CENSORSHIP AND THE INTERNET

Introduction

By any measure, the Internet has grown and is growing by leaps and bounds (1). With this growth has come the recognition that the Internet is indeed a powerful medium—powerful because it can do much good in education, commerce, and general social development. Conversely, it also has the power to do much harm.

Such power has not gone unnoticed by governments. Around the world today there is an increasing awareness of the need to regulate the Internet, both to promote good and to minimize harm. It is a delicate balance because the conventional wisdom, as yet unproven, is that overregulating the Internet stifles information flow, a result that can damage the economic and social well-being of a country.

This article looks at such controls, and seeks to explain the rationale and limitations of censorship.

Definition of Censorship: Part of the Rubric of Content Regulation

Censorship is easier to spot than to define. (Not that it is always easy to spot.) Sometimes what may appear as censorship has legitimate backing in law. For example, the European Union (2) recently listed the following as reasons for restricting information that is “potentially harmful or illegal contents or can be misused as a vehicle for criminal activities.”

- National security (instructions on bomb making, illegal drug production, terrorist activities)
- Protection of minors (abusive forms of marketing, violence, pornography)
- Protection of human dignity (incitement to racial hatred or racial discrimination)
- Economic security (fraud, instructions on pirating credit cards)
- Information security (malicious Hacking)
- Protection of privacy (unauthorized communication of personal data, electronic harassment)
- Protecting of reputation (libel, unlawful comparative advertising)
- Intellectual property (unauthorized distribution of copyrighted works—e.g., software or music)

This list includes restricting information that violates privacy, reputation, and intellectual property rights. By most reckoning, such restrictions should not be considered censorship, but it is not easy to craft a definition that would skirt them.

Applied to traditional print and broadcast media, censorship may be defined as the removal or deletion of forbidden material. As will be shown below, it is not always possible with the Internet to remove material. Instead, the most frequently used method is to block or filter access. A working definition of censorship on the Internet would therefore be the intervention by a third party between the free exchange of a
willing sender and a willing receiver of information. Typically, both sender and receiver do not want the intervention.

The working definition would exclude such acts as editing, which seeks to improve the meaning and clarity of the message. The definition may or may not include gatekeeping functions, such as which messages should appear and in what order. In those instances, it is not always clear if it is censorship in the sense of intervention with the primary intent of blocking the transmission and reception of the information, or that what appears as censorship has valid reasons behind the act.

For example, files with pornographic images are large and so system administrators may refuse to carry them not because of the images but because of the memory resources consumed. Although such decisions may have a benign intent, some users see them as censorship, with the negative connotations.

**Problems of Internet Censorship**

Censorship even of traditional media is difficult; it is never 100 percent effective 100 percent of the time. Censors know this and so their intent is not to be wholly effective, just to make the material inaccessible for most people. With the Internet, however, the difficulties of achieving even that aim are compounded.

The root of the problem for censors is that the Internet combines characteristics of the newspaper, telephone, radio, television, and computer. Each of these inventions alone has contributed to an increase in the transmission and reception of information. By combining them, the Internet offers an explosion of information for censors.

The Internet can narrowcast instead of broadcast messages, a phenomenon known as demassification. It converges technology so that censoring one part of the Internet could censor parts that even the censors may not want censored. It arose from a free, almost anarchic computer culture in which regulation was minimal to nonexistent. Finally, the Internet has global reach, so community standards in censorship become questioned.

**INFORMATION EXPLOSION**

The Internet’s ability to store and transmit information means that more information can be gathered and distributed at a faster pace; that is, the flow of information in circulation increases at an exponential rate, which creates a lot of work for censors.

Take the example of Singapore, which bills itself as a wired island. Over a fifteen-year period (from 1978 to 1993), the amount of material the censors had to vet increased fivefold from about 5,500 in 1978 to more than 25,000 in 1993 (3). By default, censorship has become more selective.

**NARROWCASTING**

The reach of the Internet ranges the spectrum from one to one (E-mail) to one to many (Web sites) and many to many (Usenet groups). No technology before has had
CENSORSHIP AND THE INTERNET

such a reach. Censors are most comfortable working on mass as opposed to specialized or private communication media. It is familiar terrain. At the very least, it is more efficient to censor the mass media.

On the Internet, the boundary between mass and private or customized communication is blurred. Usenet groups and Web sites, for example, are open to anyone who cares to click to them. They look like a mass medium but are intended to cater to a specialized audience. In fact, the irritation with advertisements on Usenet groups is not because of advertising per se but because the ads are often off-topic and irrelevant to the discussion of the group.

On the other hand, E-mail is generally seen as a private mode of communication, even though it is possible to conduct mass mailings and even though some discussion groups are conducted through such mailings. In short, E-mail, a private communication medium, has the potential to be a mass medium.

Theoretically there is no reason that E-mail cannot be read and censored. It just takes a lot of work. Opening and reading E-mail, however, may well be the most effective means of turning users away and killing the growth of the Internet. In 1994, through a misunderstanding of a high-level official request, Internet accounts of an access provider in Singapore were scanned for .GIF files. Of 80,000 files scanned, five were found pornographic by Singapore standards and the users were warned. Although no non-GIF file was opened, users nevertheless were irate. Many expressed grave reservations about security and privacy on the system. In the end, the access provider had to assure its users that no such scanning will occur in the future (3).

Ironically, reading and censoring messages may expose an Internet access provider to more liability than not reading and censoring. In the U.S. case of Straton Oakmont v. Prodigy Services Co. (4), the online service provider Prodigy was held to be liable because by reading each message before it was posted, it had exercised editorial control.

PARADIGM

By combining the traits of traditional communication media, the Internet poses problems for censorship because it becomes difficult to classify it and to decide who regulates the various traits and how. This is the problem of the regulatory paradigm.

Should the Internet be treated as a postal service because it has E-mail? Then again, don’t the capabilities of Internet relay chat and voice telephony make it a telecommunication service? Then does the presence of electronic newspapers make it a print medium, or should the availability of radio and television stations make it a broadcast medium? Should its use of the computer mean that the computing model of regulations apply? Can the advertising model—in which advertisements are often screened before they are placed in the media—be used for censorship?

For censorship purposes, the postal/telecommunications, computing, and advertising approaches may be rejected. The postal and telecommunication paradigm may be rejected because most if not all countries do not monitor all or even a large part of such exchanges; it would be too expensive for any country.

Next, the computing paradigm may be rejected because—besides notable exceptions such as Myanmar’s recently imposed law against unauthorized use of networked
computers (5)—most countries impose minimal regulations on computers. Until recently censors saw computers as yet another manufactured product—just hardware.

The advertising model may be ideal for censors, as most countries have a regulatory scheme to prevent fraudulent or misleading advertising. Even in the United States, in which advertising is deregulated, the response of a television or radio station to complaints about advertising is a factor that is considered in the renewal of the broadcasting licence (6).

There are, however, two problems with using the advertising model. First, contents on the Internet cannot be analogous to advertisements. There is no one to screen all postings, and no one, not even the Internet access provider, would want the responsibility of vetting all contents.

That leaves two possible approaches: print and broadcast. In all countries there is some experience of content regulation with one or both media. The difference may not be trivial. At the time of writing, Germany was debating whether the Internet is a print medium and therefore to be regulated at the state level, or a broadcast medium to be regulated at the federal level (H. Berkes, personal communication, 1996).

For practical purposes, perhaps because the Internet is seen as a modern electronic medium, many countries have placed the Internet under the regulators of the broadcast industry. In the execution of regulation, however, the functions of the Internet may be broken up so that parts of the Internet are regulated under different approaches, as will be shown below.

COMPUTER CULTURE

Another problem in Internet censorship is that the computer culture celebrates maximum (and sometimes anarchistic) freedom, not censorship. The culture may be traced to its origins. The Internet was designed to function as a communication channel even after a nuclear attack (7, 8). Censorship is read by the Internet as "damage" and the system will attempt to correct it. Dynamic rerouting ensures that if one communication link is broken, traffic can be redirected through other existing links.

The very structure of the Internet militates against censorship. As an "organization," the Internet has no central controlling body, just a voluntary council that sets technical standards. There is no one to whom a complaint about objectionable material may be made. It is therefore inherently resistant to censorship in both its operating philosophy and technical setup.

No matter how system administrators at individual sites may restrict access to objectionable materials, savvy users can overcome the hurdles. In a case in Canada, a couple was charged with the gruesome murder of a girl, Karla Homolka. The judge ordered a complete press ban on the trial. In the face of such a judicial ban, two Canadian university students created a newsgroup alt.fun.karla-homolka to post information and rumors about the case. Canadian universities later removed the newsgroup, but other users created alt.pub-ban.homolka to serve the same function as the banned group.

In the worst case, users may pay to access restricted materials directly from overseas Internet service providers.
GLOBAL INTERCONNECTIVITY

The Internet highlights a major legal issue in global interconnectivity: which censorship standard applies? The issue extends beyond the classic “what is pornography” debate as highlighted in a U.S. case in which a bulletin board service (BBS) operator in California was convicted of delivering pornography to a resident in Tennessee (9).

The Internet offers a myriad of material on subjects such as drug culture, bomb making, murder, and anti-Semitism. Material that is illegal in one country and punishable with a heavy sentence may be legal many other parts of the world.

Germany’s case of the neo-Nazi frames the problem best. In January 1996, German phone company Deutsche Telekom blocked users of its computer network from accessing the Web site of Ernst Zündel, a German-born activist living in Toronto, Canada, suspected of distributing neo-Nazi and anti-Semitic material over the Internet (10). Given the history of Germany, such a response is perhaps understandable.

Elsewhere anti-Semitic speech does not have such a grave history as in Germany. In fact, in the United States, when Germany blocked access, several prestigious universities offered to mirror Zündel’s site (11). Similarly, when Germany tried to block access to a magazine called Radikal, forty-seven other sites all over the world mirrored the Radikal site (11). Enforcement of the German law is very difficult, if not impossible.

Any attempt at censorship also has to consider the international dimension. In December 1995, again in Germany, CompuServe Inc. blocked worldwide access to sexually explicit material on the Internet after German authorities ordered it to suspend newsgroups with the prefix alt.sex (12). Because it did not have the capability to suspend materials on a country-by-country basis, CompuServe had to use blanket censorship. As a result, 4 million subscribers around the world were affected. Not only was this the first time that CompuServe had suspended access because of content restriction, but it was on a global scale, as well. The suspension was later lifted, with CompuServe promising to explore ways of tailoring access to selective audiences (12). The Internet thus not only throws up the question of what standard of censorship to adopt, but also suggests that local community standards have to be worked out in juxtaposition with global ones.

LEGISLATIVE LAG

Finally, the process of regulation tends to proceed piecemeal and almost always lags behind changes in technology. Censorship of any new medium can only operate when the objectionable material has been sent or the objectionable conduct taken place. Until then, censors would not be aware of the possibility of circumvention or violation. In the interim, before the passage of the law, there is the gray area.
CENSORSHIP AND THE INTERNET

Approaches to Censorship

PASSING LAWS

As regulators understand the Internet better, they have attempted to pass legislation to regulate aspects of its content. Passing Internet-specific laws for censorship is necessary in many countries because the medium is new to regulators; otherwise, in some countries, censors may not have the power to censor. Perhaps because the medium is so new, the laws appear to have been not well thought out.

In the United States, the controversial Communications Decency Act of 1996 had some of its key provisions governing censorship ruled to be unconstitutional (13). A similar fate befell a comparable law in France. In 1996, the French Constitutional Council struck down provisions of a new telecommunications law that empowered the Conseil Supérieur de la Télématique to make recommendations on what types of content were permissible (2). Striking down laws that conflict with freedom of expression does not mean that censorship of the Internet is not legally possible. It does mean, however, that legislators cannot simply rush the laws for policital expedience, and must write them better.

Where the constitution does not recognize such freedom of expression, the law may be used as a direct tool of censorship. For a while in China, Internet users had to register with police (14).

In Singapore, censorship is exercised through a multipronged approach of blocking certain Web sites as well as a scheme that deems most Web sites to be licensed. Other Web sites of religious and political organizations, as well as online newspapers produced locally, have to be registered (14). Although the law appears novel, it was essentially an adaptation of existing media laws in Singapore.

Sometimes the law need not be Internet-specific. In South Korea, security police tracked down users of a Korean version of the Internet who in an online debate expressed opinions about an intruding North Korean submarine that could “benefit the enemy” (15). Earlier, a government official was quoted as saying: “A South Korean who meets by chance a North Korean on Internet had better report to the police within seven days” (16). Such actions are authorized by the National Security Law. According to a civil rights activist, Kim Young Sik, president of the South Korean Civil Union Against Censorship, users have had their access restricted because of comments that were deemed to be in violation of national security laws (17).

The common factor in the various laws appears to be that they are modeled after print or broadcast media laws; that is, the laws do not stand on their own but have been adapted from existing regulations (18).

USING TECHNOLOGY

Laws, however, are blunt instruments for what is essentially a delicate task of picking and choosing content to be removed. Inevitably the very technology that enabled the spread of the information has been used to censor it. The result has been mixed at best.
CENSORSHIP AND THE INTERNET

Probably the first program to censor the Internet was one developed by Richard DePew. Annoyed by anonymous messages on the Usenet groups he read, he developed a program he called ARMM (automated retroactive minimal moderation) to delete them. The program failed at first. Several versions later, when it succeeded, it actually affected the workings of other connected computers (19).

Many Usenet readers disagreed with DePew’s deletions because it deprived them of the messages. Since then, DePew has stopped using ARMM. Instead, he has developed a program called a bincancel-bot, which removes inappropriately placed binary files from Usenet groups. Such binary files tend to be large, usually contain either programs or images, and are often off-topic. This time there was a more muted reaction.

Such a cancelbot was first used against a law firm, Canter and Siegel, who sent off-topic advertisements to more than 1,000 Usenet groups hawking their legal services. A twenty-five-year-old Norwegian programmer, Arnt Gulbrandsen, developed a “cancelbot” that hunted down and deleted messages that were sent by the firm (20).

There is room for abuse, however. In September 1996, a computer user in the United States sent a cancelbot to remove 25,000 messages from the Usenet. According to press reports, the U.S. Federal Bureau of Investigation is looking into the case (21).

In Singapore, Internet access providers have enlisted the help of proxy servers, which are widely used to speed up access, to censor Web sites blacklisted by the regulators, the Singapore Broadcasting Authority. The process of having to look up the blacklist does slow down access a little—In the order of a second or so (22), nevertheless, there are complaints that access seems to take longer. At the time of writing, the Singapore Broadcasting Authority said it had placed a little more than a hundred sites, mostly containing pornography, on its blacklist. Such centralized controls have limited capabilities, because to add to the list is to add to access time, frustrating users.

SELF-REGULATION BY INDUSTRY

Seeing how governments are attempting to regulate the Internet, in some parts of the world the industry has developed a code of conduct. Such codes go beyond acceptable use policies to address objectionable content.

There is a fundamental conflict, however. On the one hand, the industry wants the business to grow. On the other hand, any form of regulation is seen as stifling growth. Not surprisingly, there has been little incentive for Internet access providers to develop such codes. Where industry has developed such codes, it has typically been because of pending legislation. In Europe, the slew of codes has been sparked by the possibility of European Union-wide Internet content laws.

In the United Kingdom, the industry’s code established an independent body, the Safety Net Foundation, to provide a rating service for newsgroups and a hotline to which members of the public can report content they consider illegal. Similar steps have been taken or are being taken in Germany and the Netherlands (2). In France, a code of conduct has similarly been proposed in the Rapport de la Mission Interministérielle sur l’Internet (23).

Codes will require an element of the force of law. Penalties may be imposed on the
violators of the code directly through law or through some self-help mechanism, such as suspending the account of the violator. Self-help mechanisms may require the force of law to empower and protect those who penalize the violators.

SELF-REGULATION BY USERS

Partly because of industry lethargy and partly because codes have wider application, various parties have come together to create filtering software and labeling standards. Filtering software programs are endorsed by industry and governments in Europe, Australia, and the United States.

At the end of 1996, there were more than a dozen such software packages, complete with their own jargon. There are blacklists—which are also known as refusal access lists because they may not be accessed—and whitelists—only those on the list may be accessed. Some of them use algorithms to prevent attempts to circumvent the filtering. For example, in some cases it is not even possible to conduct searches with certain keywords.

Such programs have their limitations, however. Less sophisticated software can create problems. One type of filtering software deletes offensive words without warning the reader that words have been deleted. The meaning in a sentence can be dramatically altered.

Perhaps the biggest limitation is that inherently even the more sophisticated programs require updating. More than twenty industry players, including companies that develop the filtering software, have established a consortium to label Internet content. Called World Wide Web Consortium, they have worked with MIT’s Laboratory for Computer Science to come up with PICS (platform for Internet content selection), which is a labeling convention (24, 25).

In the past, blocking software could not process the labels provided with competing programs. In contrast, PICS establishes standardized label formats, technical specifications, and rating systems so that PICS-compatible programs may read labels from any source. In summary, PICS “is analogous to specifying where on a package a label should appear and in what font it should be printed without specifying what it should say” (26).

In February 1996, the Recreational Software Advisory Council launched an objective, self-rating content-labeling advisory system for the Internet, RSACi, which is compatible with PICS. Contents are labeled by the provider on three categories: violence, nudity/sex, and language. There is a total of five scores from 0 to 4, with each score explicitly defined (27). It is then up to the receiver of the material to set the scale on which materials may be received.

The RSACi approach is unlikely to be widely adopted. Although RSACi views itself as value-neutral, its values are based on those in the United States. Anti-Semitic, racism, and religiously offensive speech, for example, are not rated. As it is a voluntary system, the content providers with more offensive material are unlikely to desire rating. Another reason is that such filtering software is targeted at children and requires active intervention by parents and other adults.

A recent controversy that has emerged is whether or not filtering software programs can be held liable if a site is mislabeled. For example, a site might be labeled as being
CENSORSHIP AND THE INTERNET

pornographic when it is selling lingerie because the programmers decided that the models were too scantily clad (28). As far as is known, there have been no lawsuits filed.

Ironically, users with such software will encounter a more extensive refuse-access or blacklist than users with filters at the servers. Typically a program will block several thousand sites (29).

Issues for Research

Censorship, perhaps better phrased as content regulation, of the Internet is here to stay. The question is the degree and form of the censorship.

Theory would suggest that the more stringent the regulations in a country, the more impeded its development. It is possible to say that the more extreme forms of censorship will hurt the social and economic well-being of a country. In Internet censorship, Singapore and China typically come to the fore, but these countries are among the fastest growing economies in the world. There is no research that conclusively proves Internet censorship hurts.

Will Internet censorship have a spillover effect? For example, the Internet has many resources to offer in education. It may be that censorship will inadvertently affect the availability of resources by shutting off access to certain sites.

A third area is Internet commerce, which is growing fast. It is, however, an area largely unaffected by censorship. Again, is there a possibility of spillover effects so that censorship in one arena affects commerce?

If evidence is presented to show that censorship has negative consequences in these areas, then governments will be willing to relent; otherwise there is little incentive to do so.

Conclusion

A common argument against censorship is that the Internet cannot be reliably blocked because a user can always make an international phone call. That is not the point. It has never been possible to reliably block anything, even at customs. The censors’ point is to make it difficult for most users to access the material. The persistent will always find a way around the censors.

Why governments would want to exercise censorship is a matter of each country’s history and culture. In the classic case, Germany has its memory-searing record of anti-Semitic speech. Singapore had a history of race riots in mid-1960s. South Korea has its tear of the North Korean invasion. In short, acts of censorship that may seem overdone to outsiders cannot and should not be blithely dismissed as mere violations of free speech.

In some ways censorship of the Internet is more severe than censorship of traditional media. Often censorship is through a blocking mechanism, which is prior restraint. Legal doctrine views this as a more severe form of censorship than restriction after publication.
Censorship affects all Internet users. Because the Internet is a global communication and information system, any reduction in that communication anywhere on the globe will hurt others in the link.

Any Internet user can point out the harm and limitations of censorship, but somehow it should be done while respecting the history and culture of each country and node.

REFERENCES

18. P. H. Ang, How Countries Are Regulating Internet Content.
22. M. C. Tong, "Device to Block Out Blacklisted Web Sites." Straits Times (July 20, 1996).
COMPUTER NETWORKS AND THE VIRTUAL COLLEGE

Introduction

While there have been numerous publications discussing the potential of computer networks to revolutionize scientific work, there have been a fairly limited number of empirical studies that attempt to measure the impact of this new technology. What follows is a summary of the existing literature on the effects of computer networks on scientific work and a discussion of the impact that this may have in the field of library and information science. Computer networks, which create a "virtual college" in this context, refer to computer-mediated communication (CMC) via a network (i.e., the Internet). Electronic discourse (E-mail, E-bulletin boards, E-conferencing, E-journals, E-chat), along with accessing computer databases and transferring electronic files, are included under this broad use of the term computer networks.

This article is organized as follows: "Usage Estimates" reports usage of CMC in select disciplines; "Collaboration Patterns" gives details on remote collaboration, international collaboration, and changes in work group organization brought on by CMC; "Frequency of Communication" explains levels of communication intensities facilitated by CMC; "Global Science" introduces the idea of geographic cooperation through shared databases; "Peripheral Effects" discusses changes in status distinctions and access to information due to CMC; "Productivity" introduces the CMC effects on scientific productivity; "Social Contexts" outlines social factors that may impact upon the use of CMC; and finally "Implications for Library and Information Science" summarizes CMC use by and impact upon library and information professionals.

Usage Estimates

Previous research on CMC suggests that the adoption of CMC technology can have a variety of effects on the social structure of work organizations (1, 2). Before we