NETWORK NEWS

The Internet and the State: Instrument of Social Control or Subversive Tecnology?

Chris Atchison, University of Toronto
Jim Thomas, Northern Illinois University

The dramatic and continuing expansion of computer technology in the past decade has expanded public access to computer-mediated Internet communication such as email and the World Wide Web (WWW). The proliferation of Internet newsgroups, discussion lists, and personal homepages has further increased participation in public and private electronic interaction. As a consequence, the potential for creating, disseminating, and archiving information combines to potentially enhance the democratization of society. Yet, in an ironic twist, the same technological forces that contribute to democratization may also increase the power of the state to monitor citizens and control the so-called 'Information Highway.'

Some observers optimistically view the expansion especially of the Internet as a way to level social and political inequality. Other observers are less sanguine, seeing the technology as potentially dangerous to civil liberties, especially privacy. In this essay, we begin exploring the question of whether computer-mediated communication is a potential tool of oppressive state control or whether it instead subverts unnecessary state power and enhances democratization.

THE DEMOCRATIZATION POTENTIAL

Some critics suggest that the 'computer revolution' is available to and benefits only an elite few, subverting any possibility for democratization. However, in North America the availability of computers and Internet access in homes, schools, and libraries allows most people who choose to go online the means to do so. The Internet contributes to the democratization of society in several fundamental ways, and no single factor has primacy over the others. A few examples will illustrate the diversity and complexity of how, in the aggregate, the new technology provides a means of social and individual empowerment.

The Communication Revolution

The ability to communicate freely with whom one chooses without imposed constraints of status, fear of reprisal, or asymmetrical power games is essential to the democratic process (Habermas 1972, 1984). The Internet brings several tools by which people can easily communicate with each other, share ideas, and obtain or disseminate information. First, the most popular tool, electronic mail (e-mail), offers a means of inexpensive and near instantaneous contact with others around the world. Fears of reduced email privacy neglect the fact that e-mail is no less secure than its postal counterpart, and communicants who fear interception of their messages can use encryption software to virtually assure the security of the message.

Second, discussion groups such as Usenet or listservers bring people together across ideological, geographical, or cultural boundaries. Usenet is a system of world-wide public discussion groups consisting of electronic messages relayed between posters (people who send a message to a group) interested in discussions, political organizing, or simply chatting. With over 100,000 different Usenet topics ranging from the most banal to extremes of political action or graphic sexual content, posters can communicate openly or anonymously. The international character of Usenet makes it difficult for governments or groups to suppress ideas without also banning computer communications entirely. Unlike Usenet, which has no central authority responsible for controlling or maintaining discussions, listserves are smaller electronic discussion groups managed by an individual (or 'list owner') and that originate from a specific computer system. Lists may be public or private, and the number of participants can range from two to tens of thousands. This provides a forum for discussion of topics ranging from sexual bestiality and bondage to the doctrinal disputes between leftists and the diatribes of right-wing militia advocates.

A third means of communication, Internet Relay Chat (IRC), allows users to engage in synchronous, or real time, conversation by using software that allows them to 'log on' to a 'place' where others are discussing topics of mutual interest. IRC also allows users to initiate their own private topics for discussion, thus preventing unwanted eavesdroppers. This form of communication is especially useful for those engaging in illicit group activities because it can be done anonymously and, unlike email or discussion groups, leaves no record of the participants or the content of their discussions.

The fourth and perhaps the most important contribution of the Internet for enhancing communication is the WWW. The Web is a method of exchanging text files or pictures across the Net by placing them in a given location, called a homepage, that can be accessed by others. Because there are few restrictions on who can create a homepage, the Web offers everybody the potential to be a publisher. With over 50 million homepages estimated to be on the web in late 1999, millions of people and organizations are taking advantage of the ability to write and make available opposing views, products, photographs, or even video segments. As a consequence, homepage publishers can provide a resource base for their users on any conceivable topic, even those that depart from propriety or legality. For example, right-wing militia groups, organizations espousing terrorism or child pornographers can organize and provide resources for sympathizers as easily as can politicians, governments, or educators.

How Does This Lead To Democratization?

The expanded communicative power made possible by the Net does not, in and of itself, assure more egalitarian power arrangements within a nation or culture, between nations, or among people. It does, however, offer the potential for subverting abuses of power in several ways. First, the Net offers a voice to all groups or individuals, including those with unpopular minority views. People who may otherwise have felt isolated because of their sexual preferences, political ideology, or esoteric interests, can easily find an outlet in newsgroups or on homepages.

Although the Net does not fully remove all of the interactional problems associated with real-life status, such as sex and racial identity (Herring 1993, 1996), Net communication does tend to reduce most status differences, while race, gender, class and other status stigmata are less obvious, and therefore less intrusive, in online communication. This feature is a special advantage to those who feel silenced in face-to-face communication.

Third, the Net partially dissolves geographical boundaries that might allow a government to suppress expression or publication of some ideas. For example, it has become common on the Net for system administrators to mirror (or duplicate) on their own computer systems material that puts original distributors at risk in a more repressive own country. Chinese students illustrated the utility of e-mail when they used it to circumvent government censorship during the Chinese Tiananmen Square crackdown in June, 1989.

Fourth, the Net allows resistance to abuses of government power, such as those that occur through over-zealous prosecutions or repressive legislation. For example, in an attempted federal prosecution of a young college student in 1990 for electronically 'stealing' proprietary documents from BellSouth Corporation, organized Net opposition to the case revealed that the documents, alleged by the government to be worth over $79,000, were publicly available by mail from the BellSouth for under $13 (Sterling 1992). In another example, passage by the U.S. Congress of the Communications Decency Act (CDA) in 1995 led to resistance that began as online organizing and later escalated into conventional legal battles. Because of the online organizing, the CDA was overturned by the U.S. Supreme Court in 1997 (Godwin 1998). A watered-down resurrection of the law in 1998, referred to as 'CDA II' (47 USC Sect 231(a)(1)), was immediately challenged by the same online coalition that defeated the first one, illustrating the rapidity by which groups can organize against state actions.

Fifth, the Net provides a means to counter conventional news media spin by providing an antidote to conventional news accounts. In one of the first examples of a successful Net attack on a major news medium, Time magazine was forced to acknowledge the flaws in a cover story that demonized 'Net pornography' (Godwin 1998). A less noble example can be found in Internet reporter Matt Drudge's lowering of journalistic standards of conventional media with his online 'Drudge Reports' of the salacious details of Monica Lewinsky's relationship with President Bill Clinton.

These are just a few of the examples of the empowering potential of the net. Ironically, however, the empowering capacity of the Internet also brings a darker, more repressive side. Not every democratization influence is equally distributed within or across populations, and these influences are mediated or subverted by countervailing factors. Burstein and Kline (1995) offer 'road warrior' imagery in reminding us that the Internet is still in its infancy. Political, economic and ideological battles will continue to be fought over control, content, and accessibility. We next identify several features of Internet expansion that possess a potential anti-democratic effect.

Informal Censorship Restricting Access

Critics of the Net (Stoll 1995) are less optimistic about its social value. Some remind us that, while it is easy to become caught up in the hysteria surrounding the unprecedented growth of the Internet with its 100 million users, we must remember that there are still several billion people who are not on-line. The most basic and yet pervasive way in which world governments control content and communications on the Internet is by restricting access. In most cases, in many of the less economically prosperous nations this control is not difficult, because most citizens of these countries do not even have a telephone (Human Rights Watch 1996; Salbu 1998). In countries such as China, Singapore, Saudi Arabia, Vietnam, India and North Korea only those individuals of high status and close ties to the State are even permitted access to the Internet. Even these more trusted citizens are often required by law to register with the state and their on-line conduct and communications may still be monitored by state agents.

THREATS AND PROMISES

An increasingly popular method of informal censorship used by the State and its agents has been the use of subtle and not so subtle threats and intimidation. Most often individuals and/or Internet service providers are warned by state officials that certain services, links, or communications are either a violation of the law or are not approved of by the State. These warnings create a chilling effect that is effective system of self-censorship. This type of control is preferred by many of the Asian and Middle Eastern Governments.

Formal Attempts To Censor:
Legislated Censorship

Various world governments have utilized legislation as a means of expanding their jurisdiction into cyberspace to enable them to prosecute residents and non-residents for what they deem to be offensive or harmful on-line activity. French rules of civil procedure give the French courts jurisdiction over cases involving actions or communications originating from or entering into French soil by its citizens at home or abroad (Sdallian 1996). A similar system exists in Britain (Cohen 1998). The blurring of international boarders and citizenship created by the newly formed European Union may create an interesting legal scenario for Internet users who possess a European Union passport.

In the most widely publicized North American attempt to obtain control of Internet content, the United States Congress passed the Communications Decency Act in June 1995. The wording of the Act set the standard of indecency, never unambiguous in the best of circumstances, to the broadest definition by restricting Net content to the most stringent community standard in the country. Although two years later the Act was ruled unconstitutional by the United States Supreme Court, this attempted legislation clearly indicated the United States government's intent to directly control Internet conduct and communications.

Technological Initiatives And ISP Liability

Another popular method proposed and/or utilized by governments such as Singapore, Australia, Vietnam and China is the legally mandated use of special screening software to restrict what can be seen or said by its citizens (Rodan 1998). Such measures do not affect just the criminal element they also prevent legitimate users from accessing or distributing information that, while not deemed illegal or offensive, gets caught within the web of censored material due to slight overlaps in ideas or wording. For example, when popular filtering systems are programmed to prohibit access to sexually explicit pictures it often becomes impossible to access pages or newsgroups dealing with AIDS awareness or sex education materials. In one ironic example, Special Prosecutor Kenneth Starr's report to the U.S. Congress of grand jury transcripts summarizing juror testimony before the special çouncil was banned in China and other countries, and was blocked by filtering software on many U.S. ISPs.

One means by which various governments such as Canada, the United States, France, Germany and Australia have decided to control the content of the Internet and on-line communications has been to make Internet service providers (ISPs) responsible for ensuring that users do not encounter illegal or offensive material. Two distinct approaches have been taken to accomplish this responsibility. The first and least successful approach has been to enact legislation that makes the ISP legally responsible for the illegal or offensive conduct of its customers. This method has been employed with little success in France (Sdallian 1996) and is currently subject to public debate in Australia (Electronic Frontiers Australia 1998a; Alston 1998; DCA 1997).

A second, successful approach has been to enlist the co-operation of ISPs in setting up systems of self-regulation whereby ISPs essentially enforce non-legislative guidelines or codes of conduct for their subscribers. These guidelines are based upon mutually agreed upon industry standards and the suggestions of various law enforcement agencies. The genius of this approach is that the State does not run the risk of losing control over the individual. Instead, the ISP becomes an unofficial agent of the State, allowing the state and its official agents of control to bypass legislative restrictions on their power to investigate and prosecute. In a recent and highly publicized example of this potential, a United States Federal court ruled that evidence volunteered to the Federal Bureau of Investigations by America Online (AOL) was not subject to restrictions of the Fourth Amendment because AOL is considered a private party under the law (Gilligan and Imwinkelried 1998; United States v *Maxwell* 1996).

Database Collection: Big Brother Is Watching

Many critics of Net expansion remind us that we must not view some of the apparent failures by the State to legislate direct control over actions and communications on the Internet with too much complacency. Because oppressive potential also rests below the surface where State agents have at their disposal data collection, storage and analysis devices that allow them to easily monitor and target individuals or groups that they define as deviant or threatening. Many analysts tend to forget that the Internet was originally created by the United States Government and military, and there is little reason to believe that government agencies in the more economically and technologically affluent nations do not possess the resources to monitor on-line communications and activities within their own domain.

Holding The Master Key: Encryption And Key Escrow/Key Recovery

Recent technological developments in conjunction with government and business-imposed restrictions on anonymity create a dangerous environment for Internet users, providing further reason to question how free we are to speak and act in the online world. One of the most effective means available for the State to control the actions and communications of private citizens is to prevent anonymous action or communication. For several years, the United States government has tried, unsuccessfully, to introduce a voluntary encryption standard known as the Clipper Chip that would allow state policing agents to decrypt any and all encrypted electronic files, email messages, or data packets. They have also proposed that a third party monitored key registry, referred to as key escrow or key recovery, be set up to house duplicate copies of all private encryption keys used in the United States (Jones 1997). The key registry approach has recently been adapted by the French government (Lawmoney 1998) and both the British and Canadian governments are currently considering implementing similar programs (Global Internet Liberty Campaign 1998; Department of Industry Canada 1998a, 1998b; Department of Trade and Industry United Kingdom 1997). The lone exception to the overwhelming tendency towards State control of individual anonymity on the Internet can be found in the Australian government's approach to encryption. Australia has taken the position that it is not in the best interests of the citizen or the state to prevent the free use of encryption software by individuals (Electronic Frontiers Australia 1998b).

CONCLUSION

Technological progress always contains within it the ironic dialectic of liberation and domination. The computer-based information highway is no exception. As a consequence, our own view is that the computer revolution contains the potential for both over-control and subversion of control. Science and technology are not neutral. They are social constructs that exist only within a context of choices of development and application. Therefore, it is not the technology that constrains, or oppresses, or liberates. Rather, the emancipatory potential of this new technology lies in the degree to which those who use it can disseminate it and maintain it as a relatively low-cost communication tool. To date, many of those involved in expanding the Internet frontier have generally been suspicious of and resistant to government intrusion into the Net. While it is often easier to simply dismiss such suspicion as the ranting of conspiracy theorists, history has taught us that such a naïve faith in the benevolence of the government is unwise. Our intention here has not been to provide a definitive conclusion about the past, present, or future state of technological progress; instead we hope that our discussion will spark further critical analysis of technology and related topics.

REFERENCES

Attorney General of the Commonwealth of Australia. 1997. *Discussion Paper Copyright Reform and the Digital Agenda: Proposed Transmission Right, Right of Making Available and Enforcement Measures.* Web posted July 1997 [http://www.law.gov.au/publications/digital.htm]

Alston, R. 1998. *Regulation of Internet Content Media Release.* The Minister for Communications, the Information Economy, and the Arts Deputy Leader of the Government in the Senate. Web posted January 23, 1998 [http://www.dca.gov.au/nsapi-graphics/?MIval=3Ddca_dispdoc&ID=3D212]

Borland, J. 1998. 'Court Orders ISPs To Identify Subscribers,' *TechWeb,* Friday, July 10

Burstein, Daniel and David Kline. 1995. *Road Warriors: Dreams and Nightmares along the Information Highway.* Harmondsworth: Penguin

Cohen, S. 1998. 'Jurisdiction Over Cross Border Internet Infringements,' *European Intellectual Property Review.* August 20 (8): 294-297

Department of Communications, Information Technology, and the Arts, Australia (DCA). 1997 *Principles for a Regulatory Framework for On-line Services in the Broadcasting Services Act 1992.* Web posted September 13, 1997 [http://www.dca.gov.au/nsapitext/ ?MIval=3Ddca_dispdoc&pathid=3D%2fpolicy%2=fframework%2ehtml]

Department of Industry, Canada. 1998a. *Setting A Cryptography Policy Framework for Electronic Commerce: Building Canada=92s Information Economy and Society.* Notice No. IPPB-003-98 Release of Public Discussion Paper on Setting a Cryptography. Web posted February 18, 1998. [http://strategis.ic.gc.ca/SSG/cy00002e html]

Department of Industry, Canada 1998b. *Background: Public Discussion Paper on Setting A Cryptography Policy Framework for Canada*. Web posted February 23, 1998 [http://strategis.ic.gc.ca/SSG/cy00004e.html]

Department of Trade and Industry. 1997. *Paper on Regulatory Intent Concerning Use if Encryption on Public Networks*. Web posted February 26, 1997 [http://www.dti.gov.uk/CII/ENCRYPT/regpap1.htm]

Electronic Frontiers Australia. 1998a. *Submission to Senate Select Committee on Information Technologies Self-Regulation in the Information and Communications Industries Inquiry*. Web posted January 1998 [http://www.efa.org.au/Publish/sscit.html]

Electronic Frontiers Australia. 1998b *The Walsh Report*. Web posted January 1998 [http://www.efa.org.au/Issues/Crypto/Walsh/]

Glasser, P. 1998. 'Sparklers on Your Digital Sundae,' *North American Review*. March/April: 39

Gilligan, F.A. and E. J. Imwinkelried. 1998. 'Cyberspace: The Newest Challenge for Traditional Legal Doctrine,' *Rutgers Computer and Technology Law Journal*. 24 (2): 305-343

Global Internet Liberty Campaign. 1998. *Reproduction of Department of Trade and Industries: Secure Electronic Commerce Statement*. Web posted April 27, 1998 [http://www.gilc.org/gilc/crypto/uk/dti-statement-498.html]

Godwin, Mike. 1998. *Cyber Rights: Defending Free Speech in the Digital Age*. New York: Times Books

Habermas, Jurgen. 1972. 'Toward a Theory of Communicative Competence,' Pp. 115-148 in H. P. Dreitzel (ed.), *Recent Sociology*. No. 2: Patterns of Communicative Behavior. New York: Macmillan

Habermas, Jurgen. 1984. *The Theory of Communicative Action, Volume I: Reason and the Rationalization of Society*. Boston: Beacon Press

Herring, Susan. 1993. 'Gender and democracy in computer-mediated communication,' *Electronic Journal of Communication*. 3 (2). Special issue on Computer-Mediated Communication, ed. by T. Benson. Available from comserve@rpitsvm.bitnet

Human Rights Watch. 1996. *Silencing the Net – The Threat to Freedom of Expression Online*. Human Rights Watch. Web posted May 1996 [gopher://gopher.igc.apc.org:2998/0HRW/r.904402921.11394.1]. May 1996, Vol. 8, No. 2 (G)

Jones, C. 1997. 'Oddball archivist aims to save the Net,' *Now*. Thursday, February 13

Jones, D. 1997. 'Can you keep a secret?' *The Convergence*. August 02

Lawmoney. 1998. 'France Updates Encryption Regime,' *Lawmoney News*, Euromoney Publications PLC [http://lawmoney.oyster.co.uk/public/news/hotnews/news9803/news980324.1.htm=1]. March 24, 1998

Rodan, G. 1998. 'The Internet and Political Control in Singapore,' *Political Science Quarterly*. 113 (1): 63-89

Salbu, S. 1998. 'Who Should Govern the Internet?: Monitoring and Supporting a New Frontier,' *Harvard Journal of Law and Technology*. 11 (2) Winter: 429-480

Sterling, Bruce. 1992. *The Hacker Crackdown: Law and Disorder on the Electronic Frontier*. New York: Bantam Books

Stoll, Cliff. 1995. *Silicon Snake Oil*. New York: Doubleday

Sdallian, V. 1996. 'Controlling illegal content over the Internet: the French situation,' Paper presented during the debate *Censoring the Internet: a lawyer's deceit of the Media Law Committee*, 26th International Bar Association Conference, Berlin, 23 October 1996. Available on-line at [http://www.argia.fr/lij/control.html] 1996

United States v. *Maxwell*. 1996. 45 M.J. 406 C.A.A.F.