and current affairs defines a network and its credibility and respect with audiences.

Technology can do so much to bring us closer. It can increase the sense of community. It can aid in the process of integrating our rich and diverse culture. It can provide the basis for a major export industry that will cement forever Australia's identity on the global stage. It can also, if we aren't very careful, cause us to lose touch with our neighbours and fellow citizens as we disappear in a fog of global tecnobabble. Technology is a tool and a good and useful tool, but it is a tool nonetheless. 158 years ago, Wheatsone and Cooke in England, and Morse in America, invented a means of transmitting coded letters by copper at close to the speed of light. 158 years is only a brief period in history, but it has delivered all the ingredients to radically change our media, our lives, our culture and our national identity.

Technology took a giant leap forward in 1948 when Shockley's team in the United States invented the transistor. Today, a single chip can contain 10 million transistors - a number that nearly doubles every couple of years. Once it was thought that the world would only need a few computers. Today, computers are a part of our lives and computer capacity doubles and halves in price every two years. 40 years ago, hardware encompassed a typewriter, a telephone, a radio... and possibly a television set. Today the hardware includes: set-tops, servers, terminals, consoles, CD-Roms, VCRs, facsimiles, PCS and television.

The delivery platforms have also come a long way. Broadcast television, telephone companies, cable television, direct broadcast satellite, personal computers, wireless, on-line, cinemas - even the corner video store. How individuals, community organisations, businesses and government respond to technological changes is very important to Australia. The technologies have the potential to increase our standard of living, not just economically but also qualitatively. They can make us better human beings with a wider knowledge and understanding of the world in which we live. They have their dangers too, especially for a country like Australia. The principal danger is that we become swamped and our culture eroded by the avalanche of material from other countries, particularly the United States.

There is an Australian culture and it is worth preserving. Information and communications policy is essential to that task. Very simply, without communication, there is no culture. The two are almost synonymous: most acts of culture are acts of communication of one sort or another. The greater the level of foreign involvement in these acts or communication, the greater the risk that our culture will be diluted. There is a unique Australian identity that is worth preserving and this identity is under threat from the globalisation of the information industries and the present lack of direction and co-ordination in the introduction of new communication technologies. At the moment, Australia is hell-bent on laying cable above and below the ground - at a cost of many billions of dollars. All these services could be much more easily provided through satellite delivery, a process which would ensure a quality of service at a fraction of the cost to all Australians. Technically, there is no reason why we cannot be providing hundreds of channels from the sky before the cable is rolled out.

As I outlined in the Boyer Lectures, capital is a limited resource and as a nation we should be looking to optimise its utilisation. A little earlier, I referred to a danger that we could become a suburb of Los Angeles. This is no particular slight on Los Angeles - it's just that Los Angeles is not Australia and there is no need for us to surrender our cultural identity, certainly not without a fight.

Kerry Stokes is Chairman of the Seven Network. This is an edited transcript of a speech presented at a recent Cable and Satellite Television Conference in Sydney.

The Legal Frontier of the Internet I

Robert Cumbow predicts that the United States response to the legal and regulatory challenges posed by the Internet will generally be the adaptation and application of traditional legal principles.

The Internet, though not new, has enjoyed phenomenal growth in the last couple of years, and even more phenomenal media attention in the last few months. The past year has certainly been the year of the Internet This has been due, in large part, to the advent of the graphically appealing World Wide Web, and computer software that enables it to be accessed and used efficiently.

With the increase in population on the Internet has come an increase in conflicts and controversies, giving rise to a recognition of the need for some form of authority and order, some standard by which conduct on the Internet can be measured.

But because the Internet has, until recently, been a frontier, populated by pioneers, and pioneers do not take easily to being told what they can and can't do, there is considerable resistance to the idea of Law on the Internet.

And not without good reason. It is entirely legitimate to ask not only whether there **should** be law on the Internet, but whether there **can** be.

People who ask whether there **should** be law on the Internet often point out that the Internet doesn't need law, because it is self policing. 'Netiquette' is the term given to the unwritten code of behaviour that governed the Internet community while it was still a close-knit group of computer cognoscenti.

One rule of Netiquette was 'Thou shalt not advertise'. Any effort to turn the net into a commercial communication medium was staunchly resisted. 'Spamming' - the sending of self-promoting messages to all members of one or more news groups was universally condemned. It was the one form of net misconduct that justified 'flaming' - the sending of harassing and insulting messages in reaction to someone else's communication.

In a way, this resistance to early efforts to use the net for commercial communication led to the growth of the

WorldWide Web. While deliberately sending commercial information to an audience that mostly did not want it was intolerable, no one could fault you if people came to you for it. As soon as it became practical to do so, businesses and other organisations began establishing web sites, offering information about themselves and their services. Spamming is still frowned upon; but the battle to keep the Internet non-commercial has already been lost.

That fact has made it seem increasingly necessary that some form of control be exercised with regard to what can and cannot be done on the Internet. But many people - particularly the long time Net pioneers - ask whether there can be law on the Internet? Some believe the transfer of digital information, by its very nature, excludes the possibility of law - at least in the traditional sense. They speak in terms of 'virtual space', the realm in which Internet communication takes place, a community without boundaries, in which information can be received, copied, altered, and re-ransmitted in seconds. There are a number of reasons why such a community does not easily lend itself to the traditional rule of law. Not the least of these is the question, Whose law? The Internet is truly global, so what nation's law can contain it?

But, others argue, virtual space is not real space, and the Internet is not an actual 'place where transactions occur' it is merely a network of relationships, not significantly different from telephone service networks. Telephone services span the globe; yet there has never been a serious legal difficulty in determining what law to apply to a question or dispute arising from some intercontinental communication, transaction, or transgression involving the use of the telephone. Like any new medium, the Internet may simply seem more different that it actually is. Digital information may not, after all, be substantively different from physical property; and people's rights and responsibilities may not be so terribly different on the Internet than they are in any other medium of human intercourse.

Arguments for regulation.

There are certainly compelling arguments for some form of control on Internet communications. Among these are:

- The need to protect Children: There is a need to assure adult's privacy and free expression, while still protecting children from abusive, harmful, or simply inappropriate materials.
- The need to protect consumers: The Internet may be used as mechanism for consumer fraud. On the Internet, its easier to pretend to be someone or something you aren't.
- The need to protect business and property interests, to prevent theft or devaluation of intellectual property and to preserve fair competition among businesses.

Even people who see the need for Internet users to recognise the rule of law urge caution in the area of government control. In the United States, a number of questions have arisen with respect to governmental regulation of the Internet.

- Since the government built the Internet, why shouldn't it regulate it?
- If the government should police the airwaves, why shouldn't it police the Net?
- Is the Net enough like broadcasting or publishing to be subject to similar regulation?
- Or is the Net more like the mail? The government doesn't read my mail (at least as far as I know), so why should it read my e-mail?
- Or is the Net more like the phone system? Federal wiretap law applies to phones and faxes - and maybe to e-mail.

Arguments against regulation

Those who oppose government regulation argue that such control could mean censorship; but the mere threat of government control could mean self-censorship, which can be just as chilling to free expression. If the Internet stands for anything, it is free expression. That is its principal attraction and another reason that its users are so resistant to external constraint.

A more practical argument is often put forward by those who oppose the rule of law on the Internet - enforcement is difficult if not impossible. As we examine briefly some of the legal disputes that have already arisen with regard to certain Internet issues, we shall see that there is a measure of truth in this. Sometimes it may be difficult to tell whether a wrong has been done, or, if it has, who the perpetrator was. But the practical difficulties of enforcement should not serve as an excuse to abridge substantive rights such as the right to one's own creative work, or the right to have one's reputation untarnished by lies or misinformation.

One form of enforcement already exists, not in the government but in the online service providers, many of whom have subscriber rules regarding copyright, defamation, offensive language, abusive activities (such as screen scrolling). These are easily enforced by the threat of cancellation of one's access.

Despite the voices of the pioneers who claim that the Internet is so different that traditional law cannot apply to it, the general consensus seems to be that the law as it already exists applies in most ways to Internet communication. Let's look at some of the ways in which traditional law continues to provide the rules of the road for the Internet and some of the areas in which new law is being made.

Defamation

Although the Internet is an important medium of free expression, and has arguably become so popular precisely because its users feel they can truly speak their minds online, there is a limit to what anyone can say about another person. Defamatory speech is not protected as free expression.

Generally, to be defamatory, a statement has to be false, it has to be published, and its publication has to harm the person about whom the statement is made. A statement of opinion, or a mistake of fact, is not defamatory. There must be an intent to publicize a falsehood, or at least negligence with regard to the truth.

Internet users have always been less than careful about the truth, often sending emotionally-driven messages off the tops of their heads, without pausing to consider where they are going, who will see them, and what harm they might do - in both directions. This has made the Internet a particularly hazardous environment for commercial businesses, who are considered fair game for net talk, and who may be seriously damaged (or rewarded) by online commentary about them and their competitors.

But although there is a fair amount of arguably defamatory speech on the

Internet, online defamation cases have so far concerned themselves with the question, Who is liable? The author of online defamatory remarks is often not a likely target for a lawsuit, but the online service provider may be. In *Cubby v. Compuserve*, 776F. Supp. 135 (S.D.N.Y. 1991), an online service provider was held not liable for defamatory information published on its service. It was held to exercise little or no control over the content of messages and postings carried on its service, making it more like a common carrier, and less like a publisher. But in *Stratton Oakmont v. Prodigy*, 1996 N.Y. Misc. LEXIS 229; 23 Media L. Rep. 1794 (Sup. Ct. N.Y. 1995), a court found that the Prodigy online service might, after all, be liable for defamatory comments made on its service, because Prodigy had held itself out to the public as a family online service that supervised for suitability the content of its various service features. More recently, in *Carib Inn v. America On Line*, the question has been asked whether an online service provider has a duty to reveal the identity of a subscriber who used its service to post arguably defamatory comments anonymously.

Harassment

Another form of unprotected speech is the kind of speech that is used to harass or threaten another person. Besides being a matter for civil action, this can potentially be criminal in nature, as was discovered by a Connecticut computer user who was prosecuted and had his equipment briefly confiscated under the State's computer harassment statute after posting unflattering comments about the State's governor. (News media republished the remarks verbatim with impunity under the news reporting privilege.) Jake Baker, a University of Michigan student, was arrested and charged with interstate threat under a federal statute after posting online a story in which he expressed dangerous fantasies about a female classmate. Baker was freed when the court decided that his posting was merely a piece of fiction, not an expression of his intentions regarding the woman.

Advertising

In the United States, commercial speech enjoys a lower level of protection, so a distinction has to be made - in peoples minds, on the net, and in the law - between purely informational communication and *promotional* communication. It may be harder to make that distinction online than in the pages of a newspaper or on television. One of the basic precepts about World Wide Web site, for example, is that, to be successful, it has to offer useful information. Does the fact that a commercial web site offers something useful to its visitors entitle the site owners to greater protection than that given to, say, a television commercial?

In the United States, the advertisement of cigarettes and alcoholic beverages are strictly regulated, and altogether prohibited in some media. Will advertisers use the net to find ways around these prohibitions? If they did, would that prompt the government to step in?

In France, advertising that expressly compares the advertiser's product with another is prohibited, and all advertising is required to be in French. Would a web site or a promotional posting in English, promoting one cola that was preferred over another in a taste test, be subject to censorship in France?

These questions are still being asked, so it is clear that, in this area of Internet use, the traditional law is not enough.

Privacy

The privacy questions raised with regard to the Internet express two sorts of concerns:

- Individuals invading one another's privacy
- Government invading everyone's privacy

Whether or not privacy has been violated depends first of all upon whether there was a reasonable expectation of privacy to begin with. Should someone who uses the net have a reasonable expectation of privacy? This comes back to the question whether the net is more public or private, more like a news publication or broadcast, or more like a personal letter or a phone call. But even that distinction does not work as well as it used to. Cellular phone users, for example, know that they are entitled to less expectation of privacy than users of conventional phones or writers of letters. Will the same be held to be true of those who use the Internet?

Questions of security are raised with regard to commercial transactions on the Internet, especially those involving credit card numbers. Ironically, many of the people who most resist the idea of giving out a credit card number online readily give out their credit card numbers on the phone, through the mail, and over store counters every day - yet these media of commercial transactions are no more secure than the Internet.

The ready availability of transaction records, however, can be used to great marketing advantage. Using the net, it may become easier for a business to know who is reading what, asking about what, and buying what. How much of this information *should be* accessible? And would a business be liable if someone got a customer's card number or other information from one of its transaction records? This concern presents an obstacle to online marketing - and that is why online security is one of the big issues of research right now.

One possible solution is the traditional one of limiting access by means of subscriptions (paid or unpaid), keyed to passwords without which a site cannot be accessed or a transaction cannot be made. Another is encryption, with which a site or posting might be accessed but cannot be *interpreted* until it is decoded. Encryption, if not the whole and final answer, is at least a good interim tool.

The United States government's restriction on the export of strong encryption, which it classifies as munitions, has stood in the way of universally available encryption sufficient to ensure a high level of security. But such encryption is already available in and from other countries, and the United States appears to be relaxing its encryption policy.

Its reasons for wanting to control the availability of strong encryption are, of course, good ones. Strong encryption can be a potent weapon in the hands of an opposing military or criminal force. For the same reason, the government pushed for the 'Clipper Chip', a proposed standard component of computer hardware that would provide the government with a 'back door' into encrypted communications. The proposal is virtually dead, following impassioned opposition by computer privacy advocates.

Another way of making online commercial transactions more secure is the use of digital cash. Services known as 'Digicash and 'Cybercash' have already appeared. Under these systems, generally, a consumer or business opens an account with a deposit of conventional money, and receives an equivalent amount of electronic cash, which can be used for quick, secure online cash transfers at the depositor's command. A system of multiple passwords and coding accounts are kept anonymous, so that only the depositor knows where and how the money has been spent, and is the only one who can access the electronic cash or transaction records.

Online crime

As already noted, some uses of the Internet may go beyond the bounds of merely civil dispute to become actual crime. Although not as prevalent as the news media make them seem, computer 'hackers' are out there, invading other people's files for fun and sometimes profit, occasionally causing costly damage. Less sophisticated, but also becoming Net-wise, are the more traditional thieves and grifters. An Arizona couple cheated Internet users out of $27,000 by offering to sell trading cards for a popular game called 'Magic', at $85 per card set. Money was sent, but no cards were delivered. The couple were indicted for mail fraud and went to prison. No wonder some Net users are nervous about online transactions.

The difficulty of detection and investigation makes online crime a continuing - perhaps growing - danger. Another problem in the war against online crime is that of evidence. What constitutes admissible evidence of a crime when you're dealing with digital information? How do you know it hasn't been altered or modified? How do you even know it's genuine? An American accused of violating child pornography laws escaped several of the charges against him when his prosecutors were not allowed to present into evidence materials from the hard disk of a computer in Denmark from which he had allegedly down loaded the pornographic images. And arrests have been made under child pornography laws for the computer transmission of images that were entirely computer-generated, and not photographs of real children at all.

In the criminal arena, too, encryption can be a threat rather than a welcome assurance of security or privacy. This is why government access to encryption keys is such a hotly debated issue.

Procedural Issues of Law

As mentioned earlier, if law applies on the Internet, *whose* law applies? Does sending or receiving information via the Net subject someone to the jurisdiction of the courts of a different state even a different country? If so, that could pose a serious obstacle to the much-predicted emergence of the Net as a widespread means of soliciting and transacting business. The problem of disparate advertising laws between the United States and France was mentioned earlier as one example. But even within the United States, local laws and community standards vary. A citizen of California went to prison for operating a bulletin board service that transmitted materials that, while perfectly legal in California, violated local laws in Tennessee, where the stuff was unfortunately down loaded by a US government employee.

Another legal issue arises from the growing use of the Internet as a source of legal research. Should non-lawyers who use the Net to provide information on law be subject to prosecution for practising law without a license? Should people who rely on legal advice given online by a lawyer from another state or country be entitled to sue that lawyer for malpractice if the advice turns out to be wrong? At what point in an online conversation about a legal issue between a lawyer and a non-lawyer does a lawyer client privilege attach? If a lawyer sends a client a document by e-mail, is the attorney-client privilege waived by arguably 'publicizing' the document? Should the attorney be required to encrypt the message? What impact will the availability on self-help legal resources on the Internet have on the legal profession?

Already mentioned in the defamation context is the issue of liability. Who is responsible when a civil wrong is committed online? Service providers were held not liable in *Cubby v. Compuserve*; but potentially liable in *Stratton Oakmont v. Prodigy*, and bulletin board operators have been found quite definitely liable for copyright violations in *Playboy Enterprises v. Frena*, 839 F. Supp. 1552 (D. fla. 1993) and for criminal violations of pornography laws as noted earlier.

Conclusion

So what are the trends for the future? Not the development of a complete new concept of former for a law-free Internet community, but the slow, agonizing process of adapting the principles and application of traditional law to fit the special cases that the Internet will, increasingly, present. But despite the agony and the slowness, the legal frontier of the Internet is an interesting place to be, and now is an interesting time to be there.

Robert C Cumbow is an Associate with Perkins Coie, Seattle, Washington.