Controlling and Enhancing the Information Society in the United States

J.A.N. LEE
IEEE Computer Society
janlee17@verizon.net

"The advent of the computer...has changed the way we do business, the way we live, the way we educate our children, and a myriad other things we do on a regular basis. So far, US Internet governmental policies have been targeted toward economic development, not toward societal impact. Efforts to create legal approaches limiting what have been determined by a minority to be the less appropriate uses of the Internet have not been wholly successful."

Key words: USA, CDA, Communications Decency, COPA, protection of Children, COPPA, regulation.

INTRODUCTION

The Internet has been a self-developing, self-directed, self-governed entity, even though in many ways it developed from a collection of networks that had more organized origins. Crossing international boundaries, individual countries have their own approaches to the control of the usage of the Internet primarily influenced by indigenous cultural beliefs and expectations. The interrelationships between Internet users and their governments is also significant, principally relying on the understanding of the responsibilities of the government to provide an environment which is in the best interests of its citizens. This is not simply a difference between a benevolent, representative governance system and a totalitarian government system, but is instead a function of the acceptance of who knows best what

is best for individuals. Is it a totally utilitarian governance system or one that has respect for minority opinions and the dignity of the individual? This paper reports on the legal aspects and potential legal approaches to the governance of the Internet but concentrates on the cultural expectations of governance within one country – the United States of America.

IMPACT

Of any country in the world, the USA has probably been impacted by computing and advanced communications technologies to a greater extent, through the intrusion of those technologies into almost every aspect of the daily lives of its citizens. The computer and the computer industry found a receptive niche in a society that has always been open to new ways of doing business. Prosperity has also been kind to the USA, thereby permitting a larger proportion of the population to indulge in adding gadgets to the home and the office, mostly in the name of time-saving capabilities but often for the mere thrill of adopting novelty. The analogy of the Information Superhighway is an appropriate metaphor when one reflects that the USA has been the host to a number of revolutions that included the integration of the automobile into the American way of life. The problems arising today, in response to the demand to control the Internet, show parallels to the problems of controlling automobiles on the early, primitive roads. The primary purpose of the "rules of the road" is to create an environment in which users can more easily get from place to place with due respect to those others who have similar goals. Over the years, as automobiles have been imbued with greater capabilities, these rules have been amended to include regulations protecting users against their own indiscretions. It is rare, for example, that the failure to use a seat belt has a deleterious impact on others involved in an accident. Speeding can be dangerous to the public, but regulations on maximum speeds also seek to limit drivers to a range within the capabilities and skills of the average driver. Automobiles can be used, as can much advanced technology, for nefarious purposes, just as the telephone can be used for purposes beyond the original intentions of Alexander Bell. Just as the Polaroid camera and the camcorder provided the means to forward the proliferation of objectionable images without the potential intervention of commercial photo-developers, so the Internet can be used in ways that are not always acceptable to everyone who uses it. Yet in what manner will we be ready to accept "rules of the road" for the Internet, and to whom will we ascribe the right to make those rules?

The advent of the computer and advanced communications has changed the way we do business, the way we live, the way we educate our children,

and a myriad other things we do on a regular basis. So far, US Internet governmental policies have been targeted toward economic development, not toward societal impact. Efforts to create legal approaches limiting what have been determined by a minority to be the less appropriate uses of the Internet have not been wholly successful.

Throughout the 1990s, and primarily during the administration of President Clinton and led by Vice-President Gore, numerous attempts were made to introduce legislation to regulate the impact of the content of Internet while at the same time ensuring access to information technology for all citizens.

GUIDELINES

Recall that the name of this country is the United *STATES* of America, and that differences exist between Federal and State policies, regulations, and activities. Each state is responsible for those elements of government that impact their own citizens and for which there is no need for Federal oversight. Thus the Federal government is primarily responsible for those things that deal with Inter-State commerce, social programs, and foreign relationships. Consequently, many statutes and policies reside in the domain of the locality rather than the federal government. For example, the definition of obscenity is local, based on a 1973 Supreme Court decision on the appeal of a case involving the conviction of an appellant accused of mailing unsolicited sexually explicit material in violation of a California statute. The Supreme Court provided the following "basic guidelines for the trier of fact":

(a) whether ...the average person, applying contemporary *community* standards... would find that the work, taken as a whole, appeals to the prurient interest,

(b) whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable *state* law, and

(c) whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value. If a *state* obscenity law is thus limited, First Amendment values are adequately protected by ultimate independent appellate review of constitutional claims when necessary. [1] [Emphasis added.]

REGULATING THE INTERNET

The Communications Decency Act was enacted by the U.S. Congress in February 1996; it basically attempted to regulate the access to "inappropriate" materials by young people. The Act stated that (slightly paraphrased):

"Whoever in interstate or foreign communications knowingly--

(1) (A) uses an interactive computer service to send to a specific person or persons under 18 years of age, or

B) uses any interactive computer service to display in a manner available to a person under 18 years of age, any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs, regardless of whether the user of such service placed the call or initiated the communication; or

(2) knowingly permits any telecommunications facility under such person's control to be used for an activity prohibited by paragraph (1) with the intent that it be used for such activity, shall be fined ..., or imprisoned not more than two years, or both."

Initially, a special three-judge court in Philadelphia, Pennsylvania ruled on June 12, 1996 that the Communications Decency Act was an unconstitutional abridgement of rights protected by the First and Fifth Amendments to the US Constitution. The Department of Justice immediately filed an appeal with the US Supreme Court, which heard oral arguments in the case on March 19, 1997. In a landmark decision issued on June 26,1997, the US Supreme Court held that the Communications Decency Act violated the US Constitution First Amendment guarantee of freedom of speech. The Court's opinion, written by Justice John Paul Stevens, claimed that the Act comprised a censorship of the on-line medium. Commentators lauded this decision as establishing the fundamental principles that would guide any judicial consideration of the Internet for the 21st Century. A major portion of the arguments against the Act involved the proposed use of "blockers" in schools and libraries, and by Internet Service Providers that blocked more than the prescribed offensive material. Many legitimate medical advice sites were blocked as well as sites related to sex education.

In 1998, Congress introduced the Child On-Line Protection Act (COPA), which was a "Restriction of Access by Minors to Materials Commercially Distributed by Means of World Wide Web that are Harmful to Minors":

(a) Requirement To Restrict Access.--

(1) Prohibited conduct.--Whoever knowingly and with knowledge of the character of the material, in interstate or foreign commerce by means of the World Wide Web, makes any communication for commercial purposes that is available to any minor and that includes any material that is harmful to minors shall be fined not more than $50,000, imprisoned not more than 6 months, or both.

Very quickly this new law was challenged, and a temporary restraining order was filed to prevent the US Justice Department from enforcing it. The U.S. Supreme Court reversed the earlier US appeals court ruling which found the 1998 Child Online Protection Act (COPA) too broad in scope in May 2002. In an 8-1 vote, the justices ruled that the appeals court could not bar enforcement of the law on the basis that it relied on community standards to identify harmful material.

To reinstate many of the concepts within the Computer Decency Act, the Children's Internet Protection Act (CIPA) was signed into law by President Clinton in December, 2000. This law required public libraries receiving certain federal funds to: (1) adopt Internet safety policies; and (2) use mandatory filtering software to block Internet access for children and adults to materials that are obscene, contain child pornography or were deemed to be harmful to minors. The Act required that schools and libraries that receive federal funding verify that they had both "Technology Protection Measures" and an "Internet Safety Policy" in place. The Technology Protection Measure required that blockers or filters be installed to prevent access to visual depictions on the Internet that were considered to be obscene, to child pornography, or to other sexual content that is claimed to be harmful to minors. The law required that the Internet Safety Policy similarly must address access by minors to inappropriate material, and, in common with COPA, ensure the safety and security of minors when using email or other forms of electronic communication. By linking these requirements to federal funding, the Congress attempted to circumvent previous criticisms that it was not in the purview of the Federal government to regulate private institutions. However, there are very few schools or public libraries that do not receive some form of federal funding!

The American Civil Liberties Union and the American Library Association both challenged the constitutionality of CIPA and in May 2002, a three-judge panel in Philadelphia, Pennsylvania, held that CIPA is unconstitutional because the mandated use of blocking technology on all computers will result in blocked access to substantial amounts of constitutionally protected speech. The Court found that filters both overblock (block access to protected speech) and underblock (allow access to illegal or unconstitutional speech). At the same time the Court enjoined

the government from withholding funds from public libraries that chose not to install blocking technology on all their Internet-ready terminals.

In June 2002, the U.S. House of Representatives voted by an overwhelming margin to pass the Child Obscenity and Pornography Protection Act of 2002 (COPPA). The bill, sought to criminalize the production, dissemination, or possession of computer-generated, or computer images that are, or are virtually indistinguishable from, child pornography. Civil liberty groups immediately warned that this new bill contained similar flaws to the Child Pornography Prevention Act (CPPA), a bill banning obscene images that "appear" to be of minors, which was declared unconstitutional by the United States Supreme Court in April 2002. COPPA criminalized as child pornography any image as long as it is, or is indistinguishable from, child pornography. This would include images in which adults were used and made to look like minors. COPPA also prohibits selling or receiving materials that are, or are advertised as, child pornography. Furthermore, in Section 5 of HR 4623, it criminalizes anyone who knowingly produces, distributes, receives, or possesses a visual depiction that is, or is indistinguishable from, a pre-pubescent child engaging in sexually explicit conduct, including drawings, cartoons, sculptures, and paintings. Several persons have been successfully prosecuted for contravening the provisions of this bill.

PRIVACY

Not to be deterred by the striking down of the CDA, the US Congress responded with the passage of the "Children's On-Line Protection Act" to control one aspect of Internet usage – the solicitation of children for immoral purposes through persons who attempt to pass themselves off as friends of children. The Children's Online Privacy Protect Act (COPPA), passed on October 23, 1998 [2], and described as "Regulating Unfair and Deceptive Acts and Practices in Connection with the Collection and Use of Personal Information From and About Children on the Internet", prescribed that (slightly paraphrased):

> (1) In General.-- It is unlawful for an operator of a website or online service directed to children, or any operator that has actual knowledge that it is collecting personal information from a child, to collect personal information from a child in a manner that violates the regulations prescribed [elsewhere].
>
> (2) ... Notwithstanding paragraph (1), neither an operator of such a website or online service nor the operator's agent shall be held to be liable under any Federal or State law for any disclosure made in good

faith and following reasonable procedures in responding to a request for disclosure of personal information ... to the parent of a child.

The Protection of Citizens' Privacy on Federal Web Sites Act [3] was passed in December 2000, primarily requiring the reporting of the collection of personal data, not the prohibition of any collection activity:

... the Inspector General of each [Federal] department or agency shall submit to Congress a report that discloses any activity of the applicable department or agency relating to --

(1) the collection or review of singular data, or the creation of aggregate lists that include personally identifiable information, about individuals who access any Internet site of the department or agency; and

(2) entering into agreements with third parties, including other government agencies, to collect, review, or obtain aggregate lists or singular data containing personally identifiable information relating to any individual's access or viewing habits for governmental and non-governmental Internet sites.

THE DIGITAL DIVIDE

There have been concerns about the accessibility of electronic information by two major communities – the socially disadvantaged and those with disabilities. On August 7, 1998, President Clinton signed into law the Rehabilitation Act Amendments of 1998 (originally passed in 1973.), which covered access to federally funded programs and services. The law required access to electronic and information technology provided by the Federal government, and required Federal agencies to ensure that this technology was accessible to employees and members of the public with disabilities to the extent it did not pose an "undue burden." It does not apply to web pages of private industry. Interestingly enough, it was not until 2001 that the White house upgraded its own site to conform to this requirement. In September 05, 2001 the Bush Administration unveiled its accessibility-improved web site, www.whitehouse.gov. The White House had come under a barrage of criticism from the disability community for deficiencies in its web site's accessibility features. The White House's web site is now accessible to people with disabilities, especially blind, visually impaired, hearing-impaired and deaf individuals, and includes a Spanish language section, multi-media components, and an area designed specifically for children (www.whitehousekids.gov). For blind and visually impaired individuals the web site is programmed so a voice synthesizer can read aloud the contents, including online forms and photo captions. For the hearing-impaired, videos of presidential events will be captioned, and efforts are underway to encode previous video with captioning.

The Digital Divide Elimination Act of 2001 [4] was introduced into the U.S. House of Representatives in July 2001. The bill would provide tax incentives to working families wanting to purchase a computer and increase the charitable deduction for technology donations.

PRESIDENTIAL EXECUTIVE ORDERS

Since the President has direct management responsibilities for the Federal government departments, he can direct that certain procedures be followed without the need for Congressional legislative actions. Two of these involve the activities of Federal departments in use of Information Technology to improve society (December 1999) [5] and the need to protect "Critical Infrastructure" (October 16, 2001) [6], both signed by President Clinton.
In using IT to improve society, Clinton suggested that studies should be undertaken to:

1. promote expanded access to higher quality, cost-effective health care to underserved rural communities and inner city clinics;
2. make "school report cards" available on the Internet;
3. to remove legal and regulatory barriers to high-quality distance learning, to increase awareness of the availability of distance learning as an alternative means of
4. education and training, and to find ways to promote the earning of
5. credentials through distance learning;
6. determine how telecommuting might be used to help more disabled Americans get jobs and to provide jobs for Americans located in geographic regions outside traditional commuting areas;
7. encourage the private sector to make web content, software, standards consistent with the Web Accessibility Initiative;
8. develop a national strategy for promoting environmental applications of information technology (such as disseminating information about manufacturing techniques that reduce pollution, and increasing the timeliness of environmental information).
9. identify services that can be delivered electronically to rural Americans and develop the policies needed to promote;
10. encourage more effective use of information technology by nonprofit organizations.

The Executive Order regarding the protection of critical infrastructure created a national policy that stated (in part): It is the policy of the United States to protect against disruption of the operation of information systems for critical infrastructure and thereby help to protect the people, economy, essential human and government services, and national security of the United States, and to ensure that any disruptions that occur are infrequent, of

minimal duration, and manageable, and cause the least damage possible. The implementation of this policy shall include a voluntary public-private partnership, involving corporate and non-governmental organizations.

FEDERALLY FUNDED RESEARCH

> *Throughout the history of computing, even going as far back as the work of Charles Babbage, governmental funding has had a significant impact on the computing field. While some of this work has benefited the military establishment, there has always been significant fallout in the non-governmental fields. The funding of ARPANet, and NSFNet led to the Internet, and new funding is now developing the next generation, logically named "Internet2".* [7]

Internet2 is a consortium led by 200 universities, working in partnership with industry and government, to develop and deploy advanced network applications and technologies, accelerating the creation of tomorrow's Internet. Internet2 is recreating the partnership among academia, industry and government that fostered today's Internet in its infancy. The primary goals of Internet2 are to:

1. Create a leading edge network capability for the national research community
2. Enable revolutionary Internet applications
3. Ensure the rapid transfer of new network services and applications to the broader Internet community.

The Federal government is playing a critical role in both support of some key technology development projects through the National Research Foundation, as well as direct collaboration with university and industry researchers investigating next generation internet technologies and infrastructures. In parallel, the Federal government has its own advanced Internet initiative, called the Next Generation Internet (NGI) initiative. The Next Generation Internet (NGI) initiative is a multi-agency Federal research and development program that is developing advanced networking technologies, developing revolutionary applications that require advanced networking, and demonstrating these capabilities on test-beds that are 100 to 1,000 times faster, end-to-end, than today's Internet. The key distinction between the NGI initiative and Internet2, however, is that NGI is led by and focuses on the needs of the Federal mission agencies, including NASA, National Institutes for Health and others.

THE US CULTURE

Beyond these special aspects of any attempt to control the Internet, the culture of the USA promotes policies that primarily favor non-governmental development of control mechanisms and the support of self-discipline through appropriate organizations. Thus it is appropriate that The Internet Corporation for Assigned Names and Numbers (ICANN) and the Internet Society (ISOC) have taken on those responsibilities that in many other countries are under governmental control.

That is not to suggest that there are not oversight opportunities within the US government, with concerns to provide the best services to the general public. The primary goals are to provide:

- Economic development through collaborative projects
- Encourage competition
- Support standards
- Get out of the way and let private enterprise do its job
- Maintain American expectations of their "way of life"
- Self-regulation rather than governmental regulation
- Independent development rather than governmental development

Within these joint governmental/free enterprise collaborations there must be concern for the risks and dangers of abridging the Constitutional Rights of people with respect to:

- Freedom of Speech (and expression);
- Privacy;
- Censorship, while at the same time looking to concerns for the protection of Children; and
- the disadvantaged, maintaining throughout consideration for impartiality and equality.

There have been significant changes in the Executive Branch attitudes towards the control of the Internet since the change of administration in 2001. Whereas the Clinton administration had a large staff in the White House Office of Telecommunications, and the Vice-President actively promoted activities to enhance information technology, the Bush White House has minimized the staffing of the Office of Telecommunications, and there is no one who is taken over the role of Al Gore.

OVERVIEW

The Internet and the content carried therein should not be treated any differently than other communications media, just in the same way that we should not treat electronic expressions any different from printed matter. In

summary we can suggest that within the US community, the overarching concerns in general are to:

- Instigate rather than create;
- Support rather than control;
- Promote rather than patronize;
- Promote competition rather than to monopolize;
- Provide diversity rather than insist on commonality; and
- Let the market find its niche.

REFERENCES:

1. US Supreme Court, MILLER v. CALIFORNIA, 413 U.S. 15 (1973), APPEAL FROM THE APPELLATE DEPARTMENT, SUPERIOR COURT OF CALIFORNIA, COUNTY OF ORANGE , No. 70-73, Argued January 18-19, 1972, Reargued November 7, 1972, Decided June 21, 1973.
2. Children's Online Privacy Protection Act of 1998, http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/children105_277.doc
3. Section 646, Protection of Citizens' Privacy on Federal Web Sites, Treasury and General Government Appropriations Act, 2001 (P.L. 106-554, DECEMBER 21, 2000), http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/section646.doc
4. The Digital Divide Elimination Act of 2001,HR 2281, statement read on the floor of the U.S. House of Representatives by Rep. Jefferson on July 2, 2001, http://www.digitaldividenetwork.org/content/stories/index.cfm?key=155
5. Use of Information Technology to Improve Our Society, THE WHITE HOUSE, Office of the Press Secretary, December 17, 1999, http://www.gsa.gov/attachments/GSA_PUBLICATIONS/extpub/31.pdf
6. Critical Infrastructure Protection in the Information Age, Executive Order 13231, THE WHITE HOUSE, Office of the Press Secretary, October 16, 2001, http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=2001_register&docid=01-26509-filed
7. About Internet2®, http://www.internet2.edu/html/about.html