IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITP4756

In the Virtual World

Michelle W. L. Fong
Victoria University of Technology
School of Applied Economics
PO Box 14428
Melbourne City
MC 8001 Australia
Phone: 61-3-96884507
Fax: 61-3-96884888
email: Michelle.Fong@vu.edu.au

INTRODUCTION

Internet Users and Their Activities

An increasing number of Internet users have been using the Internet's powerful link and searching capabilities to conduct activities that were once envisaged as only feasible through the traditional communications means (such as telephone and postal system) or at the physical locations. The key technical factors driving this embracement of the Internet in our daily life has been technological innovation and improvement such as open architecture, share source code, user-friendly interfaces, and rapidly declining costs of information technology (Braga 1996, Wallis Report 1996). In Australia, although both the household and business segments have been experiencing an increasing rate of Internet technology adoption, household subscribers constitute the majority of Internet subscribers (88 percent), accounting for 58 percent of the data downloaded from the Internet in the March quarter of 2002, as compared to business and government subscribers (ABS 2002). Sixty-four percent of the households in Australia have access to a computer at home, in which 52 percent of these households have home Internet access (NOIE 2002b). In regard to the household's Internet adoption rate, it has been reported by the Australian Bureau of Statistics (ABS 2001) that the annual growth in home Internet access has been exceeding growth in home computer ownership (with and without Internet facility) over the past years. Comparatively, a greater proportion of children (50 percent) used computers at home than adults (26 percent). Children under 14 years access the Internet at home mainly for school homework or educational activities (83 percent), followed by corresponding with friends or visiting chat rooms (51 percent), and browsing for leisure and playing games (40 percent). Adults' Internet activities have been considered more wide-ranging than children's (NOIE 2001, ABS 2000a). Besides using the Internet for emailing messages and visiting chat rooms (68 percent), general browsing (57 percent), and work related purposes (36 percent), the adults also use it for slower growth activities such as online bill payment and fund transfer (13 percent), and online shopping (7 percent). A survey conducted on ten countries[1] (one of which is Australia) by the International Commissions Research found that 74 percent of current and future Internet users ranked personal use as the reason for accessing the Internet over business use (MC Marketing Intelligence 2000). This survey corroborates the aforementioned findings that the Internet has extended into our daily life and home environment.

Figure 1 is a simple illustration of the types of online activities undertaken by the Internet users (adult and children). Transactions involving the maintenance of basic livelihood such as online shopping, utilities payment, teleworking are classified as 'Basics' activities. 'Communication/Socialisation' activities cover communications such as email corresponding and chat room visiting, whereas 'Recreation/Entertainment' includes activities that are hobby-related or for relaxation such as online playing or downloading of games or music files from the websites. Activities related to learning or self-development such as research for school assignment or personal quest for knowledge, are categorized under 'Education/Self-development'. The 'Voice' category, on the other hand, covers activities that involved the Internet as the channel for expressing one's rights or beliefs, or demonstrating for a cause. Activities are not mutually exclusive as some of these activities can be classified into more than one category, such as researching for a holiday destination and finding out more about the country's culture before making a decision for the holiday plan. Such an activity can be considered as having both education and recreation values. Therefore, the circles representing the different activity categories overlap with one another.

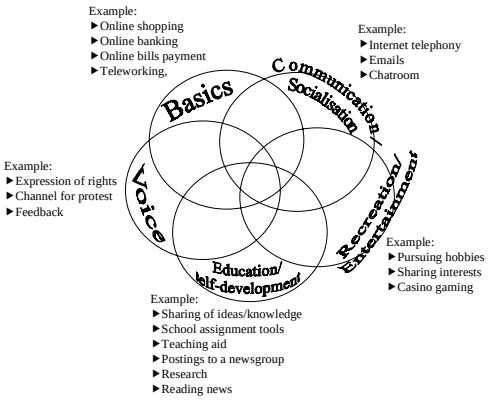
Because the Internet is increasingly playing a pervasive role in our daily lives, there has been extensive discussion on whether the Internet is harming economic life and social relationship. The Internet's rapid pace of evolution has resulted in the need for government and policy makers to address its impact on society and to take into account the externalities[2] generated by Internet users 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, NOIE 2002b). This paper identifies the positive potential of the Internet and the negative externalities created by some Internet users as a result of their actions. In addition, the Australian regulatory framework, as well as its legislative insufficiency, is highlighted.

THE IMPACT OF CYBER ACTIVITIES

Internet as an Education and Research Tool

The information posted in cyberspace makes education, reference work and research easier for researchers and students. In the field of

Figure 1 – Types of Online Activities



research, the global nature of the Internet enables researchers to participate in international collaborative research projects, seek out the work of others, and communicate and share information with colleagues or other researchers in the same field of interest. In distance-learning education, the Internet means that time and space are no longer inhibiting factors in the online learning environment of a busy executive or the underprivileged children from the Third World countries. A good web-based design can bring about interactive, individualized learning environment or help overcome the shortage of educators in the remote regions. Alexander (2001) highlighted that Internet-enabled learning for classroom and distance learning education can improve the quality of learning, the access to education and training, and the cost-effectiveness of education, as well as reduce the costs of education. The U21 global Internet-based university project led by the University of Melbourne (in partnership with an international publishing organization and about 20 other universities around the world) aims to achieve these positive attributes. The project is envisaged to be 25 percent cheaper in tuition fee than that of the traditional university's on-campus education for students (Gottliebsen 2001). Because the U21 e-university is opened to qualified students from any part of the world, these students will enjoy a savings of about 60 percent of the total cost of an overseas on-campus education (including overseas travel and accommodation).

Children Accessing Internet at Home

Although an increasing number of students are using the Internet as a research tool in classroom and at home for their school assignments, information in cyberspace is neither classified nor censored by a unified regulating entity. The non-proprietary network or open Internet access allows people to have quick access to any kind of information in 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). It was found that such information is perceived to be as credible as that found in magazines, radio and television (Flanagin and Metzger 2000). As Internet users grow more reliant on the Internet for news and information, there is the danger that they might be misinformed because some of the information contributed to cyberspace lacked fairness, completeness, balance and accuracy. Misleading information may bring about costly psychological and financial damage, particularly to young children. The Australia Bureau of Statistics 1998 survey on final year primary school and junior secondary school students revealed that about 85 percent of these students acquired the skill of using the Internet at home rather than at school (ABS 2000b). This suggests that children spend more time using the computer and accessing the Internet at home. The survey further identifies that younger children use computers at home more often than older children. The concern for underage youngsters and teenagers accessing the website unsupervised at home is because of objectionable contents in cyberspace. 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 has been 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 illicit websites unintentionally (The Straits Times 2001).

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 in its co-regulatory approach 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. The Content Code mandates Internet service providers to take reasonable measures to prevent children from accessing prohibited content, including making approved filtering technology available to the subscribers and informing parents of procedures concerning supervising and controlling children's access to Internet content. However, the legislative frameworks are not capable of completely shielding children from such information and websites. In particular, they lack juridical authority on prohibited content hosted overseas. Although it is hoped that sophisticated technology will one day afford comprehensive protection for children using the Internet, the advent of technology can also dampen efforts. 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 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. Furthermore, the concern that naïve and inexperienced children might fall prey to exploitation on the Internet, such as communicating with strangers who harbor malicious intent, has added impetus to the need for parental supervision. The Internet age certainly requires parents to supervise their children's Internet activities (self-regulation) in the home.

Cyber Activist

Prior to 1990s, the issue of Internet regulation attracted fewer concerns than today. At that time, the insignificant impact of the Internet and the number of Internet users did not warrant the need for government intervention or regulation. Gradually and over the years, the nonproprietary architecture of networks and open technology standards gave rise to the expansion of cyberspace and the increase in the number of Internet users. Along with these, the various types of information contributed or exchanged in cyberspace have also increased. As Internet users tend to behave or act in a manner that produces optimal satisfaction only for themselves and disregard or may not be aware of the possible widespread benefits or costs that their actions may bring to the community as a whole (Eatwell et al., 1991), information contributed by them may be beneficial to themselves but may be harmful to society. Negative externalities and misconduct (such as hate speech and blasphemy) committed on the pretext of free speech in cyberspace have brought on intervention from government and policymakers, undermining the openness and democracy in cyberspace. There have been cases where the Internet users committed hacker attacks on websites for the purpose of demonstration or vengeance, or for fun, curiosity or profit. Predictive Systems, a consulting firm that specializes in network security, has reported twelve million hacking efforts between September and December 2001 in cyberspace (Predictive Systems 2002).

The Internet has become a powerful tool for staging online disturbances and for serving as the voice of the protestors. For example, anti-globalisation was shifted into cyberspace when the World Bank decided to host its annual conference online to avoid disruption from activists at the physical venue in Barcelona in 2001. However, activist groups retaliated with the warning that they will hack into the conference site and shut it down by bombarding it with emails (known as 'denial-of-service' attacks), generating disruption equivalent to that of their mass

street demonstrations in previous years (Riley 2001). In another case, a different activist group undertook a similar plot on the White House's official website several times to protest against US President George Bush's refusal to ratify the Kyoto protocol on climate change. Because cyberspace collapses spatial differences and provides a veil of anonymity to the activists, organizations such as NASA, the United States Department of Defence, and the White House find their official website under constant hacker attacks, waged by activists from different regions (Barker 2001). Cyberspace can also be turned into a battlefield by hostile hackers such as the hackers' war between the US and China over the US spy plane incident in April 2001 (Lever 2001). In about one week of the hackers' war, at least one thousand websites in each of these countries were defaced.

Prior to the enactment of the Cybercrime legislation in Australia, it seems that hacking as a form of protest is acceptable if a hacker abides by a code of hacker etiquette, which allows the defacing of a web page but leaving data on the servers unaltered. However, hackers who specifically target and damage infrastructure such as using viruses to destroy and wipe out a server's operating system, were said to have broken the code of hacker etiquette because such damage was considered irreversible or costly. The Code Red and Nimda viruses spread by hackers were know to have caused US$4 billion in downtime and equipment damages worldwide in 2001 (The Electric New Paper 2001). On the other hand, the 'Love Bug' virus inflicted an exorbitant global cost of A$25 billion or US$13 billion in 2000 (Taylor 2001). These viruses are usually spread through email attachments and through vulnerable Internet information servers. Accessing infected Internet site can also infect the computers of unsuspecting Internet users, who may not be the intended target. Presently, there are about 50,000 computer viruses in existence, with ten new viruses being created each day (Croucher 2002). This rate of virus proliferation means that software technology is an insufficient measure to combat against deliberate act of virus spreading. The 2002 Australian Computer Crime and Security Survey report (AusCERT et al. 2002) revealed that although 99 percent of the companies surveyed use anti-virus software, viruses infected 76 per cent of these companies. As a result, forty-three percent of these companies suffered financial losses. The Australian Computer Emergency Response Team (Australia's computer watchdog) has recorded an increase of virus and hacker attacks by four times between 1999 and 2000 (Johanson 2001). Because hacking and virus attacks can inflict economic damage, undermine consumer confidence and threaten national security, the Australian Government enacted the Cybercrime Act in December 2001 which outlawed hacking, denial of service attacks, spreading computer viruses and website vandalism. Despite this legislation, there have been concerns that crime investigators such as the Australian Federal Police and National Crime Authority are not equipped with advent technologies and expertise to effectively combat cybercrime (Taylor 2001)

Workplace 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 (Forfa 2002, NOIE 2002a, Mandel and Hof 2001, DePrince Jr. and Ford 1999). 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, legal entanglement, viruses and leaks of confidential information to competitors, companies have began to monitor staff activities on the Internet. Such process did raise discussion on the issue of the invasion of staff privacy at the workplace. In December 2000, the Australian Government introduced a 'light touch' privacy legislation that allows companies to access staff emails and browsing logs under certain circumstances, based on the National Privacy Principles for Fair Handling of Personal Information (The Office of the Federal Privacy Commissioner 2000). The 'light touch' approach is intended to give companies greater flexibility in determining what they consider to be appropriate usage of their email and Internet systems; and also to reduce compliance cost burden for business due to differing privacy regimes between States and Territory. Compared to the US, a higher proportion of companies in Australia (75 percent as compared to 57 percent in the US) monitor employee emails and Internet use (Zimmerman 2002, Croucher 2001b).

The communication support provided by the Internet is enormous and we are becoming increasingly reliant on emails as a communications mechanism. While an increasing percentage of email exchanges are taking place on company time, the continuing expansion of Internet usage means that companies need to take steps to manage their Internet traffic and establish or enforce Internet usage policies already in place. Computers and internal networks are company assets; management has a responsibility for issuing clear instructions and enforcing policies as to the proper use of such property. The Australian Privacy Commissioner encourages companies to involve their staff in the development of privacy policy on the proper and permitted use of email and Internet systems in order to maintain morale and productivity in the workplace (The Office of the Federal Privacy Commissioner 2000).

CONCLUSION: THE NEED FOR UNIFIED REGULATORY EFFORT

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 measures. 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. Online activities that are socially acceptable, tolerated or even legal in one locale may not be so in another, as each country differs in its unique social and political milieu. 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.

Regulating transborder flow of information is indeed a novel and substantial challenge for national regulatory authorities. 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. History has shown that bilateral dialogues and cooperative efforts can lead to effective international cooperation. Some of the Australian government agencies have taken steps to work with partner country agencies in combating negative externalities and misdemeanors. For example, international dialogue about objectionable content has just begun and is relatively rudimentary. Though such efforts are underway, we have to rely heavily on self-regulation and co-regulation because traditional forms of regulation and filtering technology are not yet fully extended or developed to ensure a safe and reliable Internet environment.

ENDNOTES

1. Argentina, Australia, Brazil, Canada, Great Britain, Hong Kong, Italy, Japan, Sweden and the United States.
2. Externality is a cost or benefit arising from a transaction or activity that spillover to a third party and is not taken into account by those who undertake the transaction or activity.

REFERENCE

References will be provided on request.