



**Romel Cabiling** ▾



Home

Home > My courses > Social And Professional Issues > 10 Regulating Internet Content (Cont.) > Lesson Proper for Week 10

# Lesson Proper for Week 10

## Internet Technologies Supporting Free Expression

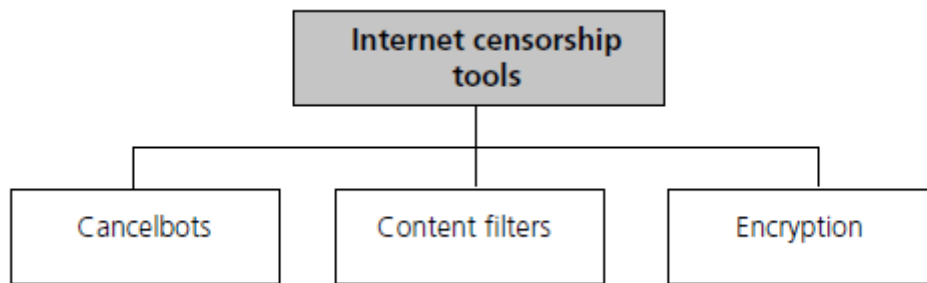
In addition to the foregoing characteristics, specific Internet technologies can enable free expression.

Those Internet technologies that tend to enhance free expression are as follows:

- Electronic mail. The Internet essentially started with electronic mail as its primary communications medium, and has historically fought hard to keep this free from censorship. By its very nature, electronic mail is extremely hard to censor, especially simple, point-to-point mail, because of the distributed and robust nature of routing protocols.
- Newsgroups and UseNet technologies are widespread and difficult to censor.
- Internet chat facilities can also enable free expression, where unregulated, and provide the opportunity for anonymity (though this can have its own drawbacks as we shall see in the following section)
- The Web is a democratic publishing medium where there are few restrictions. Any business, organization or individual can set up a home page on the Web
- Cryptography has protected free expression by allowing people to express their opinions with some degree of confidentiality and privacy. As discussed in Module 3, encryption scrambles messages so that only the legitimate recipient, or intended parties, can understand them.

## Internet Technologies as Tools for Censorship

The three technologies that effectively act as 'censorship tools', are indicated in Figure 5.3 and are briefly discussed below:



**Figure 5.3:** Exemplar tools that may be used to impose degrees of Internet censorship

### Cancelbots

Certain Internet technologies, such as Usenet news, have shown themselves vulnerable to cancellation of previously published information, for example through the use of cancelbots. A cancelbot is a robot program that sends a message to one or more Usenet newsgroups to cancel, or remove from posting, a certain type of message. It searches for messages matching a certain pattern, whether it is a duplicate message or offensive material, and sends out cancels for them. When a message has been cancelled, its status is changed to 'cancel,' and the Usenet servers will no longer post them.

### Encryption

We have seen that encryption technology protects confidentiality and privacy and can thereby enable freedom of expression. However, control of, and access to, the same technology can undermine free speech. Examples are the intercepting of e-mail and other forms of electronic communication by governments and state agencies, and the monitoring of employees in workplaces (this issue will be discussed in greater detail in subsequent chapters). In the mid- 1990s, for example, the US government demanded limits on encryption technology and access to all encrypted messages. The government's efforts took the form of proposals for a 'clipper chip' in 1993, a technology that would have been installed in all electronic communications devices, and which would have required encryption users to submit their encryption keys to a government database. The proposals met with such a hail of objections from technical and civil liberties groups that they were never implemented.

### Content Filters

A web filter is a piece of software that prevents certain web pages from being displayed by a browser. While a browser application is running, the filter runs as a background process, checking every page your browser attempts to load. If the filter determines the page is objectionable, it prevents the browser from displaying it.

Filters can be installed on individual computers, or an ISP may provide filtering services for its customers. Programs designed to be installed on individual computers, such as Cyber Sentinel, eBlaster, and Spector PRO can be set up to e-mail parents as soon as they detect an inappropriate web page. They enable parents to set the level

of filtering on their children's accounts. It also allows parents to look at logs showing the pages their children have visited. Filtering software is also used in libraries, educational institutions and other areas of public Internet use, especially those to which children have access.

Typical filters use two different methods to determine if a page should be blocked. The first method is to check the URL of the page against a blacklist of objectionable sites. If the web page comes from a blacklisted site, it is not displayed. The second method is to look for combinations of letters or words that may indicate a site has objectionable content.

Neither of these methods is foolproof. The Web contains millions of pages containing pornography, and new sites continue to be created at a high rate. Hence any blacklist of pornographic sites will be incomplete by definition. The algorithms used to identify objectionable words and phrases can cause web filters to block out perfectly innocent and legitimate web pages for no apparent reason. For example, the websites of Middlesex, Essex or Sussex universities might be blocked by some web filters simply because they contain the word 'sex', one of the words most commonly entered into search engines!

ISPs can also implement their own restrictions on the content of websites, newsgroups and emails that are hosted on their servers. Some of these content regulations might be self-imposed by the ISP, as specified in their acceptable use policies. Others may be imposed by legal restraints – for example, the case of Yahoo.

### **The case of Yahoo!**

In 2000 a French court ordered Yahoo! to block access by French people to Yahoo!'s USbased auction sites where Nazi memorabilia were sold. Display and sale of Nazi memorabilia is illegal in France and Germany (with some exceptions for historical purposes). The order raised several technical and legal issues, and was widely viewed as a threat to freedom of speech.

- It was technically not feasible to block access by all French people because they could access Yahoo!'s sites from outside France or use anonymizing services that obscured their location. One of the basic characteristics of the Internet is that one's physical location is irrelevant, in terms of access. One's physical location is also difficult to determine.
- The use of filters to screen out Nazi material has the problems we discussed earlier. Yahoo! said filters would be less than 50% effective and could not distinguish references to Nazis in hate material and from references in, for example, *The Diary of Anne Frank* or Holocaust memorials (Baase, 2003).
- Free speech advocates worried that the policy changes demonstrated the power of one government to impose its censorship standards on other countries. Others saw it as adoption of a responsible policy, discouraging the spread of Nazi material.

### **Anonymous Expression: For and Against**

Anonymous communication in cyberspace is enabled largely through the use of anonymous remailers, which strip off the identifying information on an e-mail message and substitute an anonymous code or a random number. By encrypting a message and then routing that message through a series of anonymous re-mailers, a user can assume that their message will remain anonymous and confidential. This process is called 'chained re-mailing'. The process is effective because none of the re-mailers will have the key to read the encrypted message; neither the recipient nor any re-mailers (except the first) in the chain can identify the sender. The recipient cannot connect the sender to the message unless every single re-mailer in the chain cooperates. This would assume that each re-mailer kept a log of their incoming and outgoing mail, which is highly unlikely.

There are many specific examples in support of the argument that anonymous free expression deserves protection. Social intolerance may require some individuals to rely on anonymity to communicate openly about an embarrassing medical condition or an awkward disability. Computer-mediated communication, in a more general sense, enables a degree of social anonymity by removing status cues such as sitting at the head of a table, or body language. Computer-mediated communication may be attractive to those who feel less competent in face-to-face settings where the subtleties of voice, dress, mannerisms and vocabulary are mixed in complex ways. In fact, investigations into computer conferencing and e-mail have highlighted that group decision-making discussions using computers exhibit more equal participation and a larger coverage of issues.

Whistle-blowers are another group that can benefit from anonymity. People who wish to publicize what they see as 'wrongdoing', but are wary of repercussions (e.g. from employers) may understandably be reluctant to come forward with information unless they can remain anonymous. Such information might include exposure of corruption, wrongdoing or abuses of power within an organization. Political dissent, even in democratic societies that prize free speech, may be impeded unless it can be voiced anonymously. Anonymity has an incontestable value in the struggle against repression, and even against the more routine corporate and government abuses of power. In the Kosovo conflict, for example, some individuals relied on anonymous programs (such as Anonymizer) to describe atrocities perpetrated by Serbians against ethnic Albanians. If the Serbians were able to trace the identity of these individuals, their lives would have been in grave danger.

Anonymous communication, whether facilitated by re-mailers or by other means, does of course have drawbacks. For example, it can be abused by criminals or terrorists seeking to communicate anonymously when plotting the crimes. It also permits cowardly users to communicate without civility, or to libel someone without accountability and with little likelihood of apprehension by law enforcement authorities. Anonymity can also be used to reveal trade secrets or violate intellectual property laws. There are also a number of documented cases where anonymity has been abused by sexual predators, to conceal their identity, in online chatrooms. For example:

In 1995, Katie Tarbox, a 13-year-old swimmer from New Canaan, Connecticut, met a man in an AOL chat room. He said his name was Mark and his age was 23. His grammar and vocabulary were good, and he made her feel special. Katie agreed to meet Mark at a hotel in Texas, where her swim team was competing. Soon after she entered his hotel room, he molested her. 'Mark' turned out to be 41-year-old Francis Kufrovich from Calabasas, California – a man with a history of preying on children. In March 1998, Kufrovich was the first person in the United States to be sentenced for Internet pedophilia. After pleading guilty, he served 18 months in prison. (Quinn, 2004)

## Ethical and Professional Issues

What are the responsibilities and duties of computing professionals on matters to do with free speech? Many professional computing bodies echo the proclamations about free speech in the legislation cited earlier. Rule 4 of the British Computer Society Code of Conduct, for example, states that members 'shall conduct ... professional activities without discrimination against clients or colleagues..' and that they 'should adhere to relevant law within the jurisdiction where [they] are working and, if appropriate, the European Convention on Human Rights'. The Association for Computing Machinery (ACM), meanwhile, states that '... as a professional you have a professional duty to safeguard the basic human right to freedom of speech'.

In a broader sense, freedom of expression can also be taken to entail thinking about questions of social responsibility in the design of technology and software. For example, when designing new Internet technologies, computing professionals arguably have an ethical responsibility to think about how the uses and functions of those technologies might allow certain actions, and restrict others. Clearly, some computer technologies can be designed to enable freedom of expression, whereas others can be designed to more easily enable censorship and control of expression.

The Internet was founded on the principles of sharing programming ideas. Early web technology was placed in the public domain. The technological infrastructure of the Internet was deliberately designed to make the centralized control of the network difficult. It could easily have been designed another way.

## Internet Governance

The Web and the Internet have created many opportunities for data sharing and eCommerce, but, as we have seen, they have also posed some formidable problems for lawmakers of national governments. The Internet has traditionally been decentralized and self-governing, and it has so far evaded strict or systemic regulations. However, there will always be a need for some type of stability imposed from above, that is, from the government or other centralized authorities. At a minimum, there must be a central body to manage Internet domain name distribution and to handle trademark disputes.

But what exactly is the right mix of top-down regulations and bottom-up control? There are at least three basic top-down models that have some plausibility and are worth a cursory review:

- **Direct state intervention:** the existing laws of each nation could govern the Internet; thus, the state could amend or extend its current laws so that they apply to pertinent activities in cyberspace
- **Coordinated international intervention:** a new intergovernmental organization composed of representatives from countries that use the Internet could establish new rules and regulations for cyberspace that will have international jurisdiction
- **Self-governance:** the Internet would develop its own semi-official political structure; it would be governed by charters established by non-profit organizations that represent the Internet's stakeholders.

## An Ethical Dilemma

*Let us suppose that you are employed by a company that develops websites for clients. One day your boss presents you with a new project. In brief, your company has obtained a contract from a law enforcement agency to develop several websites. These are to act in line with the 'honeypot' scenario mentioned in the previous chapter. The project being undertaken by the law enforcement agency is to gather information in relation to individuals who may be 'interested' in extreme forms of violence. By developing this website you will be assisting the law enforcement agencies who will gather material in relation to people who peruse the site.*

*What is your ethical position? Do you think this is an appropriate agenda in terms of invisibly policing the Internet? Since your boss has presented you with this brief, in the case that you do not agree with the ramifications of policing the Internet in this way, do you have any practical alternative but to undertake the work? (Here we assume that your boss is insistent that the work should be carried out by you.) What – if any – real objections do you have? Do you feel this is encroaching upon the liberty of the individual? Are your views influenced by the nature of the content of the website? For example, would your views be any different if the website related directly to terrorism or other forms of political extremism? To what extent do you think that the Internet is currently being policed – not only in terms of monitoring those who enter particular websites or who enter contentious chat room areas or the like?*

◀ Preliminary Activity for Week 10

Jump to...



Analysis, Application, and Exploration for Week 10 ►



### Navigation

Home

 Dashboard

Site pages

My courses

Capstone Project 1

Network Attacks: Detection, Analysis & Counter...

Ojt/Practicum 1

Social And Professional Issues

Participants

General


06 - Preliminary Examination

09 Regulating Internet Content


10 Regulating Internet Content (Cont.)

 Preliminary Activity for Week 10

 **Lesson Proper for Week 10**

 Analysis, Application, and Exploration for Week 10

 Generalization for Week 10

 Evaluation for Week 10

 Assignment for Week 10

System Integration And Architecture 2

Courses

---

## Fair Warning

**NOTICE:** Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for ***free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.***

**PROSECUTION:** Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for the second offense.

**COURSE OF ACTION:** Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

---

## Activities

 Assignments

 Forums

 Quizzes

 Resources