

- conducted with knowledge of the legal risks that are associated with the e-commerce process.

5.2 Teaming

One traditional model of legal practice is that you don't do the work until a file is opened. This means that there is an inevitable delay as the lawyer waits for instructions, opens the file, digests the instructions and then works towards a solution.

This delay will become intolerable for businesses participating in the new economy. Faced with the choice of waiting for the lawyers to signoff and getting a product to market the business may sooner proceed to market in the knowledge that there may well be legal flaws than risk losing the window of opportunity in which they can expect to make money.

What may be required is a rethink of the relationship between the lawyer and the client and the manner in which they interact. Lawyers will need to sense the market alongside the client to ensure that steps are taken along the way which will enable the client to respond with a minimum of legal friction.

The teaming approach maximizes the window of opportunity for the client's product. However, in order to work the approach may require a complete rethink on how information is exchanged between both parties, and the time costing revenue model which has been serving lawyers for years.

6. The Future

We may not always see the changes which transform our lives:-

1859: "Drill for oil? You mean drill into the ground and try to find oil? You're crazy!" Drillers whom Edwin Drake tried to enlist in his project to drill for oil.

1876: "This "telephone" has too many shortcomings to be seriously considered as a means of communication. The device is inherently of no value to us." Western Union Internal Memo.

1920: "The wireless music box has no imaginable commercial value. Who would pay for a message sent to nobody in particular?" David Sarnoff's associates in response to his requests for investment into radio.

1968: "'But what...is it good for?" Engineer at the Advanced Computing Systems Division of IBM, commenting on the microchip.

Whether the new economy is just the old one dressed up by a clever marketing department somewhere remains to be seen.

However, what cannot be ignored is that when you look beyond the buzzwords, business strategies are starting to reflect the themes of the new economy. Most notably, in the case of e-commerce many businesses are changing their market processes and the sum of these processes will, at least in part, define commerce in the future.

Unlike those who failed to recognize the changes that have transformed our lives, lawyers have no excuse for not recognizing the threats and opportunities that the new economy is bringing with it. More importantly, if you now take time to think about the new economy, you may avoid wondering later - with all the dubious benefits of hindsight - "What might have been, if only I had seen what was coming?"

Cyber Jurisdiction—Emerging Issues & Conflicts of Law when Overseas Courts Challenge your Web

Bernadette Jew, Gilbert & Tobin Lawyers

- 1.1 In considering the legal issues relating to jurisdiction and their application to the Internet, we are forced to think beyond the question of whether we "should" regulate the Internet and to consider whether we actually "can" regulate the Internet. In other words, do the Australian courts legally have jurisdiction to govern any particular activity on the Internet?
- 1.2 The issue is basic to maintaining a viable judicial system: when can one party require another party, which is located outside of Australia, to come and defend itself before the Australian courts? Or vice versa? Given the litigious world in which we live, this uncertainty in the area of jurisdiction has the potential to inhibit the growth of the Internet.
- 1.3 The jurisdiction of the conventional courts over disputes is geographically based - courts in Australia have power only over persons and things having some relationship with Australia, and courts in other countries or states only have jurisdiction over persons and things having some relationship with their own particular country or state.

- 1.4 By comparison, the Internet is both multinational and non-national. For example, in moving from one website to another by following hypertext links, the user is almost completely indifferent as to whether the file he or she is viewing resides on a computer down the road in Sydney, or across the other side of the world in London. The cost and speed of message transmission on the Internet is almost entirely independent of physical location. Also, there is no necessary connection between an Internet address and a physical jurisdiction. In fact, the Internet is so insensitive to geography that it is frequently impossible to determine the physical location of an Internet user or the location of materials which are accessed on-line.
- 1.5 Also, anonymous communication is within the reach of anyone using the Internet, thanks in large part to the easy availability of powerful cryptographic tools and the services of third parties such as remailer operators.¹
- 1.6 Australian courts may not only have difficulties in asserting territorial jurisdiction over matters arising on the Internet, but it may not even be possible to ascertain:
- the location where materials are sourced; or
 - the identity of the person or entity against whom a party is seeking to bring legal action.
- 1.7 Furthermore, the technology enables users to engage in regulatory arbitrage - to choose to evade unfavourable domestic regulations by communicating or doing business under regulatory regimes with different rules. The transfer need not even involve any physical movement on the part of the operator, since all Internet addresses are portable - they are not physical addresses in real space but, rather, are logical addresses on the network. The Internet user can simply reconfigure his connection so as to appear to reside in a different location. Today the operator of "****.com.au" domain may reside on a machine operating in Sydney, but tomorrow he may transfer his operation - and his Internet address - to a host machine in the United States, while at the same time remaining physically in Sydney.
- 1.8 We cannot ignore the flexibility of the structure of the Internet - it was, after all, created by the US Defence Department with the intent of ensuring that, in the case of war, no single computer or communication link was vital to the net's continuing operation. In other words, it was self-healing.
- 1.9 The issue of whether we "should" legislate matters relating to the Internet cannot be separated from the potential inefficacy of any such regulation. Rules which cannot be effectively enforced, whether due to lack of jurisdiction or otherwise, simply create a mockery of the Government.
- 1.10 It is often said that the Internet challenges the very notions of sovereignty. Principles of territorial jurisdiction that are reliant on physical location no longer work in the world of cyberspace where physical boundaries are irrelevant. Some writers have gone so far as to suggest that cyberspace needs to be treated as a separate jurisdiction.² However, before we can consider this extreme approach to jurisdiction in cyberspace, we need to "begin at the beginning" and take a brief look at the law relating to jurisdiction in the "real" or "physical" world. This is not just for the purpose of identifying those issues which the courts have taken into account in determining jurisdiction up until now. A review of existing law also illustrates the fact that, even without the added complications of the Internet and "cyberspace", the laws relating to jurisdiction and conflict of laws are full of uncertainty. It is one area of the law where there have never been clear-cut black-and-white rules. The courts have preferred to reserve a measure of discretion in order to ensure fairness on a case-by-case basis.
- 1.11 Accordingly, while the Internet community may be feeling frustrated by the lack of clear answers to the legal position on jurisdiction in cyberspace, this needs to be tempered with a "reality check". In many instances there are no clear-cut rules or instant answers to matters involving jurisdiction even in the real world.
- 1.12 Following a brief overview of the law relating to jurisdiction in Australia, we will then take a look at how the courts overseas have tried to apply their existing laws on jurisdiction to cases involving the Internet over the past 12 months. There are very few cases in the area, and they emanate mainly from the United States. However, they do illustrate the manner in which the courts are already relaxing the criteria required to establish jurisdiction - thus enabling the courts to reach beyond their own geographic jurisdiction and to assert some control over activities in cyberspace. It has reached the stage where courts are asserting jurisdiction on the basis that the "effects" of on-line activity are felt within their own geographical borders.
- 1.13 We will then look beyond existing laws to the future and "a world without borders". At the extreme end, it is advocated that territorial governments

cannot solve on-line disputes, and that there should instead be a self-regulatory regime - possibly a "cybercourt" established and run by system operators and users who know and understand the media. At the other end of the spectrum, the question arises as to whether there is any "new" issue worth discussing, or whether our existing laws can simply accommodate technological change without any alterations to the system.

1.14 In the context of this discussion, we will keep an eye on the real world and look at the efforts of various territorial governments and states to regulate the Internet. One Canadian writer has described this rush to legislate in vivid and colourful language:

"What rice is to the Japanese, what wine is to the French, regulation is to the Canadians.

When any new phenomenon appears on the horizon, whether it's in vitro fertilisation or superconductivity our first response is always the same: how do we regulate this sucker?"

There has been severe criticism levelled at much of the legislation introduced around the world to regulate the Internet. We therefore need to consider the wisdom of the Australian government following this direction, and whether there are other more viable options available to us.

2. JURISDICTION IN THE "REAL" WORLD

2.1 The term "jurisdiction" is often used in a very generic sense to cover several distinct legal concepts which arise in the case of a conflict of laws:

- governing law
- jurisdiction
- forum conveniens
- enforcement of judgments

2.2 The question of jurisdiction is quite independent of the question as to which law applies. Australian courts can, and do, decide cases in which issues are governed by foreign law.

2.3 Also, jurisdiction and forum conveniens are distinct concepts:

- "Jurisdiction" is a matter of whether a court has the power to hear and determine a case.
- Forum conveniens involves a determination of the court in which the matter can most appropriately be tried, in the interests of the parties and for the ends of justice.

2.4 Under Australian law, personal jurisdiction depends solely on valid service of the defendant. Generally speaking, if a defendant is properly served with Australian proceedings in accordance with Australian law, an Australian court has jurisdiction to hear and determine the case.

2.5 As a separate issue, "forum conveniens" involves a consideration of the forum in which the dispute can most suitably be tried. "Connecting factors" which the court will look for include not only factors affecting convenience and expense (such as the availability of witnesses), but also factors such as the law governing the relevant transaction, the places where the parties respectively reside and carry on business, and which forum can most effectively afford a complete resolution of the parties' dispute.

2.6 The final stage of the process, the enforcement of a judgment, can take place in a different jurisdiction to that in which the judgement was given. In Australia, it is possible to enforce certain judgments obtained in other

countries either on the basis of common law principles of recognition and enforcement, or by following the procedures set out in the *Foreign Judgments Act 1991 (Cth.)*.

Contractual arrangements

2.7 Where parties from more than one jurisdiction enter into a contract, the laws of several different jurisdictions could be relevant to issues arising under the contract. The law of the place where the contract was made, the law of the place of performance and the law of the domicile of each party are all relevant in the conflict of laws as it relates to contracts.

2.8 Often the parties to a commercial contract will include a specific clause dealing with issues relating to conflict of laws in order to try and ensure some certainty on the matter. For example, an Australian company selling goods to a Japanese distributor might want to obtain some certainty that it is not going to be required to defend a product liability claim in the Japanese courts, with the accompanying risk of exposure to enormous legal costs and legal liability (including possible liability for personal injury). By the same token, a German manufacturer selling goods to an Australian distributor might have concerns about being caught up in any legal action involving Australian law, given that our legal system is fundamentally different to the German legal system.

2.9 However, contractual provisions which seek to remove any uncertainty in relation to a potential conflict of laws are not always as effective as people might assume. For example:

- While the courts of most countries will normally give effect to a clause in a contract specifying the choice of law to govern the

contract, this does not amount to an agreement to submit to the jurisdiction of that country.

- A clause to the effect that the parties submit to the jurisdiction of a particular country does not mean that claims must be brought in that forum: only that they may be. Therefore, a defendant's agreement to submit to Australian jurisdiction is a relevant factor when considering whether Australia is the appropriate forum, but it is not decisive.
- Even where the parties have agreed to the exclusive jurisdiction of a particular country, eg: England, it is still possible for one of the parties to the contract to seek a stay of proceedings in that country, or to bring an action in another country, eg: Australia, if the party can establish that the Australia is clearly the more appropriate forum for determining the dispute.

2.10 The courts have avoided fixed rules which could operate in an arbitrary and unfair manner, and instead have placed greater importance in matters of jurisdiction on ensuring a fair outcome in each case. This is important to bear in mind as we move to the issue of jurisdiction in cyberspace. The ideal of developing a fixed set of rules on issues relating to jurisdiction in cyberspace may simply be unrealistic, and may not necessarily provide the best - or fairest - solution for on-line participants.

3. RECENT DEVELOPMENTS IN THE COURTS — ALTERING AN OLD COAT?

3.1 Much of the Internet jurisdiction jurisprudence comes from inter-state litigation in the United States over the last two years. However, many of these

decisions have been criticised for failing to seriously grapple with the nature of the Internet. They demonstrate the difficulty that courts will have in extending the existing criteria for jurisdiction into an electronic environment.

3.2 These cases also exist within the inter-state context, rather than the international environment. The issues tend to be simpler in an interstate arrangement, because State jurisdiction is governed by a common type of statute, and courts always have the reassurance of higher national courts to pronounce on matters of jurisprudence. In an international context, countries may have to depart from U.S. precedent and apply general principles to their own indigenous jurisdiction statutes. They also must decide the case without the possibility of being overturned or by a higher, universal court, and so are forced to develop their own jurisprudence on the matter.

3.3 Most American cases are based around the State's "long-arm statute", which asserts jurisdiction if the defendant has regularly solicited business, engaged in any other persistent course of conduct, or derived substantial revenue from goods used or services rendered in the State in question. This test is applied hand-in-hand with the "minimum contacts" test established by *International Shoe Co. v. Washington*.⁴

Compuserve v Patterson

3.4 The most publicised of these cases is *Compuserve v. Patterson*⁵, a decision of the United States Court of Appeals relating to an on-line trade mark dispute. In this case, a software designer based in Houston, Texas was found by the Appellate Court to be subject to the jurisdiction of Ohio. Mr Patterson used the on-line services of

Compuserve to sell his software. The software was distributed from Compuserve's computers located in Ohio, although the majority of sales were to individuals located outside of Ohio. While Patterson transmitted 32 software files to Compuserve to display for downloading, and also advertised software on the Compuserve system, he claimed that he sold less than US\$650 worth of software to only 12 residents of Ohio via Compuserve.

3.5 The dispute arose because Patterson alleged that Compuserve was infringing his common-law trade marks. Compuserve started distributing software of its own under a name very similar to that of Patterson's product. Compuserve sought a declaratory judgment in the federal district court in Ohio to the effect that they had not infringed Patterson's trade mark, and Patterson sought to have the case dismissed for lack of personal jurisdiction.

3.6 The Court has been severely criticised for finding jurisdiction where it almost certainly should not have.⁶ The Court acknowledged that Patterson's minimal sales in Ohio, taken alone, were not enough to establish minimum contacts with the State. While the contract between the parties provided that the agreement would be governed by Ohio law, this contract was entirely irrelevant to the due process analysis under the relevant law. However, the Court found jurisdiction only because it combined Patterson's Ohio sales with the contract - even though the contract had nothing to do with the suit relating to trade marks.

3.7 Looking at the case a little more closely:

- It is useful to remove the electronic distribution system from the scenario.

Suppose that Patterson had physically delivered the software to CompuServe, instead of distributing it on-line. It seems fairly clear that jurisdiction relating to trade mark rights would not be established simply as a result of the goods passing through Ohio or even being loaded and handled in Ohio.⁷

- What about the place of sale? Common law marks usually accrue rights at the place where consumers buy and use the goods to which the mark is affixed. In this case, there were only twelve sales in Ohio. That means that common law rights were most likely being generated outside Ohio. The Court seems to be assuming that when software held on a machine that is physically in Ohio is downloaded outside of Ohio, the sale of software takes place in Ohio. However, for purposes of common law trade mark law, this is not the case - the relevant acts in those sales (such as the decision to buy, usage and the association of the name with the source) would most likely have occurred where the users were located, not where the software was stored.
- It was simply fortuitous that CompuServe's server was located in Ohio - the same place as CompuServe's headquarters, and the State specified in the contract. The server could have been located in another state or in several states, each unknown to Patterson. Focusing on the physical location of the server in the analysis of matters involving jurisdiction

may create problems, because vendors who lease space from Internet providers may not know where their server is located - especially as overloaded servers may automatically default to secondary servers in remote locations, and because multiple servers in many jurisdictions may be dedicated to taking orders for the same product.

- In short, all the facts in the opinion seem to point to common law trade mark rights arising outside of Ohio. However, the decision clearly illustrates how the Internet will have an expansive effect on the jurisdictional reach of both state and national courts as the courts seek to control activities in cyberspace.

Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.

3.8 A District Court in New York applied similar reasoning to hold an Italian company in contempt of court in the United States in the case of *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*⁸ Back in 1981, a group of companies had been enjoined from:

"...using 'PLAYBOY', 'PLAYMEN' or any other word confusingly similar ... in connection with the sale, offering for sale or distributing in the United States, importing into or exporting from the United States, English language publications and related products."⁹

At that time one of the defendants, Tattilo Editrice, S.p.A, planned to sell a magazine called "PLAYMEN" in the United States. Playboy obtained an injunction against the publication of the magazine in the United States and in several other countries, but was unsuccessful in obtaining an injunction in Italy. Therefore, Tattilo continued to publish "Playmen" in Italy.

3.9 Around 1995, Tattilo established two "PLAYMEN" websites at <http://www.playmen.it> - a free service and a subscription service. When Playboy discovered the websites, it brought a contempt proceeding. The Court had to determine whether Tattilo had used the name "PLAYMEN":

"...in connection with the sale, offering for sale or distributing in the United States, importing into or exporting from the United States, English language publications and related products."¹⁰

3.10 Tattilo argued that it was merely posting pictorial images on a computer server in Italy, rather than distributing those images to anyone in the United States. They claimed that:

"...The use of the Internet is akin to boarding a plane, landing in Italy, and purchasing a copy of *PLAYMEN* magazine, an activity permitted under Italian law."¹¹

3.11 However, the Court found that Tattilo had actively solicited United States customers to its Internet site, and in doing so had distributed its product within the United States. When a potential subscriber faxes the required form, he receives back via e-mail a password and user name. By this process, the product is distributed within the United States.¹²

3.12 Recognising the territorial limits of its authority, the Court held that Tattilo could continue to maintain their website, but the Court prohibited them from accepting subscriptions from customers in the United States (although see paragraph 3.22 below for further developments in this case).

Bensusan Restaurant Corp. v. Richard B. King

3.13 Despite the "over-reaching" of the courts in *Compuserve v Patterson*, it seems clear that a passive-local website will not confer jurisdiction. This is a website that does not have interactive components (eg, order processing capabilities) and is only directed to people in a limited geographic area.

3.14 For instance, it was held that a New York Court did not have jurisdiction over a Missouri restaurant for trade mark infringement where the website for the Missouri restaurant was not interactive and was not designed to attract New York residents. In *Bensusan Restaurant Corp. v. Richard B. King*,¹³ a jazz club named The Blue Note had set up a website located on a computer server in Missouri. The website listed a telephone number that users could call to order tickets to attend shows at the club.

Bensusan Restaurant Corp owned a jazz club in New York which also was known as The Blue Note, and had a federally registered trade mark for "THE BLUE NOTE". The court dismissed the argument that jurisdiction was established merely as a result of the Missouri restaurant's website being available for viewing in New York. King did not have a presence of any kind in New York other than the website that could be accessed worldwide. The mere fact that a person can gain information on the allegedly infringing product is not the equivalent of a person advertising, promoting, selling or otherwise making an effort to target its product in New York.

Cybersell v. Cybersell

3.15 Similarly, in *Cybersell v. Cybersell*,¹⁴ the Court held that a web site run by Cybersell Inc., a website development company operating in Florida,

did not infringe the federally registered trademark rights of Cybersell, Inc., a commercial services company of Arizona. Applying the "minimum contacts" test, it found there was no infringement because the Florida company had no contact with Arizona other than hosting a web site which could be accessed by people in Arizona, and anywhere else in the world. The Court rejected the argument that because the Internet recognises no jurisdictional boundaries and is accessible around the world, a web site is necessarily intended for universal use. The Court said that to find otherwise would mean that "every complaint arising out of alleged trademark infringement on the Internet would automatically result in personal jurisdiction wherever the plaintiff's principal place of business is located."¹⁵

3.16 In summary, the effects of creating a website may be felt nationwide - or even worldwide - but, without more, it is not an act purposefully directed towards the forum state.

Zippo Manufacturing Co. v. Zippo Dot Com, Inc.

3.17 At the other end of the spectrum is the website that is specifically designed to attract people in all states, process orders and establish ongoing relationships with customers. For example, a company that offered a paid news service over the Internet, which had more than 3,000 paying customers in Pennsylvania, and had also entered into contracts with multiple Internet service providers to furnish its services to its customers in Pennsylvania, was held to have satisfied the minimum contacts requirement.¹⁶

3.18 In that case, the judge stated that the likelihood that personal jurisdiction can be exercised is directly

proportionate to the nature and quality of commercial activity that an entity conducts over the Internet. A passive website that does little more than make information available to those who are interested is not grounds for the exercise of personal jurisdiction. The middle ground is occupied by interactive websites where a user can exchange information with the host computer. In these cases, the exercise of jurisdiction is determined by examining the level of interactivity and commercial nature of the exchange of information that occurs on the website.

Blumenthal v. Drudge

3.19 In *Blumenthal v. Drudge*,¹⁷ where a Californian web host defamed a presidential adviser in Washington D.C., the Columbia Federal District Court found minimum contact to be established through a combination of the defendant's Internet contact and real-world contact with people in Columbia. The defendant lived, worked, and had his server located in California. However the Court took into account the fact that he "e-mailed D.C. residents, solicited funds from them, travelled to D.C. and phoned and mailed D.C. residents in search of gossip" in order to post his information on the Web.¹⁸

A balancing act

3.20 For the time being, there will be uncertainty in relation to Internet activity that falls somewhere between the passive-local presence and full interactivity examples. While the mere establishment of a website does not give rise to jurisdiction, since there is no intent to make direct contact with people in any particular location, the position may change after a certain number of sales have occurred in a particular jurisdiction, or

contracts have been entered into with a number of persons in a particular jurisdiction.

3.21 One factor which has always been relevant in determining jurisdiction is matters relating to convenience and expense (such as the distance that the defendant would have to travel, and the availability of witnesses, etc). However, as mobility increases, the importance of this factor will most certainly decrease.

3.22 It is unclear how a court would view the non-interactive website that serves as a mere advertisement, attempting to attract customers in all jurisdictions. If such a website is considered equivalent to an advertisement, then there will be no jurisdiction because advertisements placed in national publications do not by themselves provide a basis for jurisdiction wherever they appear. However, the contact achieved by even a passive website may greatly exceed that achieved by an advertisement. As one has court noted:

*"...unlike hard-copy advertisements ... which are often quickly disposed of and reach a limited number of potential consumers, Internet advertisements are in electronic form so that they can be accessed again and again by many more potential consumers."*¹⁹

3.23 In that particular case, a District Court in Connecticut found that because a website operated by a company in Massachusetts included an 0800 number, which presumably encouraged contact from another jurisdiction, this was an indication that the website was purposefully trying to reach residents outside of its jurisdiction. The Massachusetts company was therefore held to be subject to jurisdiction in Connecticut. This is despite the fact that there was little if any discussion in the case as to

whether any users within Connecticut had actually accessed the particular website or called the 0800 number. There was also little discussion of whether or not the Massachusetts company was aware that individuals in Connecticut had accessed its website or called the 0800 number.

PLAYMEN revisited

3.24 While there is certainly a fine line in striking the right balance between all these factors required to determine jurisdiction, we see a clear example of a New York Court "overreaching" its jurisdiction in the expansion of its opinion on the "PLAYMEN" case following a motion for reconsideration.²⁰ On reconsideration, the Court clarified its ruling with respect to the non-subscription portion of the Playmen website, that is, the portion that could be visited without the defendants knowing the identities or locations of the users viewing the website. The Court held that the fact that users "pull" the images from a computer in Italy rather than having the transaction initiate in Italy was irrelevant. The mere fact that the website invited users to download these images was sufficient to cause and contribute to their distribution within the United States. The Court required the defendants to:

*"...either shut down PLAYMEN site completely or prohibit United States users from accessing the site in the future."*²¹

3.25 Accordingly, while physical custody is still essential for personal jurisdiction in the criminal context (with reliance on extradition treaties and the like to effect enforcement), it has been relaxed in the civil context to allow courts to assert jurisdiction over persons involved in Internet activity simply where the "effects" of

that activity are felt in the forum state. The dividing line between passive/local activity, and activity which entitles a court to assert jurisdiction in the country or state where the website is accessed, is by no means clear. A proper resolution of these issues is critical in order to realise the promise of the Internet. The average user simply cannot afford the cost of defending multiple suits in multiple jurisdictions, or of complying with the regulatory requirements of every jurisdiction from which their website is accessed. This is totally at odds with the aims of international law, and has the potential to cause international chaos among web users.

4. WHAT IS "CYBERSPACE"?

4.1 The new global electronic network does in a sense create a new space or make it seem as if we have been moved into a new space. This is commonly called "cyberspace", but there is no generally accepted meaning for the term.

Cyberspace. A consensual hallucination experienced daily by billions of legitimate operators, in every nation... A graphic representation of data abstracted from the banks of every computer in the human system. Unthinkable complexity. Lines of light ranged in the nonspace of the mind, clusters and constellations of data. Like city lights, receding...²²

4.2 Whatever space we are entering, it amounts to a "displacement" in that these changes put us in a different environment from where we were. While the new media does not physically move us, it can have as much an effect on our orientation toward space and distance as any mode of transportation.

- 4.3 The theme of "displacement", of being put into a new space, shifts our attention away from the issue of what information is being communicated (whether it be pornographic, private or whatever) to how we use and communicate information on the Internet.
- 4.4 In cyberspace, it does not matter whether a website lies in one country or another because the networked world is not organised in that fashion. Internet protocols generally ignore geographic documentation. While Internet machines do have "addresses", these locate the machine on the network and not in real space. Also, while some Internet addresses do include geographic designators they are by no means conclusive. By way of example, the "www.nz.com" website was established some time ago by an Australian living in Boston in the United States, and it is maintained from the United States (with much of the content being prepared in Australia and then loaded on the server in the United States).
- 4.5 In order to fully appreciate what we mean by the Internet being both multinational and non-national, with events on the Internet occurring everywhere but nowhere in particular, it is useful to consider the common Internet practice of "caching" copies of frequently accessed resources. Some Internet servers will store partial or complete duplicates of materials from frequently accessed websites in order to avoid the need to repeatedly request copies from the original server. Therefore, the user may be accessing materials at a website located in, say, New York, or he may be accessing copies of those materials located on a different machine in Melbourne. Alternatively, he may be receiving materials transmitted from the cache in Melbourne, updated by occasional transmissions from the original server in New York. As a result, material which is being accessed may be compiled from information stored on more than one machine around the world.²³ For this reason, decisions such as *Compuserve v. Patterson* which place such emphasis on the physical location of the server to determine jurisdiction give rise for concern - they simply demonstrate a lack of understanding of the medium.
- Can we adapt existing law to cyberspace?
- 4.6 In many instances there may be concern over the legal questions in cyberspace when, in fact, there is no "new" issue worth discussing. What makes a legal issue new? After all, every new medium is fraught with complex new legal questions. Every player in every new technology thinks that their technology is fundamentally different and that the old laws don't apply. For instance, the U.S. position on jurisdiction would have it that if a company has physical contacts in a country, or has proven sales there, it generally will be bound by that country's jurisdiction. But in a country where they have an internet presence only, it generally will not be bound. However, in cyberspace, there is often no difference between having a physical presence in a particular geographical location and not. Indeed, the "minimum contacts" doctrine, which enunciates the idea of imposing different rules on the basis of physical presence and jurisdiction, is in many ways illogical to the Internet.
- 4.7 Jurisdiction depends on a State's control over a geographic area. The Internet, on the other hand, is an expression of the ability of technology to allow people to communicate and transact independent of geographical boundaries. The mechanics of jurisdiction therefore fit very uneasily with the structure of the Internet.
- 4.8 However, the common law has never "focused" on a technology, device, or medium except as necessary to the case at hand. On this basis, should existing laws simply be allowed to adapt to the new medium? Viewing the issue in this very general way would allow us to have a very simple legal system, and to accommodate technological changes without any alterations to the system. The problem with this approach is that it is unpredictable. It amounts to little more than the principle of "bring about justice as you think best". Many of the circumstances in cyberspace do give rise to new legal questions, and Internet users are calling for certainty - inconsistent outcomes means an inability to order their affairs to comply with the law. Narrowly-drawn specific rules that are addressed to the cyberspace context do have appeal. On the other hand, there is also the desire to avoid the cumbersomeness of having a multiplicity of different rules for different situations. Furthermore, simple easily articulated rules sometimes lack fairness. It is for this reason that the courts have adopted a flexible approach in relation to jurisdictional issues in the "real" world, and have reserved for themselves a large measure of discretion based on "the interests of the parties and the ends of justice".
- 4.9 These are matters of policy, and inevitably call for a consideration of cost/benefit analysis. What legal issues in cyberspace are "new" enough to merit a resolution specifically tailored to the cyberspace context? After all, some cyberspace issues seem wholly unremarkable, and are readily governed by the same

rules that are applicable to other forms of communication. Many legal issues that can arise from computer communications do not pose any new legal questions, nor should they result in calls for new or revised legislation. Other legal issues cannot be dismissed so quickly, particularly in the area of jurisdiction.

4.10 For example, there is a limit as to how far the law relating to jurisdiction can continue along current lines without there being international chaos. As we have seen, the courts are now finding that the "location" of events can include jurisdictions in which the effects of on-line activities are felt. However, because the effects of on-line activities can be felt simultaneously in every corner of the global network, all jurisdictions simultaneously feel the effects of the information posted there, so that all jurisdictions would appear to have equal claims to make law governing the content of any particular website.

4.11 The State of Minnesota in the United States has been particularly aggressive in this regard, seeking to enforce its own domestic legislation against out-of-state Internet users (even without the enactment of legislation relating specifically to the Internet). The position of the Minnesota Attorney General's office appears to be that those who venture into cyberspace must take their chances as to where they may find themselves defending a lawsuit. The official website of the State of Minnesota (located at <http://www.state.mn.us>) did at one stage post a "Warning to All Internet Users and Providers" issued by the Attorney General's Office stating that:

"...[p]ersons outside of Minnesota who transmit information via the Internet knowing that information will be disseminated in Minnesota are subject to jurisdiction in Minnesota courts for violations of state criminal and civil laws."

The Minnesota Attorney General has filed at least six lawsuits against out-of-state residents in connection with on-line activities that are allegedly harmful to Minnesota residents. The alleged activities of the various defendants include:²⁴

- Allegedly false claims about the health benefits of "germanium".
- The alleged sale of information about using two-cent stamps instead of thirty-two-cent stamps to save money.
- A credit repair service that allegedly recommends the use of an Employer Identification Number (instead of a Social Security Number) when applying for credit.
- An alleged pyramid scheme.

4.12 The high-water mark for finding jurisdiction in the USA was set by a Minnesota court in *State of Minnesota v. Granite Gate Resources*²⁵ where it held that a company based in Nevada infringed Minnesota direct marketing laws by hosting a website which advertised a planned on-line gambling service. The Court reasoned that once the site was posted on the Internet, it was available to all Internet users, 24 hours a day, 365 a year – including those in Minnesota. By posting material on a site that was accessible by Internet users in Minnesota, the Nevada company was engaging in submitting itself to the jurisdiction of Minnesota.²⁶

5. DO WE NEED NEW LEGISLATION?

5.1 It is important to bear in mind the interface between cyberspace and the real world. The Internet does not exist in a vacuum. At a fundamental level, both commercial and criminal activity affect the real-world rights to property and person. Therefore, some jurisdiction needs to be asserted if real-world property and personal rights are to be protected from attack over the Internet.

5.2 The problem comes, as we have seen, when the very idea of jurisdiction, based as it is on geographic boundaries, is difficult to apply to the Internet which does not recognise geographical distinctions. The result, according to many, is an alternative between cyberanarchy, on the one hand, and a chaotic matrix of international regulation on the other.

5.3 The common assumption that there will be anarchy in cyberspace unless governments around the world take positive steps to regulate in areas which could cause harm to citizens (such as pornography) may be misplaced. Indeed, the Minnesota example illustrates that government intervention, and the inevitable "overreaching" beyond geographical territory that this entails, can cause exactly the opposite effect. If the Australian government were to point to the effects of Internet activities within its borders to justify applying Australian law to a website containing content posted in, say, Japan, what is to prevent the Japanese government from asserting the corollary right to introduce legislation governing the Internet and to make its law applicable to content downloaded in Japan from servers located in Sydney?

What is to prevent any website being subjected simultaneously to the laws of all geographical territories?

5.4 Despite this threat of international chaos and the potential inefficacy of domestic legislation, there has almost been hysteria in the United States to legislate against, and to assert jurisdiction over, offensive material transmitted on the Internet.

5.5 In addition, the State of Georgia has been one of the few states to introduce legislation outside the area of censorship.²⁷ The Georgia law has two stated objectives:

- *"it prohibits the transmission of any information by anyone who does not fully identify himself; and*
- *it prohibits the "use" of any trade name, registered trade mark, logo, legal or official seal or copyrighted symbol, without permission from the owner, in a manner that would suggest that such permission has been obtained.*

The first objective is designed to prevent fraud, by preventing individuals from using false names, pseudonyms, or even acting anonymously, with respect to Internet communications. However, this ignores the fact that anonymous communication is within reach of anyone with access to a personal computer and a link to the Internet, with the State of Georgia having no control over, or recourse against, persons residing outside of the State who may send anonymous communications to persons residing in Georgia. The second objective seeks to protect copyright and trade mark holders from the improper use of their registered symbols and names. One State Representative has gone so far as to say that the Georgia legislation was passed by "legislators who don't know a gigabyte from a chigger bite." Similar legislation is also pending in California.²⁸

5.6 As we have seen, the Internet as a whole is not easily amenable to any nation's control. Once it allows its citizens to connect freely to the Internet, the ability of any one government to control the flow of information is greatly reduced. It is far too easy to avoid compliance with any particular domestic laws simply by hosting material in breach of the domestic legislation on a web server in another country where it is not illegal. Short of cutting off international telephone services, there is little that one can do keep out messages from any other country - or indeed to stop citizens from sending messages wherever they like. Without cooperation between the governments involved, there is relatively little that a government can do when its rules are being flouted.


5.7 Domestic regulation on the Internet will only give rise to "regulatory arbitrage". For example, Finn announced his intentions in 1995 to expand anonymous remailer services

IN OUR NEXT ISSUE...

Our next issue looks at

Telecommunications

Contributions from members of all Societies are welcome. Although this is the central theme of the issue, contributions can be on any topic relating to computers and law and can take the form of an article, product or book review, abstract or press release.

 Please send your contributions to the Editors no later than 14 February 1999.

to enable Internet users to evade national laws restricting Internet content. This is just the first of many efforts to create international havens for materials considered indecent by some countries, or havens for tax avoidance or illegal gambling or consumer-fraud scams, and so on. The same techniques can be used to avoid legal responsibility for intellectual property infringement, defamation or invasion of privacy.

- 5.8 The Florida Attorney General has recognised this position and concluded that regulation of Internet activities is a matter for national or international authorities, rather than a matter that states should address individually. According to Florida's Attorney General:

"...any effort to regulate the use of the Internet is better suited to federal regulation than to patchwork attention by the individual states. Evolving technology appears to be far outstripping the ability of government to regulate gambling activities on the Internet and of law enforcement to enforce such regulations. Thus, resolution of these matters must be addressed at the national, if not international, level."²⁹

6. RECENT DEVELOPMENTS IN AUSTRALIA

- 6.1 However, moving closer to home, Australia is in the process of drafting Internet censorship legislation. The proposed legislation, due in early 1999, will impose liability on ISPs who knowingly allow obscene or illegal content to be posted on the web by using their service.
- 6.2 The intention behind the legislation reflects traditional concerns as to the effects of publicly available content. In the words of the Federal Minister for Communications and the Arts, Senator Richard Alston, when announcing the new regime in 1997:

It's very important to strike a balance between ensuring the Internet continues to grow, and to create jobs, but at the same time to protect Australian citizens, and particularly children, from pornography and other offensive material on the Net.

- 6.3 The national scheme, which is conceived as an amendment to the Broadcasting Services Act 1992, is currently being developed by the Australian Broadcasting Authority (the ABA). Drawing from the Principles for Online Content Regulation, which were set out by Senator Alston and the Attorney-General in 1997, and the classification principles set out in the Federal Classification (Publications, Films and Computer Games) Act 1995, it seeks to identify web sites which are illegal under the Classification Act. It then proposes to inform the ISPs who provide carriage for the sites that they are carrying offensive or illegal content. Once they have been given notice, the ISPs will have a certain time period during which they must block access to the site or otherwise cease to carry it.
- 6.4 The State of Victoria was the first to revise its censorship laws for the Internet in this way. In January 1996, it inserted an online provision, section 57, into their *Victorian Classification (Publications, Films and Computer Games) (Enforcement) Act 1995*.
- 6.5 The Victorian legislation assumes that ISPs are able to exercise some degree of control over the content of material. While clause 57 prohibits the online publication or transmission of objectionable material, clause 57(2) provides that it is a defence to an offence where a person "believed on reasonable grounds that the material was not objectionable material". However, as the legislation carries a maximum

penalty of a A\$24,000 fine, or jail for two years, it has been severely criticised on the basis that it places a considerable burden onto ISPs to prove they didn't knowingly commit an offence:

"Victoria's zealous censorship laws could drive new industries and the Internet networks elsewhere...Victoria could be wiped off the online map and information industries chased from the state..."³⁰

To quote a Sydney lawyer:

"This is government by the clueless . . . They have not sufficiently discussed it and talked to people who know about these things . . . They haven't understood the medium."³¹

- 6.6 Western Australia and the Northern Territory have also legislated on Internet censorship, although adopting a less zealous approach than Victoria - with greater focus on the user rather than the intermediary.
- 6.7 The proposed federal scheme seeks to unify the various State legislation, so there will be minimal "regulatory arbitrage", where online pornographers will operate from whichever jurisdiction has the least onerous censorship regime. However, there are expected to be fundamental problems with the legislation, since as much as 98% of the content accessed by Australians over the Internet originates in the U.S.A. This will raise significant jurisdictional problems for Australian courts who wish to limit the content available over the internet. While the new federal legislation may prevent the hosting of objectionable material onto the Internet in Australia, it may not prevent Australians from accessing such material.

6.8 Applying traditional censorship models to the Internet represents a clash of technologies, as the antiquated technology of bureaucratic regulation meets the new technology of private and anonymous global communication. The likely result of the proposed scheme will be to impose significant insurance and regulatory costs on ISPs, while doing little to reduce the amount of offensive material available over the Internet. While it is all very well to bow to political pressures and to legislate in the belief that "we have to do something" and that domestic legislation will at least be effective against local content providers, there will come a time when this approach is no longer viable. After all, there is no doubt that the vast majority of so-called 'objectionable' material is created and resides outside of Australia. In the words of Ira Magaziner, President Clinton's senior Internet adviser:

*"What we understand now and what we have gone away from, is that even if it were desirable to censor the Internet, which we don't believe it is, but even if it were desirable, it is impossible, and life is too short to spend so much time doing things that are impossible"*³².

7. WHAT ARE THE OPTIONS OTHER THAN LEGISLATION?

7.1 Activities in cyberspace cannot be governed satisfactorily by domestic legislation, even legislation targeted specifically at the Internet, as any local territorial law is rendered largely futile due to the flexibility of the medium itself. Therefore, what other solutions are available to us?

- International treaties agreeing upon specific legal approaches within each country, along the lines of the General

Agreement on Tariffs and Trade (GATT 1994)?

- Perhaps an international convention that can enact uniform model laws? For example, the United Nations Commission on International Trade Law (UNCITRAL) which was established back in 1966 has issued voluntary arbitration and conciliation rules (1976), a Convention on the International Sale of Goods (1980) and other documents pertaining to international trade.
- The development by system operators and Internet users of "rules" for behaviour on the Internet? These could be enforced by system operators through the use of technical remedies, eg: banishment from the system. Alternatively, what about a separate "cybercourt" jurisdiction with a distinct delineation between cyberspace and the "real" world?
- In addition, what about the options available to individuals to regulate their conduct on a private basis - through contracts, private associations, custom (eg: "netiquette"), etc?

7.2 The prospect of all the nations of the world coming together and forging a series of comprehensive international treaties to bring all laws that could impact on Internet activity into line with each other is an appealing one - but not a likely one in the foreseeable future, given the time required for 160 countries to agree on anything. International treaties take decades to be ratified on a world-wide basis, illustrating the fact that sovereign bodies simply move too slowly, particularly considering the

current rate of growth on the Internet.

7.3 A more drastic approach is required, recognising the fact that cyberspace is more than just new technology. As information that was previously isolated and separate is now shared and used as if it were in one place, and as people who were once separated now communicate more often and begin to work together, new relationships and new institutions will be formed. Cyberspace encourages the formation of new entities and relationships linking people from all over the world in ways that could not have occurred in a print environment.

What solutions does the new technology offer?

7.4 It is becoming increasingly apparent that we should look not to existing territorial governments and their conventional laws but that, instead, a more viable solution may be found by looking to the technology itself. We need to recognise that the technology of the Internet provides system operators with technical controls over Internet users which territorial authorities could never assert through conventional legal principles.

7.5 The Internet itself comprises a set of network protocols that has been adopted by a large number of individual networks, allowing the transfer of information among them. Networks are not merely governed by substantive rules of conduct, they have no existence apart from such rules.³³ The law of cyberspace is already made by system operators and users through the existence of contracts and rules which are applicable to particular systems. System operators specify the terms and conditions of access to their particular systems or "spaces in cyberspace" - and users agree

to these as a condition of being granted entry. These agreements present the user with meaningful choice, because there is great diversity among the rules established in different areas of cyberspace. Furthermore, this cyberspace law is relatively easily enforced, because a systems operator can banish those who break it.

- 7.6 On this basis, Professor David Post of the Cyberspace Law Institute puts forwards strong arguments for the case that any discussion of rule-making in cyberspace should begin by looking at the role of the entities and institutions which are defining the network protocols.³⁴ Those entities and institutions are in a position to be the primary "rule-makers" for behaviour on the Internet. In other words, Internet technology provides scope for "digitising" behavioural rules.

Self-regulation

- 7.7 What this would mean in practice is the creation of a self-regulatory regime that is articulated and enforced by system operators and users. System operators have an extremely powerful enforcement tool at their disposal to enforce such rules - banishment. The operators in each corner of cyberspace can define the laws or "rules" for their own systems. It is likely that we will see the emergence of multiple groups of network systems forming their own confederations, each with its own rules or "constitutional" principles. Content or conduct acceptable in one "area" of the Internet may be banned in another. It is then up to individuals to choose which laws or "rules" they are willing to conform to when they choose to access particular areas of cyberspace.

- 7.8 System operators need to agree among themselves on the rules for the interaction of different groups of users, and certain

minimum principles that they will all accept - the violation of which will be met with standard enforcement strategies, including banishment. The Internet itself can provide the communication mechanisms for the development of these global rules between groups of system operators.

- 7.9 In relation to the resolution of on-line disputes, Internet users would need to agree to be bound by a particular dispute resolution mechanism as a condition of their participation in any particular network system. Furthermore, system operators would need to develop global rules for disputes involving the interaction of different user groups. In this regard, we are already seeing the gradual development of virtual courts, designed to arbitrate or mediate in the case of on-line disputes. Virtual courts have the potential to provide a very cost-effective means of dispute resolution, particularly in cases where the parties are separated by large physical distances.

Cyber-anarchy?

- 7.10 What emerges will represent the rules that people have voluntarily chosen to adopt rather than rules that have been imposed by others upon them. While this may sound like just another version of cyber-anarchy, it must be recognised that just as domestic legislation is ineffective to control the Internet, so too will it be ineffective to control the rules imposed by individual networks on their users. The technology is so flexible that, on a global basis, it will always be possible for a system operator to establish a new system which evades local territorial controls over its own system rules. We need to accept that we are dealing with an "unregulatable" medium in terms of conventional law. Only laws which can be

enforced on a global basis can impose any restraints on the rules in cyberspace.

- 7.11 Crossing into cyberspace requires a positive choice on the part of the user, which would make application of a distinct cyberspace law fair to those who pass over the electronic boundary. In addition, this approach to rule-making provides greater certainty for the Internet user than the current territorial approach with its "overreaching" beyond territorial boundaries. For example, Internet users would know that they need to abide by the "terms of service" established by a particular Internet service provider when they are in that online territory - rather than worrying about whether the Minnesota Attorney General will succeed in asserting rights to regulate their activities.

- 7.12 Thus, for Internet activities that impact only minimally on the vital interests of the government, the self-regulating structures of cyberspace seem better suited than territorial laws to deal with on-line legal issues. If a group of system operators and users collectively agree to abide by a certain set of rules in cyberspace, and if those rules do not fundamentally impinge upon the vital interests of others who never visit this new space, then the authorities of the physical world (whether territorial or international) should defer to this new form of self-government.

- 7.13 As for the international law approach, there will certainly need to be an international agreement in certain limited areas, but not on a comprehensive basis in every area of cyberspace (see paragraphs 7.15 and 7.16 below). After all, do we really need, or want, all of cyberspace to be governed by a single source of international law?

The diversity and choices that arise through the existence of numerous network systems, each with their own set of rules, is far more appealing.

"Externalities" - international co-operation still required

7.14 The proponents of a "pure" cyberspace jurisdiction would argue that territorial authorities should adopt a totally hands-off approach.³⁵ However, having argued the case for self-regulation, it is doubtful whether a totally "pure" cyberspace jurisdiction, which is totally independent from the physical world, would actually work. After all, people engaged in online communications still inhabit the real or physical world. There must be authority to remedy problems created in the physical world by Internet users which cannot adequately be addressed through self-regulation in cyberspace - bearing in mind that any such authority would need to be derived from international, rather than territorial, institutions.

7.15 Human nature as it is, there will always be areas of activity where people are reluctant to self-regulate, ie: where there is no incentive for system operators and users to act in the public interest. By way of analogy, in the real world there is not necessarily any incentive for people to take responsibilities for "externalities" such as pollution. Similarly, in relation to on-line activities there would need to be some residual jurisdiction for international institutions to exert underlying control over certain areas of criminal activity, taxation avoidance and other on-line activities which cannot adequately be controlled through self-regulation in cyberspace - and which would otherwise result in unacceptable adverse

consequences arising from a public policy point of view (with the "unacceptable" consequences needing to be defined by international agreement).

7.16 Therefore, we are not talking about comprehensive international agreement on all-encompassing areas such as web content. Rather, we are talking about addressing specific matters such as computer crimes which cannot be adequately self-regulated. In this regard, there have been calls for further harmonisation of the laws pertaining to computer crimes, both to allow transnational jurisdiction over computer crimes for new international bodies, and to enhance extradition and legal assistance treaties.³⁶

7.17 Ultimately, the ability to exert some underlying control over those "externalities" which cannot effectively be self-regulated in cyberspace will depend on the availability of civil and criminal courts based in the real or physical world.³⁷ After all, some wrongdoers can only be deterred from committing criminal acts if there is the potential for criminal prosecution. Therefore, even as cyberspace rules develop, their effectiveness may ultimately depend on the practical availability of physical enforcement in the real world as a last resort.

7.18 Therefore, there is still the need for international co-operation, and possibly some kind of international arbitration body or international court, to provide that "last resort". Private and public international institutions need to evolve to meet this requirement. Some scholars have suggested initiatives to improve the institutional framework of the International Court of Justice for dealing with international

legal disputes - it is actually an arbitration body, whose jurisdiction is presently limited to disputes between nations. Also, an International Criminal Court is being discussed under United Nations auspices.³⁸

7.19 The end result would not be dissimilar to the existing relationship between international, federal and state law. Territorial authorities would not be prevented from protecting the interests of those individuals located within their geographical territories, but they would need to exercise a significant degree of restraint when doing so. If a group of system operators and users collectively agree to abide by a certain set of rules in cyberspace, and if those rules do not fundamentally impinge upon the vital interests of others who never visit this new space, then the authorities of the physical world (whether territorial or international) should defer to this new form of self-government. This means that government control would be relative rather than absolute - in the same way that federal powers in Australia or the United States are subject to constraints due to the international obligations which they have accepted under treaty arrangements, and divested or given away to the various state legislatures.

8. CONCLUSION

8.1 The Internet is not just a new technology - it provides us with the opportunity to create new relationships and new institutions across the globe in a manner that we never previously could have contemplated. Spatial distance becomes irrelevant.

8.2 Therefore, while the age-old idea of stretching existing laws to the new technology may appeal as the most straightforward solution, it is simply not a viable one in the case of

the Internet. The Internet is too flexible a structure to be pinned down and controlled by territorial laws. Any attempts to assert jurisdiction in the enforcement of our domestic laws beyond that which we are entitled to in the "real" or "physical" world, and to try and control activities in cyberspace through the introduction of laws targeted specifically at the Internet, can only have adverse consequences for Australia. Internet activity will simply move off-shore.

8.3 In dealing with any legal issues relating to the Internet, we have to learn to understand the technology and the potential that it offers to provide its own solutions. The physical banning of pornography was once the obvious answer, but now we have technical solutions available to us that may be far more effective in keeping on-line pornography out of the reach of children than any of the existing legal restrictions on the distribution of print media which we have come to accept as the status quo.

8.4 "Self-regulation" in cyberspace is a concept which may cause a considerable amount of nervousness, particularly given the current proliferation of pornography on the Internet. By comparison, the establishment of international laws and institutions sounds a far more familiar and appealing concept. However, do we really want one source of international law to govern the Internet? This would simply inhibit the growth of the Internet, which is capable of facilitating unlimited diversity. Also, the reality is that it would take forever to forge a comprehensive international agreement on every aspect of governance in cyberspace. After all, the Internet is now impinging on every aspect of our every-day lives.

8.5 In conclusion, unless any particular activity on the Internet:

- cannot be controlled through the rules adopted by system operators and users (together with the enforcement mechanisms available to system operators though the technology itself); and
- has unacceptable adverse consequences from a public policy perspective (which would need to be agreed on an international basis to be effective), there seems to be no good argument against allowing Internet users themselves to choose the rules by which they will be bound.

- 1 See generally Froomkin, A. Michael, "Anonymity and its Enemies", 1995 J. ONLINE L. art. 4, available at <http://warthog.cc.wm.edu/law/publications/jol/froomkin.htm>
- 2 See Johnson, David R. and Post, David G., "Law and Borders - The Rise of Law in Cyberspace", Stan. L. Rev. 1367(1996), p48.
- 3 Fulford, R., "As a Rule, Canadians Love to Regulate", The Globe and Mail (22 December 1993) Cl., cited in Slutsky, B.A., "Jurisdiction Over Commerce On The Internet", available at <http://www.kslaw.com/menu/jurisdic.htm>
- 4 326 U.S. 310, 316 (1945).
- 5 89 F.3d 1257 (6th Cir. 1996).
- 6 Burk, Dan L. "Jurisdiction in a World Without Borders", 1 VA. J.L. & TECH. 3 (1997), available at <http://www.student.virginia.edu/~vjolt>
- 7 See Slutsky, B.A., supra at note 3 and the discussion of *Asahi Metal Indus. Co. v. Superior Court*, 480 U.S. 102, 112, 107 S.Ct. 1026, 1032, 94 L.Ed.2d 92 (1991) (plurality opinion) ("a defendant's awareness that the stream of commerce may or will sweep the product into the forum State does not convert the mere act of placing the product into the stream into an act purposefully directed toward the forum State."); and also discussing *World-Wide Volkswagen*, 444 U.S. at 297 ("the foreseeability that is critical to due process analysis is not the mere likelihood that a product will find its way into the forum State.")
- 8 U.S. Dist. LEXIS 8435, 39 U.S.P.Q.2d 1746 (S.D.N.Y.1996).
- 9 Ibid, p1748.
- 10 Ibid.
- 11 Ibid, p1752.
- 12 Ibid.
- 13 U.S. Dist. LEXIS 13035 (S.D.N.Y. September 9, 1996.)
- 14 Fla., No. 96-17087 (9th Cir., Dec. 2, 1997)
- 15 See also *Hearst v Goldberger*, *Hearst Corp. v. Goldberger*, 1997 U.S. Dist. LEXIS 2065; 1997 WL 97097 (Feb. 27, 1997 S.D.N.Y) (online at <http://www.esqwire.com/report.htm>), in which a New York court found that the New

Jersey provider of "Esq-wire" website, who did not trade in New York, did not infringe the rights of the New York-based Hearst Corporation, publisher of "Esquire" magazine. The Court said that to find jurisdiction would open any website provider to liability in any state, or indeed in any country.

- 16 *Zippo Manufacturing Co. v. Zippo Dot Com, Inc.*, Civil Action No.96-397 Erie (W.D. Pa.) (January 16, 1997).
- 17 992 F. Supp. 44 (D.D.C. 1998)
- 18 Cendali, Dale M. & Weinstein, Rebecca L. "Personal Jurisdiction in Cyberspace", NYLJ, July 20, 1998. Online at <http://www.ljx.com/internet/0720cyberjur.html>.
- 19 *Inset Systems, Inc. v. Instruction Set, Inc.*, 937 F. Supp. 161, 164-65 (D. Conn. 1996).
- 20 *Playboy Enterprises, Inc. v. Chuckleberry Publishing, Inc.*, U.S. Dist. LEXIS 9865 (S.D.N.Y. 1996).
- 21 Ibid, p11.
- 22 Gibson, W., *Neuromancer* (1984) p51.
- 23 See Burk, Dan L., supra at note 6.
- 24 See Slutsky, B.A., supra at note 3
- 25 No. C6-95-7227, 1996 WL 767431 (Minn. Ramsey County Dist. Ct. Dec. 11, 1996), aff'd, ___ N.W2d ___, No. C6-97-89, 1997 Minn. App. LEXIS 1053, 1997 WL 557670 (Minn. Ct. App. Sept. 5, 1997).
- 26 This decision runs counter to the more recent *Hearst v. Goldberger*, 1997 WL 97097 (S.D.N.Y. 1997), supra note 15, in which it was held that the mere presence of a site on the Internet is not sufficient to confer personal jurisdiction on the Court in the plaintiff's State.
- 27 Act No. 1029, Ga. Laws 1996, p1505, codified at O.C.G.A. 16-9-93.1. The law is commonly referred to as the Internet Police law.
- 28 California Senate Bill SB-1533, 1995-1996 Reg. Sess. (Ca. 1995-1996), and S.B. 1034, 1995-1996 Reg. Sess. (Ca. 1996).
- 29 Florida Attorney General Advisory Legal Opinion No. AGO 95-70 (18 October, 1995).
- 30 Van Niekerk, M. "News laws take state off-line", The Age, 21 November 1995, p41.
- 31 Ibid, citing Argy, P.
- 32 December 1997 online interview with Richard Cousins, president of Australia's Internet Industry Association.
- 33 For a detailed discussion, see Post, David G., "Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace" (1995) J. Online L. art. 3, 10 available at <http://www.law.cornell.edu/jol/jol.table.html>
- 34 Ibid. David G. Post is Visiting Associate Professor of Law, Georgetown University Law Center and Co-Director of the Cyberspace Law Institute.
- 35 Supra at note 2.
- 36 See Perritt, Henry H. Jr., "Jurisdiction in Cyberspace: the role of intermediaries", available at <http://www.law.vill.edu/harvard/article/harv96k.htm>
- 37 Ibid.
- 38 Perritt, Henry H. Jr., LAW AND THE INFORMATION SUPERHIGHWAY, (John Wiley & Wiley & Sons 1996), pp632-633.