which may be a critical one in some disputes.

In this article I argue that some of these problems can and should be resolved by adapting existing laws in the specific areas of evidence and contract formation. This would certainly improve the situation for consumers purchasing products over the internet from New Zealand suppliers and would be of some assistance to cyber-shoppers purchasing products from overseas suppliers. These changes alone, however, will not provide adequate protection to the cyber-shoppers purchasing products from overseas suppliers. These consumers are faced with many difficulties and new methods of protecting these consumers need to be implemented. For example, more on-line protection agencies should be introduced and serious consideration needs to be given to developing a cyber-jurisdiction which would regulate the internet independent of national laws.[9]

In Part II of this article I analyse the problems cyber-shoppers face in disputes over the quality or non-delivery of goods or services. In Part III, I examine the problem of regulating misleading statements made on the internet. Finally, in

---

2. There are also numerous articles written on the topic. See, for example, A A Tarr "Consumer Protection Legislation and the Market Place" (1983) 5 Otago LR 397. For a more critical view of consumer protection laws see R Parish, "Consumer Protection and the Ideology of Consumer Protectionists" in A J Duggan & L W Darvall(eds), *Consumer Protection Law Theory* (1980).

8 This article does not consider the issues of privacy or bank card security for consumers shopping on the internet. For a discussion of some of the problems of privacy in cyberspace, see T Miller, "Law, Privacy and Cyberspace" (1996) 1 Tolley's Communication Law 143. R Gainer discusses the security risks of using bank cards over the internet in "Allocating the Risk of Loss for Bank Card Fraud on the Internet" (1996) 15 John Marshall Journal of Computer Information Law 39. The article is about the United States situation but many of the issues are equally relevant to New Zealand.

9 In-depth consideration of the issues involved in establishing a cyber-jurisdiction is beyond the scope of this particular article. Some of the issues are, however, outlined in Part IV 3 of this article.

Part IV, I analyse some of the possible options for reform which would increase consumer protection on the internet.

II The Quality and Delivery of Goods and Services

If a consumer purchases a good or service in a shop in New Zealand and it is agreed that the good or service will be delivered at a later date, then if there is no delivery the consumer is protected by the terms of the sale contract. If a consumer purchases defective goods or services in a shop in New Zealand then they will be protected not only by the terms of the sale contract but also by the guarantees implied into the contract by the Consumer Guarantees Act 1993. This Act sets minimum standards for suppliers and manufacturers. For example, goods and services must be safe and be of acceptable quality.[10] If the consumer has a problem with non- delivered or defective goods or services, the consumer can complain to the shop or if this is unsuccessful he or she can take their complaint to the Disputes Tribunal for very little cost.[11]

Unfortunately, consumers shopping on the internet may not find the resolution of disputes over the delivery or quality of the goods and services[12] as easy to resolve as the traditional shopper for a number of reasons.

1 Evidentiary Problems

When a consumer buys a good or service in the traditional way they will often have evidence of the contract either by a paper docket or a written contract. The electronic messages of offer and acceptance which are the basis of a contract formed in cyberspace are not made on paper. The parties can of course print out these messages on to paper but the question then arises as to whether these computer printouts can effectively evidence the original electronic transaction. Some commentators have suggested that producing the computer print-outs to evidence a contract made by electronic communication may breach the "best evidence" rule as it relates to documents.[13] This rule requires that the original of a document must be produced in order to adduce proof of its contents.[14]

---

10 See ss 6-7 of the Consumer Guarantees Act 1993.

11 The New Zealand Disputes Tribunal has jurisdiction for disputes in contract, quasi contract and tort (relating to property damage or loss) and for disputes under various Acts including the Consumer Guarantees Act 1993. The amount in dispute must be less than $3000, although disputes over amounts up to $5000 can be heard by consent of the parties. The cost for taking a claim to the tribunal is $10 if the amount in dispute is up to $1000 and $20 if the amount in dispute is over $1000.

12 It is possible to purchase services as well as goods over the internet. For example, services such as education or advice may be purchased over the internet and delivered online.

13 See, for example, P Myburgh, " Bits, Bytes and Bills of Lading: EDI and New Zealand Maritime Law" [1993] NZLJ 324 at 327. Fletcher, supra n 1 at 421, also suggests that paper printouts may possibly not provide effective evidence of an electronic transaction although he does not specifically refer to the "best evidence" rule.

14 *R* v *Minnhinnck* (No 2) (1984) 12 CRNZ 196; *Westpac Banking Corporation* v *Evans* (1986) 1 NZBLC 102,563 at 102564. For the purposes of the rule, a "document" is

In the United States, computer printouts which accurately reflect the data originally stored in the computer are actually considered originals for the purposes of the best evidence rule so they pose no problem.[15] This is probably the most sensible approach in an age where more and more dealings occur by electronic communication. Even if New Zealand courts do not adopt this approach and refuse to regard the printout as an original, it is unlikely that computer printouts of an original electronic transaction would be objected to, because they probably fit into one of the many exceptions to the rule.

One of the exceptions to the rule is that secondary evidence is admissible if production of the original is impossible or impractical.[16] The immediate electronic messages are impossible to produce in court because those original electronic messages will be lost the moment the computer is turned off. The hard drive will store only a reproduction of the original and in any case it is impractical to bring the hard drive into court.

The computer printouts may be admissible evidence but there is a further issue of whether they are reliable. Some commentators argue that computer printouts carry a false sense of trustworthiness and reliability.[17] It is, however, likely that the printout from a computer will be reliable evidence of the information it has stored. In *Marac Financial Services Ltd* v *Stewart*, the New Zealand High Court considered computers to be generally trustworthy.[18] It held that in the absence of evidence to the contrary, the use of computers for recording transactions on accounts, such as the cash management bank account in this case, was sufficiently well established for there to be a presumption of fact that such computers are accurate.[19]

A further potential problem for the cyber-shopper is the lack of a written signature on the computer printout of the offer. This may make it hard to link the document to the particular supplier. In some instances the distinctive characteristics of the design and content of the document may be enough to link it to the particular supplier. In addition, if the consumer is complaining about the quality of the product rather than non-delivery, then the delivery of a product of the type supplied by that supplier could also be used as circumstantial evidence to show that the electronic offer was sent by the supplier.

In the future this problem may diminish further with the development of digital signatures. These signatures are based on encryption techniques to verify the

---

likely interpreted as in s 2 of the Evidence Amendment Act (No 2) 1980 as including "any information recorded or stored by means of any..... computer."

15 See *King* v *State ex rel Murdock Acceptance Corp*, 222 So 2d 393, 398 (Miss 1969), read in conjunction with Fed R Evid 1001(3).

16 See *Mortimer* v *M'Callum* (1840) 6 M & W 58 where it was noted that inscriptions on tombstones and walls are invariably proved by copies.

17 See, for example, R J Peritz, "Computer Data and Reliability: a Call for Authentication of Business Records Under the Federal Rules of Evidence" (1986) 80 NWUL Rev 956. For the contrary view, see M Johnson, "Computer Printouts as Evidence: Stricter Foundation or Presumption of Reliability?" (1992) 75 Marquette L Rev 439.

18 [1993] 1 NZLR 86.

19 Ibid at 17.

author and content of electronic messages.[20] A digital signature cannot be forged in the same way as a hand-written signature because people cannot decode it unless they are told the secret combination of digits by the author.[21] In Utah, legislation was enacted in 1995 which gives legal authorisation for the use of digital signatures.[22] If digital signatures are used in consumer contracts in the future, there is no reason why they should not be treated by the New Zealand courts as legal signatures of authentication.

In June 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted a Model Law on Electronic Commerce.[23] It is suggested as a common way in which national laws can be drafted to resolve some of the issues of electronic transactions. If New Zealand were to enact such legislation, many of the difficulties discussed above could be resolved. Article 8 of the Model Law prohibits the use of "the best evidence rule" to alter the legal recognition and evidential worth of electronic messages. Article 5 provides that information shall not be denied effectiveness, validity or enforceability solely on the grounds that it is communicated by electronic means and Article 7 provides that a digital signature will be recognised as a legal signature.

The difficulties of electronic evidence are relevant to both internet contracts involving New Zealand suppliers and to internet contracts involving overseas suppliers. Enacting legislation to resolve these difficulties is an immediate step that New Zealand can and should take in order to improve the legal protection available for cyber-shoppers.

2 *Contract Formation*

A further issue that arises for the cyber-shopper is one of contract formation. The formation of a contract requires, of course, an effective offer and acceptance. Whether it is the supplier or the consumer making the offer will depend on individual circumstances. It might be thought that the supplier's advertisement on the internet is always merely an invitation to treat as is the case with most displays of goods in shops.[24] This might be the case if the advertisement simply states the price and a description of the goods or services. If the supplier is merely making an invitation to treat then the consumer's electronic message asking for the goods or services is an offer to buy and the supplier may then either accept that offer by delivering the goods or services, or by sending back an electronic message of acceptance acknowledging payment and agreeing to send the goods

---

20 For further discussion of digital signatures, see C Reed, "Authenticating Electronic Mail Messages – Some Evidentiary Problems" (1991) 4 Software L J 161.

21 However if a person does learn the digital signature of another they can use it over and over again. Users of digital signatures should therefore periodically change their digital signature.

22 Utah Digital Signatures Act 1995; Utah Code Ann 43-3-101 et seq.

23 For discussion of the proposals set out in the Model Law, see R Hill & I Walden, "The Draft UNCITRAL Model Law for Electronic Commerce: Issues and Solutions" (1996) 13 Computer Law 18 , also available on the internet at http://www.batnet.com/oikoumene/arbunc.html

24 *Pharmaceutical Society of Great Britain* v *Boots Cash Chemist (Southern) Ltd* [1952] 2 QB 795; [1952] 2 All ER 456, affirmed [1953] 1 QB 401; [1953] 1 All ER 482.

or provide the services. In some situations, however, the supplier's advertisement on the internet will manifest an intention to be bound upon the consumer's acceptance. For example, if the advertisement states "Limited Stock, First in First Served", the supplier has waived the right of refusal if there are stock left. In this case the advertisement would be considered an offer to sell and the consumer's electronic message in reply would be the acceptance. Whether the acceptance is from the supplier or the consumer, that acceptance will often be sent electronically. The issue is whether the contract is formed the moment that the electronic message of acceptance is sent from the offeree's computer or whether it is not formed until the message reaches the offeror's computer.

The question of when the contract is formed is relevant to the consumer in several ways. The electronic message of acceptance may get lost in cyberspace and not in fact reach the offeror. In situations where the supplier is the offeror, the supplier will be unaware of the consumer's acceptance, they would then not deliver the goods or services to the consumer and may subsequently withdraw their offer. If the consumer does later succeed in contacting the supplier and demands delivery of the goods or services, the supplier might refuse to deliver them because of the unavailability of stock or because the price has changed. Was a contract formed at the moment the consumer sent the initial acceptance from her computer? Or was the initial acceptance ineffective because it did not reach the supplier, in which case the offer was revoked before the consumer contacted the supplier and so there was no contract formed? The alternative situation is where the supplier is the offeree and their electronic message of acceptance does not reach the consumer and they subsequently fail to deliver the goods or services to the consumer. The issue of when a contract is formed is equally relevant to the consumer in this situation because it will determine whether or not a contract exists and therefore whether the supplier is bound to deliver the goods or services.

The issue of contract formation is also relevant when disputes arise in relation to international contracts as will often be the case for the cyber-shopper. Knowing when the contract was formed, will answer the question of where the contract was formed and this may be relevant to questions of jurisdiction, *forum conveniens* and proper law.[25]

In a shop there is generally no problem deciding when the contract was formed. The general rule of contract formation which requires acceptance to be communicated to the offeror[26] applies and therefore the contract is usually formed at the till when the supplier communicates acceptance of the consumer's offer to buy.[27] Internet shopping, unlike traditional shopping, does not involve communication of acceptance face-to-face but often involves acceptance sent electronically over the internet. The issue which has been raised by several legal commentators is whether to apply the general rule that acceptance must be communicated or whether to apply the postal acceptance rule.[28] The postal

---

25 See Part III 3 of this article for discussion of these international contract issues.

26 See *Powell* v *Lee* (1908) 99 LT 284 and *Robophone Facilities Ltd* v *Blank* [1966] 3 All ER 128; [1966] 1 WLR 1428.

27 Supra n 23.

28 See for example, Myburgh, supra n 13 at 326-327; Fletcher, supra n 1 at 421-422;

acceptance rule is an exception to the general rule, it provides that where an offer is made and accepted by letters sent by post then the contract is formed at the moment that the acceptance letter is posted, even if it never reaches its destination.[29] The rule will not apply if, having regard to all the circumstances, the parties cannot have intended that a binding agreement be formed without actual communication.[30] If electronic acceptance is treated as falling under the postal acceptance rule, a contract would be formed the moment the offeree presses "send" on her computer.

The issue of when electronic acceptance is effective has not been considered by the New Zealand courts although two English cases, *Entores Ltd* v *Miles Far East Corporation*[31] and *Brinkibon* v *Stahag Stahl und Stahlwarenhandelsgesellschaft mbH*,[32] discuss these issues in relation to telex communications. These cases are relevant to resolving the issue of electronic acceptance and are examined below, but before considering them it is important to consider the policy reasons behind the postal acceptance rule. Ironically, the English case *Adams* v *Lindsell*,[33] which first established the postal acceptance rule, came before the cases which determined that acceptance must be communicated. Subsequent cases have tried to find reasons which justify acceptance by post being excluded from the communication requirement. The usual reasons given for the exclusion are that: first, without the rule, the delay in communication would result in business inconvenience, and, secondly, that the post office acts as an agent for the offeror and, therefore, as soon as the letter is in the post it is treated as already with the offeror.[34]

If we assume for a moment that these justifications are satisfactory, then it is necessary to consider the question of whether, having regard to these two justifications, sending acceptance over the internet is analogous to sending letters through the post. In relation to the agency justification the analogy between the post and internet communication may depend on the form of internet communication used. If the communication is made directly across the internet via bulletin boards then there is no third person resembling the post office. If communications are made through a service provider via e-mail then the communication starts to resemble postal communication where messages are entrusted to a third party. It has been argued that in this situation the postal rule should apply.[35]

In relation to the business convenience justification the speed of the communication is the relevant factor. Communication over the internet is

---

and I Walden, "Contractual Harmonisation in the European Union: a New Approach Towards Information Technology Law?" (1995) 11 (1) Tolley's Computer Law & Practice 2 at 3.

29 *Adams* v *Lindsell* (1818) 1 B & Ald 681.

30 See *Holwell Securities Ltd* v *Hughes* [1974] 1 All ER 161 at 167; [1974] 1 WLR 155 at 161; *Nunin Holdings Pty Ltd* v *Tullamarine Estates Pty Ltd* [1994] 1 VR 74.

31 [1955] 2 QB 327; [1955] 2 All ER 493.

32 [1983] 2 AC 34; [1982] 1 All ER 293.

33 Supra n 29.

34 See for example, *Household Fire and Carriage Accident Insurance Co Ltd* v *Grant* (1879) 4 Ex D 216 at 223.

35 Supra n 1 at 422.

certainly quicker than using the post. The parties are often, however, not in direct instantaneous contact with each other, as they are when speaking face-to-face or over the telephone. The offeror may not be at their computer when the message of acceptance arrives or may fail to read the message for some time. Since the postal acceptance rule is based on considerations of expediency then this fact may suggest that the postal acceptance rule should be applied to electronic acceptance.

The English decisions of *Entores*[36] and *Brinkibon*[37], on the other hand, tend to suggest that the postal acceptance rule should not apply to computer communications. These cases consider the above issues in relation to communication by telex. In *Entores* it was held that due to the virtually instantaneous nature of telex communications, the general rule that the contract is formed only when acceptance is communicated should apply. This result was confirmed by the House of Lords in *Brinkibon*.

In *Brinkibon*, Lord Brandon of Oakbrook concluded that telex communications are instantaneous and therefore the postal acceptance rule should not apply and the contract is formed when the acceptance is *received* by the offeror (whether this means received by the offeror's machine or actually read by the offeror is unclear).[38] Lord Wilberforce, however, acknowledged that telex communications are not always instantaneous like face-to-face or telephone conversations and they may be received by a clerk and handed to his or her principal much later. He argued, nevertheless, that the postal acceptance rule should not apply and that actual communication should be assumed to occur when the message is received by the offeror's machine because it is the offeror's responsibility to arrange for prompt handling of messages.[39] So in fact Lord Wilberforce applies a variation of the general rule. The contract is formed, not necessarily on actual communication but when the message is received by the offeror's machine. The decision was, however, confined to its particular facts which included the fact that the messages were sent during ordinary office hours. In this situation it is more likely that the offeror would read their messages promptly and thus the communication would be virtually instantaneous. In addition, the House of Lords concluded that:[40]

> No universal rule can cover all such cases: they must be resolved by reference to the intentions of the parties, by sound business practice and in some cases by a judgment where the risks should lie.

When the intentions of the parties is taken as a relevant consideration for the application of the postal acceptance rule, it becomes more logical to exclude telex communications from the rule. Where acceptance is sent by telex it seems likely that neither party would have intended a binding contract to be formed until the message of acceptance reaches the offeror's machine. It seems equally

---

36 Supra n 31.
37 Supra n 32.
38 Ibid at 301.
39 Ibid at 297.
40 Ibid at 302.

likely that parties forming a contract over the internet would also intend a contract to be formed only when the communication of acceptance arrives at the offeror's computer.

Computer communications are in many ways analogous to telex communications and therefore it makes sense to treat them in the same way. Since *Entores* and *Brinkibon* did not apply the postal acceptance rule to telex communications, computer communications should also be excluded from the rule.

Perhaps the strongest argument for not applying the postal acceptance rule to computer communications is that the usual justifications given for the rule are not generally very persuasive and it would therefore be unwise to expand the situations where the rule applies.[41] This may in fact be the real but unexpressed reason why *Entores* and *Brinkibon* did not apply the postal acceptance rule. The business convenience justification can be criticised for being one-sided and only considering the convenience of the offeree. It has been argued that the rule is not inconvenient for the offeror because if the offeror is unsure whether a letter of acceptance has been sent he or she can contact the offeree and ask.[42] The problem with this reasoning in relation to some contracts is that the offeror may be making an offer to the world at large so the offeror is not expecting to hear from particular people. This will invariably be true when an offer is made over the internet. Turning to the agency justification, it can be criticised for being based on a fiction. In fact, although the decisions in *Entores* and *Brinkibon* recite this justification for the rule, the Court of Appeal in *Henthorn* v *Fraser* in 1892, recognized that the agency idea does not work.[43] The offeror does not pay the post office to carry the offeree's letter and there is no agreement between the post office and the offeror that the post office is to receive the letter on behalf of the offeror. If the post office is the agent of anyone it is more likely to be the offeree since it is the offeree who pays the post office to carry their letter. If the postal acceptance rule is not based on sound justifications it should not be extended to cover new forms of communication.

One final point to note is that the postal acceptance rule does not apply to international sale of goods contracts made between traders whose places of business are in different states. These contracts are regulated by the Sale of Goods (United Nations Convention) Act 1994[44] which gives effect to the provisions of the United Nations Convention on Contracts for the International Sale of Goods. Article 18 of the Convention provides that, unless the parties have agreed that the offeree may indicate assent by performing an act, then acceptance of an offer becomes effective the moment the indication of assent reaches the offeror. There appears no reason why consumer contracts should be treated any differently.

An increasing number of consumer contracts are being made over the internet. These contracts may involve either New Zealand suppliers or overseas suppliers.

---

41 For a full discussion of the shortcomings of the theories behind the postal acceptance rule, see S Gardner, "Trashing with Trollope: A Deconstruction of the Postal Acceptance Rule in Contract" (1992) 12 OJLS 171.

42 Supra n 34 at 223-224.

43 [1892] 2 Ch 27, 35.

44 The Act came into force on 1 October 1995.

At present, unless the parties specifically refer to the matter in their contracts, the parties will not be certain when and where these contracts are formed and it may be some time before the issue is decided by the courts. While New Zealand courts are likely to follow *Entores* and *Brinkibon*, the uncertainty makes it be preferable to resolve the issue by legislation. This legislation should provide that the postal acceptance rule will not apply to computer communications and that the contract will be formed the moment the message of acceptance reaches the offeror's computer.

3 *Globalisation Issues*

In the dimensionless world of cyberspace there are no geographical borders and consequently trade can become increasingly globalised. Consumers can buy goods and services on the internet from anywhere in the world that is linked to the internet. If something goes wrong with a good or service purchased from an overseas supplier the consumer is in a particularly vulnerable position. Current laws do not adequately protect these consumers because they do not offer a way of obtaining redress which is feasible for most consumers. If a dispute arises in relation to a contract made between a New Zealand consumer and an overseas supplier several issues arise.

(a) In which country will the dispute be heard?

If a New Zealand consumer buys from an overseas supplier and some dispute arises, the first issue concerns which country the dispute would be heard in. The New Zealand consumer will probably prefer to have the dispute dealt with in New Zealand because this will be more convenient and cheaper for them.[45] For the New Zealand High Court or a District Court to hear the dispute it must first be determined whether the court has jurisdiction over it.[46]

Rule 219 of the High Court Rules lists situations where jurisdiction can be invoked without leave of the court.[47] Some of these may be applicable to a consumer who is claiming for faulty or undelivered goods or services bought over the internet.[48] Rule 219(b)(i) applies to contracts which are "made or entered

---

45 In some cases a consumer may prefer to have the dispute heard in the supplier's country. For example, if other consumers in the supplier's country are making similar claims against the supplier, it may be possible for the New Zealand consumer to join these consumers in their country and be part of a class action against the supplier.

46 It is unlikely that the New Zealand Disputes Tribunal is able to hear such claims. The Disputes Tribunal Act 1988 and the Disputes Tribunal Rules 1989 do not make express provision for service of claims outside of New Zealand. The common law rule is that proceedings cannot be served out of the jurisdiction without express provision to do so (*Eyre Nationwide News Pty Ltd* [1967] NZLR 851). This rule and the policy underlying the Disputes Tribunal of speedy, inexpensive resolution of disputes suggests that a Disputes Tribunal cannot hear a claim against a person outside of New Zealand.

47 The equivalent District Court Rule is R242.

48 Rule 219(a) allows jurisdiction to be invoked where "any act or omission for or in respect of which damages are claimed was done or occurred in New Zealand". If

into in New Zealand". Whether a contract made over the internet has been "made or entered into in New Zealand" will depend on the application of the postal acceptance rule to internet communications. It has been argued in part II 2 of this article that the postal acceptance rule should not be applied to internet communication.[49] If this is the case, then in situations where the supplier is the offeree and they send their acceptance electronically over the computer, the contract would be "made or entered into on in New Zealand" when the consumer receives that acceptance on her computer. It is possible, although less likely, that the reasoning of *Entores* and *Brinkibon* will not be extended to internet communications and the postal acceptance rule will be held to apply to such communications. If this occurs, then in situations where the consumer is the offeree, the contract will be "made and entered into in New Zealand" when the consumer sends their electronic acceptance and Rule 219(b)(i) would apply. Rule 219(b)(iv) is another possibility for some contracts made over the internet. It applies where the contract, by its terms or by implication is to be governed by New Zealand law.

If it is not possible to come within one of the categories under Rule 219, leave of the court is required to serve a defendant out of New Zealand.[50] To be granted leave the consumer would have to satisfy the courts that New Zealand is the *forum conveniens*; that is the jurisdiction in which the dispute can be most appropriately heard. Even where jurisdiction can be invoked under Rule 219, the overseas defendant can seek to set this aside on the grounds that New Zealand is *forum non conveniens*; not the appropriate jurisdiction in which the matter can be most appropriately heard, in the interests of the parties and for the ends of justice.[51]

The appropriate forum is the country with which the action has the most real and substantial connection. Relevant factors include convenience, expense, availability of witnesses, the law governing the transaction and the places where the parties reside and carry on business.[52]

---

the claim is in tort this may apply as there are cases decided under the former R48 which hold that if the damage occurs in New Zealand this is sufficient even though the tortious act occurred overseas. If, however, the claim is made in contract, para (a) is less likely to apply. In *Longbeach Holdings Ltd* v *Bhanabhai & Co Ltd* [1994] 2 NZLR 28 the Court of Appeal suggested that R219 should be limited to claims in tort because paras (b) and (c) provided comprehensively for contract claims. The court considered that even if para (a) did apply to contract claims, it could only apply to acts and omissions which constituted the breach and not the consequential damage caused by the breach. This is because damage is not a necessary part of a cause of action in a contract. In a contractual claim, the act of manufacturing the good is the act constituting the breach. In our example this act will have occurred overseas. For similar reasons the court in *Longbeach* also rejected the claim to jurisdiction under R219(b)(iii) which applies to contracts wholly or partly performed in New Zealand.

49 See Part II 2 of this article for discussion of the postal acceptance rule and its applicability to computer communications.

50 Rule 220 of the High Court rules. The equivalent District Court Rule is R243.

51 See *Spilada Maritime Corporation* v *Cansulex Ltd* [1987] AC 460; [1986] 3 All ER 843 applied in *Crane Accessories Ltd* v *Lim Swee Hee* [1989] 1 NZLR 221.

52 Idem and *Longbeach*, supra n 48.

In *Longbeach Holdings Ltd* v *Bhanabhai & Co Ltd*,[53] defective goods manufactured in Fiji were sent to a New Zealand company. The Court of Appeal held that even though the breaches, if there had been any, had occurred in Fiji, their consequences were felt entirely in New Zealand. The natural forum for the case was therefore New Zealand.[54] Using this reasoning it is likely that when a dispute involves a New Zealand consumer who has purchased defective goods or services over the internet from an overseas supplier of those goods or services, the natural forum for the case would be New Zealand. This is because the consequences of the supplier breaching that particular sale contract would be felt entirely in New Zealand.

(b) Which country's laws will apply?

Even if the case can be heard in the country that the consumer lives in, this does not necessarily mean it is that country's laws that will be applied although that is often the case.[55] Under New Zealand law, if the parties to the contract have expressly chosen a particular country's law to govern their contract, that law will be given effect as long as it is bona fide and legal and there is no public policy reason for disregarding the choice.[56] Some internet contracts between a New Zealand consumer and an overseas supplier will expressly state the law they wish to govern their contract.

If no express choice has been made by the parties, the court must determine the "proper" law of the contract.[57] To establish the proper law of the contract the court will infer the intention of the parties in the circumstances or consider what system of law has the closest and most real connection with the transaction.[58] It may be that particular clauses of the contract assist the court in determining the inferred intention of the parties. If the wording of the contract is of no assistance, the court will look at the surrounding circumstances. A variety of matters may be relevant including: the place of performance, the places of residence and business of the parties, the subject matter of the contract and the place where

53 *Longbeach*, above n 48.

54 *Longbeach*, ibid at 36. Part of the reason for this decision was the fact that the New Zealand company would need evidence from witnesses in New Zealand who may not have been willing to travel to Fiji to give evidence and the New Zealand company could not procure or compel them to do so. The Fijian company, on the other hand, would be using its own quality control staff as witnesses and it would be easier for them to bring these people to New Zealand.

55 *Club Mediterranee NZ* v *Wendell* [1989] 1 NZLR 216 at 220.

56 *Vita Food Products Inc* v *Unus Shipping Co Ltd* [1939] AC 277. Note that in some jurisdictions the courts almost always apply their own law even if the parties have chosen otherwise. See, for example, *Freehold Land Investments Ltd* v *Queensland Estates Pty Ltd* (1970) 123 CLR 418 (Qld).

57 *McDonnell Dowell Constructors Ltd* v *Lloyd's Syndicate 396* [1988] 2 NZLR 257 at 272-273.

58 Idem. Difficulties arise when applying these tests in cases where the defendant contends that there is no contractual obligation. It is generally accepted that issues relating to whether a contact exists are decided by the "proper" law of the contract if the contract were held to exist. For a detailed discussion of the shortcomings of this approach, see A Briggs, "The Formation of International Contracts" [1990] LMCLQ 192.

the contract was made.[59] It is potentially quite difficult to determine the proper law of an internet contract between a New Zealand consumer and an overseas supplier. The contract is largely performed overseas although the most likely dispute would concern loss in New Zealand caused by the delivery of defective goods or services. The question of where the contract is made may also be relevant but yet again this requires a decision to be made about the applicability of the postal acceptance rule to internet communications.[60]

In some cases it will not matter to the consumer which laws are applied. However, in other cases the country that the supplier is from may have either more or less effective consumer protection law than the consumer's own country. One consideration for New Zealand consumers is the Accident Rehabilitation and Compensation Insurance Act 1992. In the United States there is no similar legislation barring claims for damages for personal injury. If the consumer has been injured by the defective good or service, it is to the consumer's advantage to have United States law applied.

(c) What if the defendant does not appear in court or file a Statement of Defence?

It is more than likely that the overseas defendant will not appear in court or file a statement of defence if the case is to be heard in New Zealand. The consumer plaintiff may then apply for a judgment by default.[61] However, this judgment may not be of much use to the consumer. The most favourable situation for the consumer is if the supplier has assets in New Zealand of sufficient value to meet the judgment. If this is the case, the judgment can be enforced in New Zealand. If, however, the supplier does not have assets or does not have sufficient assets in New Zealand, then the only possibility for the consumer is to attempt to enforce the judgment in the supplier's own country. Whether the judgment is enforceable in another jurisdiction will depend on the rules of that jurisdiction. The fact that the judgment was obtained by default and the defendant was not subject to New Zealand proceedings is likely to cause difficulties.[62]

(d) What is the practical reality of obtaining redress?

The discussion above makes it fairly obvious that if the overseas supplier is not willing to rectify the problem it is extremely difficult, time consuming and expensive for a consumer to obtain redress. If a consumer buys a pair of running shoes from a shop and a week later the sole is coming off their shoes, they have several realistic options for resolving their complaint. They can go back to the supplier and try to resolve the problem face-to-face. If this is unsuccessful then it is relatively inexpensive to take the dispute to the Disputes Tribunal.

---

59 See *Re United Railways of Havana etc Warehouses Ltd* [1960] Ch 52 (CA) and *X AG* v *A Bank* [1983] 2 All ER 464.

60 Note that where the contract is made between parties from countries which have different rules regarding postal acceptance and contract formation, it is the forum country which will decide the issue with its own domestic law. See, for example, *Benaim & Co* v *De Bono* [1924] AC 514 (PC).

61 New Zealand High Court Rules 460 to 462 and Rule 226.

62 D Goddard, *Conflict of Laws - The International Element in Commerce and Litigation* (New Zealand Law Society Seminar, November 1991) at 19.

Most consumers who buy a similarly shoddy pair of running shoes on the internet from an overseas supplier are unlikely to have the time, money or inclination to do more than write a complaining email. If they have no success with this then it is unlikely that they will take the trouble to instigate legal proceedings. Even if they do it is unlikely that the overseas supplier will come to New Zealand to defend a court action and it is highly unlikely that a New Zealand consumer will be able to afford the time or the money to take a default judgment to the courts in the supplier's country. The only possible hope the consumer has in resolving the issue by legal action is if the overseas supplier has assets in the consumer's country.

Under the present law, it is easy for a company doing business over the internet with consumers in other countries to avoid liability for defective products. Cyber-shoppers are in a very vulnerable position. The consumer protection laws which protect them so well when they are shopping in the traditional way do not provide adequate protection when they are shopping globally over the internet. It is, therefore, imperative to consider new methods of legal or non-legal protection for these consumers.

III Misleading Information

The Fair Trading Act 1986 prohibits conduct in trade, which is, or is likely to be misleading or deceptive; it also prohibits making various false and misleading representations in trade.[63] If a supplier living in New Zealand places misleading information on the internet and it is read by New Zealanders, the Commerce Commission or any individual in New Zealand can lay a complaint under the Fair Trading Act. The only possible difficulty will be the evidentiary problems of computer messages discussed above in Part II *1*.

The internet opens up opportunities for suppliers to advertise their products around the globe. Therefore a lot of the misleading information reaching New Zealand cyber-shoppers will have originated outside of New Zealand. If misleading information is placed on the internet by an overseas supplier, the issue arises as to whether the New Zealand courts have jurisdiction over this conduct. If these misrepresentations are defined as conduct within New Zealand then the provisions of the Act apply to this conduct in the same way as they apply to any other misrepresentations made within New Zealand.

It has been held in Australia in *Paper Products Ltd* v *Tomlinson (Rochdale) Ltd (No 2)*[64] that misrepresentations made by telephone or facsimile by a person outside of Australia received by a person within Australia are conduct within Australia for the purposes of the Australian Trade Practices Act 1974. It has been argued that although there is no New Zealand authority on the point, it is probable that New Zealand courts would take a similar view if necessary.[65] If an overseas supplier sends information over the internet to a particular New

63 Fair Trading Act 1986, ss 9, 10, 11 and 13. The provisions in the Act allow for both criminal and civil liability. Section 9, however, which prohibits misleading and deceptive conduct generally, only creates civil liability.

64 (1993), 116 ALR 163; 44 FCR 485, upheld (1994) 122 ALR 279.

65 See J N Finn in Andrew Borrowdale (ed), *Butterworths Commercial Law in New Zealand* (3rd ed 1996) at 187.

Zealander or group of New Zealanders then this would be analogous to information sent to New Zealand by facsimile or telephone. In this situation the reasoning in *Paper Products* would suggest that any misrepresentations made in that information should be considered conduct within New Zealand and the Fair Trading Act 1986 should apply. If, however, the overseas supplier merely places the information on the internet and New Zealanders happen to access it, then this is not analogous to sending information to a particular person in New Zealand via fax or telephone. In this case any misrepresentations made in the information are less likely to be considered conduct within New Zealand.

If misrepresentations made on the internet by overseas suppliers are treated as conduct outside New Zealand, then consideration must be given to section 3 of the Fair Trading Act 1986 which states:

> This Act extends to the engaging in conduct outside New Zealand by any person resident or carrying on business in New Zealand to the extent that such conduct relates to the supply of goods or services, or the granting of interests in land, within New Zealand.

An overseas supplier who is selling goods or services on the internet to New Zealanders could arguably be said to be "carrying on business in New Zealand." This is particularly so if the supply is on a regular basis rather than intermittently. Although the supplier is not physically present in New Zealand, if they advertise in New Zealand through the internet and deliver goods or services to New Zealand, then in ordinary usage it could be said that this supplier does "carry on business in New Zealand". The placing of misleading information on the internet relating to the goods or services that they supply can be classified as "conduct relating to the supply of goods or services within New Zealand".

The problem for cyber-shoppers is that even if, as section 3 suggests, New Zealand courts have the jurisdiction to apply the Act in this situation, there remain the practical difficulties for consumers in bringing such an action, and then enforcing it.[66] In New Zealand, the Commerce Commission as well as consumers can bring actions against traders who they consider are breaching the Fair Trading Act 1986. The courts can impose criminal as well as civil liability and can fine individuals up to $30,000 and bodies corporate up to $100,000. Unfortunately, because of the immense practical difficulties in investigation and enforcement, it is unrealistic to expect the Commerce Commission to bring actions under the Act against overseas suppliers who place misleading information on the internet. The current law does not protect global cyber-shoppers from misrepresentations made in trade and therefore new ways of protecting these consumers need to be considered.

---

66 See Part II 3 (d) of this article for discussion of the enforcement and redress difficulties that consumers face when they attempt to take legal action against an overseas supplier.

IV Some Options for Reform

1 Liability of Internet Service Providers

One possible option for legally protecting cyber-shoppers from receiving misrepresentations made in trade is to put a legal duty on the Internet Service Providers (ISPs) to filter out this kind of information. This duty could either be developed into the common law of tort or it could be drafted into legislation.

In any situation in which misleading information is placed on the internet there are two ISP's on which a duty could be imposed. For example, if a United States company put a misleading advertisement on the internet, and it was received by a New Zealand internet user, there could be a duty placed on the New Zealand ISP or the United States ISP. It could be argued that the United States ISP should have a duty to check the web pages and postings on computer boards made by its internet users for not only misleading information, but also pornography, defamation and discriminatory statements. It could also be argued that the New Zealand ISP should have a duty to filter the material coming into New Zealand.

The problem with placing a duty on ISP's is that it is similar to putting a duty on Telecom to stop particular information from being given over the telephone. Telecom does not have any control over the conversations on telephones. They merely provide the lines. When an ISP receives information originating from elsewhere there may be no practical way of filtering all of this information. It is probably impossible to monitor the complicated web-like system through which information passes through the network's gateway. An ISP is, however, capable to some extent of monitoring the material posted on its own system. The issue is whether it is fair to impose a duty on ISP's to carry out this filtering process.

While there are no New Zealand court cases on this point, ISP's in New Zealand have been targeted by the Internal Affairs Inspectors in an attempt to control pornographic material published on the internet.[67] ISP's are said to be concerned about the possibility of being made liable for their customers' use of the internet when they have no real knowledge or control of this behaviour.[68]

There are two United States cases on the issue of ISP liability in relation to defamation published on the internet: *Cubby* v *Compuserve*[69] and *Stratton Oakman Inc* v *Prodigy Services Co.*[70] In *Cubby*, the ISP had delegated the editorial control

---

67 Internal Affairs have been using search warrants obtained under the Films Videos and Publications Classification Act 1993 and visiting ISP's to ask them for names of people using the internet at particular times. They have also reportedly advised ISPs to drop certain newsgroups, including those with the words "alt.sex" in their titles. See "Net Nasties", *North and South*, February 1997, at 65. In a further attempt to control pornography on the internet, former MP Trevor Rogers introduced a private member's bill to Parliament in June 1994 called, "The Technology and Crimes Reform Bill". It would require parents with a household internet connection to install a special computer programme to prevent their children from accessing pornography from the internet. The Bill is currently before the Commerce Parliamentary Select Committee.

68 See "Net Nasties", ibid.

69 776 F Supp 135 (1995).

70 (1995) 23 Media L Rep 1794 (New York Supreme Court).

to an independent third party. The court held that there was insufficient evidence produced to show that the ISP either knew or had reason to know of allegedly defamatory material published on their network.[71] The court held that Compuserve had no more editorial control over this material than a public library or bookstore and that it would therefore not be feasible to require Compuserve to examine every publication for potentially defamatory statements.[72] In contrast, the New York Supreme Court in *Prodigy* held that an ISP was liable for defamatory material posted on its system. This was because the court believed that Prodigy, the ISP, was holding itself out as an online service that exercised editorial control over the content of the messages posted on its computer boards.[73] So in the United States at least, the imposition of a duty on an ISP seems to depend on the kind of service the ISP holds themselves out as providing.

Although imposing some kind of duty on ISPs may be useful for controlling defamation or pornography on the internet it is probably not the way to solve the problem of misrepresentations in trade being made over the internet. First, ISP's would probably have much more difficulty identifying misleading information on the internet than they would have in identifying defamatory or pornographic material. In fact in most cases it would be impossible to know whether a statement is misleading or not. For this reason it is less fair to expect an ISP to filter out misleading information than it is to expect them to filter out defamatory or pornographic material. Secondly, if a duty was imposed on all ISP's to carry out some kind of filtering process, the cost of their service would inevitably increase. This cost would no doubt be passed on to consumers of the ISPs. Not all of these consumers will use the internet as a place to shop and so will not be affected by misrepresentations made in trade over the internet. It is perhaps unfair for them to pay for a service they do not use. As it is unrealistic to control misrepresentations by placing a duty on ISP's it is necessary to consider other ways of protecting cyber-shoppers.

2 *Online Protection Agencies and Self Help*

There are possibilities for consumer protection on the internet which do not involve government intervention. For example, the internet provides some scope for consumers to help future consumers by using publicity to inform them of defective products and scams. Many people around the world have probably now been emailed a copy of the United States secret cookie recipe which was sold at the exorbitant price of US$250 to a consumer who believed they were purchasing the recipe for US$2.50. Similar tactics could be used by consumers shopping on the internet to warn other shoppers of unreliable suppliers and misleading information. This kind of self-help is useful but it will not provide aggrieved consumers with a remedy.

---

71 Supra n 69 at 141.

72 Ibid at 140.

73 N Braithwaite, "The Internet and Bulletin Board Defamation" (1995) 145 NLJ 1216 at 1218, expressed the opinion that this interpretation of the facts is unrealistic. He considers Prodigy's situation to be remote from the editorial control exemplified by primary publishers since Prodigy in fact only retained a right to interfere, after the event, with material it considered unacceptable.

Another option for protecting consumers without government intervention is to introduce on-line consumer protection agencies. These are private agencies which offer a consumer protection service to suppliers and consumers. An example of such an agency is The Internet Consumer Protection Agency.[74] Suppliers who want to join the agency must pass a test designed by the agency to determine whether they are a reputable business. The agency, among other things, contacts former clients of the business to get recommendations. If the supplier passes the test they must pay the agency in order to become a member. Once the supplier is a member then the agency seal of approval will appear on their home page. Consumers can then see the seal and be reassured that this is an approved company. If a consumer has a complaint that cannot be resolved with the supplier they can take it to the agency which will try to resolve the dispute. If the agency receives a number of complaints about the same supplier then they will remove that supplier from the membership list and may also publish a warning on the internet to consumers to beware of this particular supplier.

This kind of internet self regulation is a step toward protecting consumers shopping on the net. It is an inexpensive, quick and informal way for consumers to receive some kind of redress for faulty products or misleading advertising. It is, in effect, an industry ombudsman scheme. However, like other such schemes it does have limitations in its ability to protect consumers.

One of its main limitations is that the agency has no means of enforcing its recommendations. If the agency suggests that the supplier gives the consumer a refund or replacement product they have no way of ensuring that this happens. Another deficiency from a consumer perspective is that it is a voluntary system. There are still many suppliers who will not join the agency and can continue to do business in a largely unregulated market place. Lastly, because the agency's funding comes from the suppliers it is possible that the agency will fail to be an impartial judge of consumers' complaints. Even if the agency does act fairly, consumers may not perceive that justice has been done if they are aware that the agency is not an independent body. This last concern could perhaps be dealt with by government funding of on-line agencies.

In conclusion, while on-line protection agencies are important and do offer consumers shopping on the internet some protection, by themselves they offer far less protection than the law gives to consumers shopping in the traditional way.

3 *A New Cyber-Jurisdiction*

In 1993 a group of lawyers spent several weeks online discussing the possibility of independent jurisdiction over the internet to avoid territorial laws.[75] The concept of a new "cyber-jurisdiction" has been compared to the medieval "Law Merchant" system which was a set of rules for the trade fair where merchants

---

74 Found at: http://www.glen-net.ca/icpa

75 See A Wells Branscomb, "Anonyminity, Autonomy, and Accountability: Challenges to the First Amendment in Cyberspaces" (1995) 104 Yale L J 1666.

from various European countries gathered to trade goods.[76] The rules were not linked to any one country, and there were special courts and judges drawn from the traders themselves. Following this model, a cyber-jurisdiction might have its own informal court system in the form of online discussion groups or email communication. It might be possible to expel people from using the internet if they breach the rules.

Obviously the idea of a cyber-jurisdiction has not yet been fully explored and raises a large number of interesting issues. In-depth consideration of these issues is beyond the scope of this particular article[77] but some of the issues can be briefly summarised. For example, one central issue is who should decide the rules for the cyber-jurisdiction. There are a number of possibilities. It could be the internet users, or a government, or group of governments. One obvious option for rules relating to trade is the United Nations Committee on International Trade Law (UNCITRAL).[78] The cyber-jurisdiction concept would also involve deciding on a judiciary and determining how any decisions made by that judiciary would be enforced. Decisions would also have to be made as to whether the cyber-laws should be subject to the rule of precedent and whether they should be in a written document accessible to all internet users.

V Conclusion

Some of the problems facing the cyber-shopper are able to be dealt with by adapting the existing law in specific areas. For example, computer printouts of electronic transactions should be treated by the courts as original documentation of the transaction and, unless there is evidence to the contrary, they should be presumed to be reliable. In addition, if consumer contracts made over the internet start to use digital signatures, these should be treated in the same way as hand written signatures so that they are legal authentication of a document. The UNCITRAL Model Law on Electronic Commerce would be a helpful starting point for developing legislation to deal with these issues. New Zealand should also enact legislation which excludes computer communications from the postal acceptance rule so that consumers and suppliers doing business on the internet can be clear about their legal position with regard to contract formation.

Following the above suggestions in regard to the evidentiary problems and contract formation problems of electronic transactions would greatly improve the situation for the consumer shopping globally and locally in New Zealand on the internet. The consumer shopping globally would still, however, be faced with enormous difficulties in resolving a dispute with an overseas supplier.

---

76 I Trotter, "The Proper Legal Regime for Cyberspace" (1994) 55 U Pitt L Rev 995.

77 For two recent U S articles on developing a cyber-jurisdiction, see L Lessig, "Reading the Constitution in Cyberspace" (1996) 45 Emory LJ 869 and J Reidenberg, "Governing Networks and Rule-Making in Cyberspace" (1996) 45 Emory L J 911.

78 Note that the cyber-jurisdiction could aim to regulate in areas other than consumer protection. Each different area would raise its own issues. For example, if the cyber-jurisdiction aimed to regulate pornography and obscenity on the internet it may find this more difficult to regulate than standards of trade because community standards around the world on issues of pornography and obscenity are so incredibly diverse.

Suppliers operating on the global internet market remain largely unrestrained by consumer legislation. They currently have far more power than they do in domestic marketplaces. While New Zealand consumer protection legislation provides fairly comprehensive, accessible legal protection to consumers shopping in the traditional way, cyber-shoppers purchasing goods or services from overseas suppliers are often left to rely on good luck or recommendations given by other consumers.

As the level of global internet shopping increases, governments around the world are faced with the challenge of providing this new consumer with an adequate level of protection. The introduction of more online agencies would be a step towards meeting that challenge. Of equal importance, though, is the need to give real consideration to the development of a cyber-jurisdiction which would regulate the internet independently of national laws.

This kind of global regulation raises many as yet unsolved problems. Perhaps some of the problems of regulation are insurmountable and the consumer will have to accept that shopping on the internet is a high risk activity. If this is the case, it is the government's responsibility to educate the consumer of these risks. However, the option of legally protecting the cyber-shopper should not be dismissed without much thought and further research. International co-operation will be essential to any possible development of harmonised legal rules to regulate the internet and a method of enforcing these rules.