December 2002

Regulating Cyberspace

Michelle Fong
Victoria University of Technology, Australia

Regulating Cyberspace

Michelle W. L. Fong

Victoria University of Technology
School of Applied Economics
Melbourne, Australia
Michelle.Fong@vu.edu.au

Abstract

The Internet's rapid pace of evolution has resulted in the need for government and policy makers to address its impact on society and to take into account the externalities generated in the cyberspace. Although the Internet has positive outcome in economic growth such as e-commerce, it may bring about undesirable negative consequences if it is not managed properly. This paper identifies some of the negative externalities and misdemeanours created and committed through the Internet and also discusses the possibility of unified regulatory effort for a reliable and healthy global Internet environment.

Keywords

Internet, computer and society, regulation, abuse and crime, ethics, social issues, value of information, globalisation of IS

INTRODUCTION

Advances in information technology have brought about profound changes to the lifestyle of mankind in particular, the intriguing development in electronic network capability – the Internet (Anderson *et al.*, 1995; Attewell and Rule, 1984). The Internet has evolved from a project initially funded by the US defence agency, into an academic tool and critical business infrastructure that extends into our daily life and home environment. By means of the Internet, we overcome time and spatial differences in our communication of words, sounds and pictures: making communication and learning more enjoyable and motivating.

In information sharing, the Internet enables people with common interest, but who may be strangers, to group together in cyberspace to share their views. This is evidenced by the many open websites such as hobby clubs, fans clubs and research groups. The information contributed to cyberspace by various interest groups is likened to a large library that can be accessed by anyone from any part of the world at any time so long as the users have the capability to go online. Information in cyberspace is readily available on any subject and as a result, exploring a topic of interest does not always require travelling to libraries and scrutinizing microfiches. Searching for information in cyberspace is made even easier by user-friendly search engines such as AltaVista, Yahoo! and Google.

Many of today's activities can be conducted online in cyberspace such as banking, shopping, communication and education. Increasingly, we find ourselves being embraced by a cyber environment that intertwines with the physical environment that supports our lives. The Australian Bureau of Statistics (ABS, 2001) revealed that household subscribers constitute the majority of Internet users; accounting for approximately 90 percent of the data downloaded from the Internet in year 2000, as compared to business and government subscribers. Children under 18 years access the Internet at home mainly for school homework or educational activities, followed by corresponding with friends or visiting chat rooms, browsing for leisure and playing games (NOIE, 2001). Adults' Internet activities were considered more wide-ranging than children's. These adults also used the Internet for activities such as online bill payment, fund transfer, teleworking and online shopping, although such activities have been experiencing a slow growth rate. Nevertheless, it is anticipated that our involvement in cyberspace activities will continue to grow significantly into the next decade as shown in Figure 1.

Due to the increase in the activities conducted in cyberspace as well as the capacity to transcend national frontiers and to generate substantial impact on individuals, nations and the world, there has been extensive discussion on whether the Internet is harming economic

life and social relationships. There is little consensus on the ultimate effect of the Internet on society, local communities or individual well being (Wellman and Gulia, 1999). The lack of a well defined statistical or measurement grounding hinders the conclusive assessment of the impact of Internet (Woodall, 2000; Parker and Grove, 2000; Davern and Kauffman, 2000; Cook, 1999). Despite this difficulty, it is widely acknowledged that there are negative elements in cyberspace that ought to be kept under control or even eliminated. The push for the Internet to remain open and unregulated no longer has strong support. The focus has shifted to debating the extent and type of regulation necessary for achieving a balance between the commercial aspects of e-commerce and social aspects of community living in cyberspace.

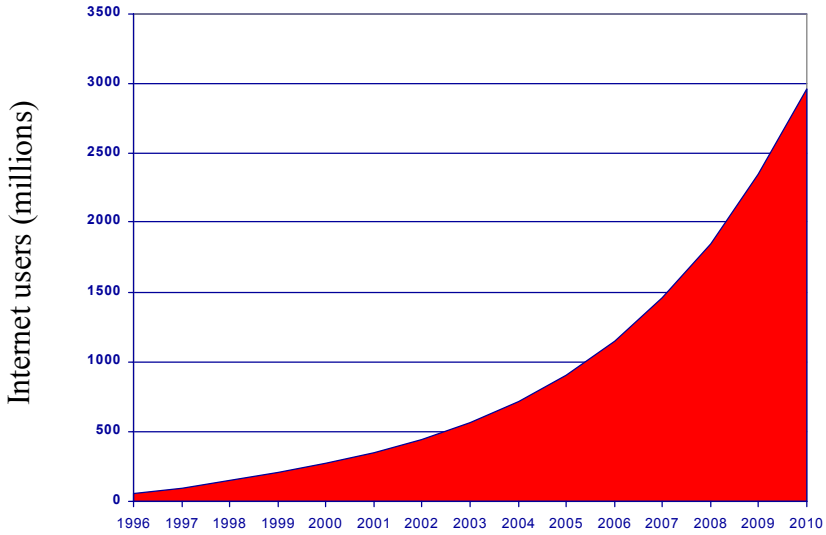

Figure 1: Global Statistics - Internet User Trends (source: NUA Internet surveys)

Prior to 1990s, the issue of Internet regulation attracted fewer concerns than today. The Internet's rapid pace of evolution has resulted in the need for government and policy makers to address its impact on society and to take into account the externalities generated in cyberspace (Morris, 2000; Lemley and McGowan, 1998). Although the Internet has positive outcome in economic growth such as e-commerce, it may bring about undesirable negative consequences if it is not managed properly (Fraumeni, 2001; Litan and Rivlin, 2001; United Nations, 2001). This paper identifies some of the negative externalities and misdemeanours created and committed through the Internet, which warrant intervention from the government, policy makers, corporations or individuals in order to ensure a reliable and healthy Internet environment. This paper also discusses the possibility of a unified regulatory system to ensure a reliable and consistent global Internet environment.

NEGATIVE EXTERNALITIES AND MISDEMEANORS IN CYBERSPACE

Cyberspace is a common property resource because no one has proprietorship and information contribution or extraction is largely unrestricted (Chrystal and Lipsey, 1997). However, free and uncontrolled access to such a resource will result in overexploitation as stated in the theory of externalities (Taylor and Frost, 2000; Randall, 1983). This overexploitation is likely to give rise to negative externalities and at a cost to society (also termed as the 'tragedy of the commons'). Examples of such problems are paralleled by happenings in our physical environment – air pollution and over-fishing in the ocean.

The non-proprietary architecture of networks and open technology standards have given rise to the expansion of cyberspace and the increase in the number of Internet users over the years. Therefore, there has been an increase in the various types of information contributed or exchanged in cyberspace. As each Internet user tends to behave or act in a manner that produces optimal satisfaction only for themselves and disregards the possible widespread benefits or costs that their actions may bring to the community as a whole (Eatwell *et al.*, 1991), information contributed by him/her may be beneficial to themselves but may be harmful to society.

Positive externalities are generated in cyberspace as more and more users are plugged into the network, as underlined by the Metcalfe's Law that the power of computers on a network rises with the square of the total power of computers attached to it (Gilder, 1995). However, the types of information contributed by the users could reduce or eliminate such externalities. Particularly when information harbours content objectionable to certain groups. In addition, unscrupulous activities (privacy invasion, lawlessness, intolerance and theft) may breed behind the veil of Internet anonymity in an unregulated cyberspace. There have been cases where criminals used the anonymity of the Internet and were often impossible to trace. History shows us that these problems will increase with increased use and knowledge of the Internet. The Internet is a powerful tool with global applications and has the potential to cause enormous harm if misused. Therefore, responsible bodies like government, policy makers, corporations and even individuals have a role in not only encouraging actions that are beneficial but also in preventing actions that are adverse.

Vulnerable Groups in Society

Pivotal to the discussion on whether the Internet is harming participation in economic life and social relationship is the concern for underage youngsters and teenagers. Computer and Internet technology are increasingly more prevalent in the home and an increasing number of children are accessing the Internet without the supervision they would have received in school. The ABS revealed that the number of children under 18 years who accessed the Internet at home rose rapidly between November 1998 and November 2000 (ABS, 2001).

Non-proprietary network or open Internet access allows people to exercise autonomy in their activities – deciding what to see and what to say. Internet users have quick access to any kind of information in the cyberspace, regardless of their age, cultural background and even legislative environment. In fact, the Internet has become a major source of information used by students and researchers (Kibirige and DePalo, 2000). Alarmingly, the information is perceived to be as credible as that found in magazines, radio and television (Flanagin and Metzger, 2000). Information in cyberspace is neither classified nor censored by a unified regulating entity. The danger in this situation depends on the information and on the extent of harm. Misleading information can bring about costly psychological and financial damage to certain groups in society. Embedded in the abundant information in cyberspace are materials that are harmful to the minds of children, such as adult or sexually explicit materials, pornography and materials promoting hate crime and deviance. The need to prevent children from accessing websites with objectionable contents without inhibiting the development of online businesses or the economy remains a challenge to government and policy makers of information economies.

Presently, the filtering software or filtered search engines available from the market place are not completely effective in blocking out the harmful materials from children (Wollenberg, 2001). Though the filtering program may block materials relating to health and sexual education issues, it may allow objectionable contents through. Filtered search engines may pick up websites that were deliberately created under innocuous address names but containing inappropriate materials for children. For example, the website 'teen.com' is an entertainment and music website for teens, but 'teens.com' and 'teenss.com' are both erotic sites. The Nanyang Technological University found that 40 percent of young teenagers in Singapore, a country with a low tolerance level for sexually explicit materials, have accessed the illicit websites unintentionally (The Straits Times, 2001). There are unscrupulous web page developers who can copy existing popular and harmless websites and insert coded instructions in the copycat sites that redirect users to adult sites operated by them (AFP, 2001). Some of the websites are known to have the capability to disable the browser's 'back' and 'exit' commands so that the Internet users are 'captured' within the websites. In addition to the redirecting capability of the websites, the web pages can also be developed with embedded text that misleads the search engines about the subject matter of the site, making it look like an innocuous link when it contains materials objectionable to children.

Effective ways are needed to prevent indecent or offensive material from reaching children through the Internet. The Australian government has introduced a number of measures to protect Australian families from inappropriate materials. One of the ways is to use Online Content legislation to remove materials identified in those categories commonly referred to

as pornography and paedophile activities. However, the legislative frameworks are not capable of completely shielding children from such information and websites. Although it is hoped that sophisticated technology will one day afford comprehensive protection for children using the Internet, the advent of technology can also bring about undesired outcome. For example, the attempt to stamp out illicit materials from the Internet in Australia has been hindered by the increasing sophistication and globalisation of electronic networks. Although child pornography offences carry a maximum penalty of ten years' jail term, paedophiles are increasingly using computer technology to communicate. Police find it harder to trace the culprits as the networks become more sophisticated (Silvester, 2001). In addition, decisions of Australian courts and legislatures have little bearing on activities outside their jurisdiction.

Currently, the best way to protect the children is through self-regulation – to supervise what they do online directly or by reviewing their activities through the browser's history list and bookmarks (Wollenberg, 2001). This means that parents in this time-poor society have to take an active interest in the activities of their children in cyberspace and may also mean that parents have to be equipped with the skill of handling the computer and software. The Internet age certainly requires parents to exercise supervision (self-regulation) on their children's Internet activities in the home. Another facet of computer usage among children that requires parental supervision is the children's tendency to become addicted to the Internet. According to The Alliance for Childhood (2000), an international child advocacy group, the computer could be hazardous to children's health. Health hazards take the form of repetitive stress injuries, eyestrain, obesity, social isolation, and may even escalate to long-term physical, emotional or intellectual damage. In addition, the group suggests that computer could cause communication problems and create a generation gap between children and parents. On the other hand, the concern that naïve and inexperienced children might fall prey to exploitation on the Internet has added impetus to the need for parental supervision. The veil of anonymity afforded by the Internet allows the easy disguise of identities, and this could turn the cyber setting into a situation of predator and prey. Cases of unscrupulous adult preying on young users have happened. Surveys have found that unwanted sexual overtures and solicitations tend to happen when young users accessed the Internet at home. In the US, it was found that only a small percentage of such cases were reported to an authority such as a teacher, Internet service provider, or law-enforcement agency (Finkelhor *et al.*, 2001).

Loss of Productivity

The Internet has been playing a large role in the corporate world for the past decade. There have been positive projections and reports of the Internet helping businesses to reduce costs, market products and services effectively and meet customer needs (NOIE, 2002a; Mandel and Hof, 2001). For example, a report from the Pew Internet and American Life Project found that 72 percent of US workers who have Internet access on the job said that the Internet helps in their job performance (Pew Internet Life Report, 2000). On the other hand, there has been press coverage and reports suggesting loss of productivity in companies because employees spend too much time on the Internet for purposes unrelated to work (Stanton, 2002). Research has shown that 32 percent of emails sent or received by Australian executives are not relevant to their job (Croucher, 2001a). In order to brace themselves against loss of productivity or legal entanglement, companies have began to monitor staff activities on the Internet. Although such process does raise the issue of invasion of privacy, 73.5 percent of major U.S. firms monitor employee phone calls, emails, Internet surfing and computer files. In Australia, it was reported that 75 percent of companies spy on staff emails (Croucher, 2001b).

While workplace Internet and email usage policies may seem strict, many companies do not enforce them unless their staff violates anti-harassment policies or basic work expectations. Companies such as Toyota, Holden, Centrelink and Telstra were reported by the press to have sacked or reprimanded workers after pornography was found on their systems. It is also noted that companies in Australia are tolerant towards staff misusing the Internet and emails. Twenty percent of the firms surveyed said that they would fire employees for the misuse of the company's telecommunications resources.

The communication support provided by the Internet is enormous. For example, Microsoft recently claimed that MSN Hotmail has been the world largest provider of free web-based email services and has 110 million active accounts worldwide (The Electric New Paper, 2002a). While an increasing percentage of email exchanges are taking place on company time, the continuing expansion of Internet usage means that companies need to adopt steps to manage their Internet traffic and to establish or enforce Internet usage policies already in place.

Spamming

Another negative impact that is related to loss of productivity is spamming. Spam is the Internet version of 'junk mail', which is an attempt by the sender to deliver a message via the Internet, to someone who would not otherwise choose to receive it. Spam can occur for several reasons, for example making a quick profit, being vindictive or for commercial advertising. An example of spamming that caused the victim to suffer loss of productivity is the case of a teenager in South India who bombarded a British company with thousands of email messages. The load of email messages generated by the spammer took up four megabytes on the company's server, forcing it to disable the email system for days. As a result, the company suffered losses in its online businesses (The Electric New Paper, 2002b).

Spamming could lead to mass-hysteria urban legend[1], whereby well-intentioned users unknowingly pass untrue or damaging piece of information onto colleagues and friends, and the spamming may be to the advantage of the original sender. An Australian was found guilty of sending about four million email messages around the world falsely stating that the shares in a US company would rise 900 percent, so that he could profit from the proceed of the sales of his shares when the mass-hysteria occurred. He was caught and sentenced to a two-year jail term (Tomazin, 2001; The Age, 2000). In another case, an email hoax was circulated by well-meaning users who trusted the content of the message that instructed readers to delete a Microsoft Windows utility before a virus supposedly in the software wiped the hard drive when activated on 1 June, 2001. The hoax, believed to originate from Portugal and translated into English by a well-intentioned computer user, caused a number of unsuspecting users to delete important Windows software from their hard drive (Johanson, 2001). Spamming is also capable of inflicting serious economic damage. For example, false rumours spread by two Chinese civilians over the Internet led to a massive run on a bank in China. The Chinese authorities claimed that they have managed to act fast in restoring stability and confidence in the financial system (Beijingscene, 1999).

While some senders of unsolicited emails contravened the law and were penalized for their behaviour, spam of a commercial advertising nature is yet to be directly outlawed by legislative provision in Australia. The problem of unsolicited commercial emails is increasing at a sharp rate. The Coalition Against Unsolicited Bulk Email estimated that the number of unsolicited emails received by Internet users in Australia has increased by six times in 2001 as compared to 2000 (NOIE, 2002b). Other surveys suggest that spam might account for ten to twenty percent of all email traffic in Australian organizations (NOIE, 2002c). Current anti-spam filters are only partially effective. If left uncontrolled, spamming could proliferate to the extent that it contributes to higher costs for Internet service providers, Internet end users and slower Internet speeds – all to the detriment of establishing an e-commerce economy. Spamming has been outlawed in European countries such as Austria, Denmark, Finland, Italy and Germany because consumers were found to have been unwittingly downloading spam at an exorbitant cost of US$8.8 billion a year (Livingston, 2002). In Australia, the government is reviewing the problem of unsolicited bulk email and possible counter-measures (NOIE, 2002b).

[1] A story, which may at one time have been true, that has grown from constant retelling into a mythical yarn (Netdictionary, 2002).

UNIFIED REGULATORY EFFORT: THE CASE OF CYBER-SQUATTING

The Internet itself does not generate negative impact or externalities but humans cause them. As a result, regulation is necessary to ensure that the Internet is a safe and secure international medium for people to enjoy and to use as a beneficial business, social and educational tool. Regulatory measures are expected to be on-going because the technology supporting the Internet will continue to evolve and force regulators to continually review their regulatory positions. One of the major issues and perhaps the most difficult facing the regulation of the Internet is unified regulation of global Internet resources due to the ease of data crossing national boundaries. Besides technical difficulty, legislation and cultural differences constitute formidable barriers for such an attempt. One obvious difference is censorship standards among countries, particularly between Asian and Western countries. For example, what is considered as obscene in Singapore is not necessarily so in Australia or in another part of the world.

Despite this, there are a number of separate initiatives at the global level. For example, the WHO (World Health Organisation) has a working group that governs the sale of prescription medicines on the Internet. This initiative is the result of concern that advertising, promotion and sale on the Internet might result in uncontrolled across-the-border trade of medical products or fraudulent imitations that may be unevaluated, unapproved, unsafe, ineffective or used inappropriately. Another example is the ICANN (Internet Commission for Assigned Names and Numbers), which is an international non-government organisation that coordinates the technical management of the Internet's domain name system, the allocation of IP address space, the assignment of protocol parameters, and the management of the root server system (ICANN, 2001). This organisation promulgated the UDRP[2] (Uniform Dispute Resolution Policy) and together with other dispute resolution providers[3], acts to discourage cyber-squatting[4] and other forms of domain name speculation that intend to create confusion with a trademark in and between countries of ICANN-approved registrars. The UDRP has been known to be a successful deliberation mechanism in a number of cases, providing an expedited, efficient and inexpensive alternative to litigation for parties in disputes involving bad-faith or abusive domain name registrations (Hillebrand, 1999).

In cyberspace, domain names and Internet addresses have become important navigation tools, facilitating global exchange of information and knowledge. Due to the free and open nature of the Internet or cyberspace during its early stage of development, it has been possible for early movers to register domain names (website addresses) that are similar to the valuable trademarks of well-known people or companies. It is especially disconcerting for these people and companies when web page owners use registered domain names in bad faith, exploiting the goodwill associated with established trademarks. The motive of these web page owners squatting in the cyberspace is usually financial gain. Those people or companies who do not want their names to be tarnished by association to pornographic or illicit websites, deliberately created by the cyber-squatters, usually have to buy the rights for these domain names. The asking price varied between US$550 and US$7.5 million. 'AltaVista.com' was sold for US$3.35 million in 1998, while 'business.com' was sold for $7.5 million in late 1999 (Sharrock, 2001). These amounts are phenomenal as compared to the cost of US$19.95 per year for registering a domain name through the internationally recognized registrar (NSI Registrar, 2000). This is a lucrative business for cyber-squatters; to the extent that a cyber-squatter was known to have changed his name by deed poll to Oxford University as part of a long-running battle to maintain a hold on the famous institution's Internet domain (Nowland, 2000).

Like the ICANN, the UDRP is not a substitute for the powers of government, courts and laws (Touton, 2000). However, most of the decisions made under the UDRP in resolving disputes

[2] The UDRP, which become effective on 24 October 1999, is a set of contractual provisions that are incorporated by reference into registration agreements between domain name registrants and ICANN-approved registrars (ICANN, 2002a).

[3] The other providers are the CPR Institute for Dispute Resolution, eResolution (has stopped accepting proceedings since 30 November 2000), The National Arbitration Forum and the World Intellectual Property Organization. The Asian Domain Name Dispute Resolution Centre (ADNDRC) was recently established on 28 February 2002 to provide domain name dispute resolution services through its offices in Beijing and Hong Kong (ICANN, 2002b).

[4] The act of web page owners using the names of well-known people or companies in their website addresses.

were not appealed despite the availability of a judicial remedy. The UDRP has become a substitute for traditional infringement or cyber-squatting litigation in most cases (Sharrock, 2001). The establishment of the ADNDRC (Asian Domain Name Dispute Resolution Centre) offices in Beijing and Hong Kong is a positive sign of further international efforts in resolving trademark dispute issues and for achieving a consistent Internet environment. Although the attempts to trample cyber-squatting and bad-faith trademark usage are still subject to criticisms of inconsistency, bias and flaws, this global initiative exemplifies the kind of international effort that could be mounted for managing and regulating other segments of the global information system, in particular Internet content. It is envisaged that achieving an internationally consistent set of rules to efficiently and impartially meet the needs of all Internet users may take a long time because of political, religious, cultural and artistic diversity. Regulating transborder flow of information is indeed a novel and substantial challenge for national regulatory authorities. However, the fact that rules do not already exist does not render an outcome impossible. Managing such information flow requires governments to move from national enforcement to more cooperative engagement with jurisdictional authorities and players in the global information network with international consultation, negotiation and rulemaking. International dialogue about objectionable content has just begun and is relatively rudimentary. Though this effort is underway, we still have to rely heavily on self-regulation (with the Internet service provider), and ethical conscience for a healthy environment. For example, though the US court ruled that Yahoo! is not subject to the jurisdiction of the French law that prohibits the sale of Nazi memorabilia, Yahoo! decided to block the sale of such items on its site on ethical grounds (Murphy, 2001).

CONCLUSION

If cyberspace were free of negative externalities and misdemeanours, the stance of the techno-libertarian might triumph in all debates on Internet regulation and might even now be enforced in our cyberspace. However, reality does not permit the Internet to be regulation free because of the subjective utility value of information to individuals, human weaknesses (such as greed, selfishness and addiction) and incapable filter technology. In addition, traditional forms of regulation (legislation) are not sufficient to prevent undesirable elements in the Internet environment. Regulating cyberspace constitutes a formidable challenge to government and policy makers. A delicate balance needs to be struck between too much and too little regulation. Too much regulation will stifle the positive potential of the Internet (such as e-commerce and economic growth) and too little regulation will give rise to negative externalities and misdemeanours in cyberspace. Although legislative attempts have been made to deter the occurrence of the negative elements, they face difficulties because the Internet is a borderless medium whereas laws are not. Therefore, there is a need for international efforts or forms of institution to regulate the Internet with consistency. If the World Trade Organisation could take a stand in trading relationships between nations, as could the United Nations in world development issues, a similar international organisation for the Internet should not be an impossible feat. However, establishing such an international body will take time. Meanwhile, we have to rely heavily on self-regulation and co-regulation because traditional forms of regulation and filtering technology are not yet fully capable of ensuring a safe and secure Internet environment. We look forward to the day that our children can grow up and learn in a healthy Internet environment.

REFERENCES

ABS. (2001) *Internet Activity 8153.0*, Australian Bureau of Statistics, March Quarter to December Quarter.

AFP. (2001) Aussie to Stop Net Hijacking, *The Age*, 13 February 2001, URL http://www.theage.com.au/frontpage/2001/02/13/FFXPFWHG4JC.html, Accessed 13 February 2001

Anderson, R. H., Bikson, T.K., Law, S. A., Mitchell, B. M., Kedzie, C., Keltner, B., Panis, C., Pliskin, J. and Srinagesh, P. (1995) Universal Access to E-Mail: Feasibility and Societal Implications, RAND, Calif.

Attewell, P. and Rule, J. (1984) Computing and Organizations: what we know and what we don't know, Communications of the ACM, 27(12) December, 1884-1192.

Beijingscene. (1999) Net Rumours, URL http://www.beijingscene.com/V05I008/inshort/inshort.htm, Accessed 8 May 2002

Chrystal, K. A. and Lipsey, R. G. (1997) *Economics for Business and Management*, Oxford University Press, New York.

Cook, B. (1999) Paradoxically Speaking: Increased IT Spending and the Lack of Productivity Improvements, *Inform*, 13(5) May, Spring, 40.

Croucher, J. S. (2001a) Number Crunch, *Good Weekend*, 2 June, 11.

Croucher, J. S. (2001b) Number Crunch, *Good Weekend*, 30 June, 13.

Davern, M. J. & Kauffman, R. J. (2000) Discovering Potential and Realizing Value from Information Technology Investments, *Journal of Management Information Systems*, 16(4), Spring, 121-143.

Eatwell, J., Milgate, M. & Newman, P. (1991) *The New Palgrave*: *A Dictionary of Economics*, MacMillan Press Limited, UK.

Finkelhor, D., Mitchell, K. & Wolak, J. (2001) Highlights of the Youth Internet Safety Survey, *Office of Juvenile Justice & Delinquency Prevention*: *Fact Sheet*, No. 4 March.

Flanagin, A. J. and Metzger, M. J. (2000) Perceptions of Internet Information Credibility, *Journalism and Mass Communication Quarterly*, 77(3) Autumn, 515-540.

Fraumeni, B. M. (2001) E-commerce: Measurement and measurement issues, *The American Economic Review*, 91(2) May, 318-322.

Gilder, G. (1995) Telecosm: Angst and Awe on the Internet. Forbes, December 4, 112-132.

Hillebrand, M. (1999) ICANN Follows WIPO lead on Cyber-Squatting Cases, *E-Commerce Times*, 28 December 1999, URL http://www.ecommercetimes.com/perl/story/2094.html, Accessed 28 August 2001

ICANN. (2001) Internet Corporation for Assigned Names and Numbers (ICANN): ICANN fact sheet, URL http://www.icann.org/general/fact-sheet.htm, Accessed 10 May 2002

ICANN. (2002a) Internet Corporation for Assigned Names and Numbers (ICANN): Rules for Uniform Domain Name Dispute Resolution Policy, URL http://www.icann.org/dndr/udrp/uniform-rules.htm, Accessed 13 May 2002

ICANN. (2002b) Internet Corporation for Assigned Names and Numbers (ICANN): Approved providers for uniform domain-name dispute-resolution policy, URL http://www.icann.org/udrp/approved-providers.htm, Accessed 13 May 2002

Johanson, S. (2001) Email Hoax Warning, *The Age*, 31 May 2001, URL http://www.theage.com.au/news/national/2001/05/31/FFXTCPREDNC.html, Accessed 31 may 2002

Kibirige, H. M. & DePalo, L. (2000) The Internet as a Source of Academic Research Information: Findings of Two Pilot Studies, *Information Technology and Libraries*, 19(1) March, 11-16.

Lemley, M. A. & McGowan, D. (1998) Legal Implications of Network Economic Effects, *California Law Review*, May, 479-611.

Litan, R. E. & Rivlin, A. M. (2001) Projecting the Economic Impact of the Internet, *The American Economic Review*, 91(2) May, 313-317.

Livingston, B. (2002) You Can Stop Spam, *InfoWorld*, 24(15) April, 22.

Mandel, M. J. & Hof, R. D. (2001) Rethinking the Internet, *Business Week*, 26 March, 117-141.

Morris, L. (2000) Direct-to-Lou: Phase II Begins, *Pharmaceutical Executive*, 20(9) September, 162.

Murphy, K. (2001) Yahoo Court Decision on Nazi Auctions Sets Net Precedent, *Network Briefing Daily*, 9 November, 5.

Netdictionary. (2002) Netdictionary, URL http://www.netdictionary.com/html/u.html, Accessed 8 May 2002

NOIE. (2001) *The Current State of Play June 2001*, The National Office for the Information Economy, Canberra.

NOIE. (2002a) *Australia's Information Economy*: *The Big Picture*. Publication prepared by The Allen Consulting Group and The Centre of Policy Studies, Monash University for the National Office for the Information Economy (NOIE), April.

NOIE. (2002b) National Office for the Information Economy (NOIE)'s Media Release: Federal Government Moves to Reduce 'SPAM', URL http://www.noie.gov.au/publication/media_releases/2002/Feb2002/Alston_SPAM.htm, Accessed 8 May 2002

NOIE. (2002c) National Office for the Information Economy (NOIE)'s Media release: Keeping Spam in the Can. URL http://www.noie.gov.au/publication/media_releases/2002/April2002/SPAM.htm, Accessed 8 May 2002

Nowland, D. (2000). Cybersquatter Changes his Name to Oxford University, *The Sydney Morning Herald*, 22 March 2000, URL http://www.akme.btinternet .co.uk/docseg11.html, Accessed on 28/8/01.

NSI Registrar. (2000) NSI Registrar.com, URL http://www.nsiregistrar.com/, Accessed 10 May 2002

Parker, R. P. & Grove, C. B. (2000) Census Bureau Moves Ahead on Measuring E-Business, *Business Economics*, 35(3) July, 63-65.

Pew Internet Life Report. (2000) Wired Workers: Who They Are, What They Are Doing Online, 3 September, URL http:// www.pewinternet.org/, Accessed 22 June

Randall, A. (1983) The Problem of Market Failure, *National Resources Journal*, January, 23, 131-148.

Sharrock, L. M. (2001) The Future of Domain Name Dispute Resolution: Crafting Practical International Legal Solutions from with the UDRP Framework, *Duke Law Journal*, 51(2) November, 817-850.

Silvester, J. (2001) Burglary Uncovers Man's Cache of Child Pornography, *The Age*, 6 June, URL http://www.theage.com.au/news/state/2001/06/06/FFXX27ZJKNC.html, Accessed 6 June 2001

Stanton, J. M. (2002) Company Profile of the Frequent Internet User, *Communications of the Association for Computing Machinery*, 45(1) January, 55-59.

Taylor J. B. & Frost, L. (2000) *Microeconomics*. John Wiley & Sons Australia, Brisbane.

The Age. (2000) Man Jailed for E-mailing False Share Information. The Age, 30 October 2000, URL http: www.theage.com.au/frontpage/20001030/A16239-2000Oct30.html, Accessed 30 October 2000

The Alliance for Childhood. (2000) Fool's Gold: A Critical Look at Computers in Childhood, URL http://www.allianceforchild…projects/computers/computers_reports.html, Accessed 24 August 2001

The Electric New Paper. (2002a) Hotmail Glitch Spotted in Malaysia, *The Electric New Paper*, 3 April 2002, URL http://newpaper.asia1.com.sg/news/npwo329.html, Accessed 4 April 2002

The Electric New Paper. (2002b) Police Nab Teen for Sending Mass E-mail, *The Electric New Paper*, 25 March 2002, URL http://newspaper.asia1.com.sg/news/npwo121.html, Accessed 8 May 2002

The Straits Times. (2001) One in Two Teens 'Tricked' into Porn Websites, 22 February 2001, URL http://straitstimes.asia1.com.sg/primenews/story/0,1870, 25106,00.html, Accessed 22 February 2001

Tomazin, F. (2001) Internet Fraud Man Sentenced, *The Age*, 23 May 2001, URL http://www.theage.com.au/news/state/2001/05/23/FFXZBE0BINC.html, Accessed 23 May 2001

Touton, L. (2000) ICANN, New TLDS, and the UDRP, *ICANN Presentations*: *Boalt Hall Speaker Series*. Berkeley, California, URL http://www.icann.org/presentations/, Accessed 10 May 2002

United Nations. (2001) *E-commerce and Development*: *Trends and Executive Summary*, United Nations, New York & Geneva

Walther, J.B. & Reid, L.D (2000). Understanding the Allure of the Internet, *Chronicle of Higher Education*, 4b(22) 4 February, B4-B5.

Wellman, B. and Gulia, M. (1999) "Net Surfers Don't Ride Alone: Virtual Communities as Communities" in Wellman, Barry (ed.), *Networks in the Global Village*, Westview Press, Boulder, CO, 331-367.

Wollenberg, Y. C. (2001) Don't Rely on Web Filters to Screen the Sleaze, *Medical Economics*, 78(7) April, 14.

Woodall, P. (2000) Survey: The New Economy: Virtual Guesswork, *The Economist*, 356(8189) September, 17.

COPYRIGHT