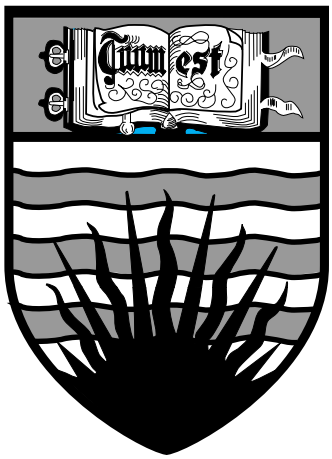

Report of the Task Force on the Appropriate Use of Information Technology

Prepared for

Dr. Bernard S. Sheehan, Associate Vice-President
Information and Computing Systems

Task Force Members

Dr. Maria Klawe (Chair)	*Dept. of Computer Science*
Professor Robin Elliot	*Faculty of Law*
Ms. Susan Mair	*University Computing Services*
Mr. Derek Miller	*Student Member, Board of Governors*
Dr. Jon Shapiro	*Dept. of Language Education*
Dr. Veronica Strong-Boag	*Ctr. for Research in Women's Studies & Gender Relations*
Staff	
Ms. Teresa Tenisci (Researcher)	*Information Systems Management*
Ms. Shirley Marcus (Secretary)	*President's Office*

The University of British Columbia
Vancouver, B.C., Canada
December 1992

§ CONTENTS

EXECUTIVE SUMMARY 2
- Fundamental Principles Used by the Task Force 3

SPECIFIC RECOMMENDATIONS 4

BACKGROUND MATERIAL 6
- History 6
- The Sexual Harassment Policy 6
- The Underlying Technology: The Internet 7
- Offensive Material: Nature and Impact 7
- Actions by Other Universities 8
- The Canadian Context 9
- The Legal Context 10
  - The Criminal Code of Canada 10
  - Civil Rights Protection Act 11
  - B.C. Human Rights Act 11
- Input Received from the UBC Community 12

DISCUSSION 14
- Fundamental Principles 14
- Restoration of Banned Newsgroups 16
- Education for Appropriate Use of Information Technology 16
- Procedures for Dealing With Inappropriate Uses 16
- Broadening the Community of Users 18

APPENDICES 19
A. Terms of reference for Task Force and list of members
B. Dr. Strangway's July 30, 1992 letter
C. Submission to Task Force by Dr. Peter Danielson, Applied Ethics
D. Submission to Task Force by Dr. Richard Rosenberg, Computer Science
E. Other submissions to Task Force
F. UBC Sexual Harassment Policy
G. Recommended wording for computer account applications
H. Recommended procedures related to inappropriate use of information technology
I. Recommended additional actions by UCS

§ EXECUTIVE SUMMARY

Our Task Force was asked to make recommendations on the appropriate use of information technology in the context of UBC's Sexual Harassment Policy. The Task Force reviewed policies at other universities, received input from the University community through written and verbal presentations, and considered a variety of related topics including limitations of the technology, policies on libraries and other communication media, and the Canadian socio-political and legal contexts. This summary highlights the major findings of the Task Force, and is followed by a set of specific recommendations. The background material and more detailed discussions of the issues are given in the body of the report.

Information technology offers tremendous opportunities for enhancing teaching and research activities at universities and UBC should take full advantage of these opportunities. Thus, we are recommending that UBC reinstate access to all available newsgroups.

As is the case for other communication media, some material carried via information technology may be offensive to some or all members of a community. Moreover, the medium may be used by individuals in ways that harass others. These abuses may include racism and other violations of human rights as well as sexual harassment.

The University must work to create a climate in which the users of information technology treat each other with respect, and in which abuses of others are not tolerated. It is, however, technically infeasible and also inappropriate for a university to attempt to restrict access to material that some may consider offensive. The Task Force believes that the best approach to creating an acceptable climate is through education, and through the establishment of procedures and penalties for inappropriate use. Some procedures are already available through the Sexual Harassment Policy. Moreover, based on our study, the Task Force feels that some of the changes to that policy now under discussion by the President's Permanent Advisory Committee on Sexual Harassment would result in procedures better suited to handle problems arising from the inappropriate use of information technology. Our study also points out the immediate need for an effective Human Rights Policy at UBC, since many incidents of inappropriate use are not sexual harassment but are still violations of human rights. In addition, it is important that UBC identify a single individual with responsibility for providing advice, and for contacting the appropriate authorities external to UBC when, for example, material that is believed to be illegal is involved.

Another important issue is the need to broaden the community of users of information technology at UBC and elsewhere. This will significantly contribute to the creation of a culture more sensitive of the views of others. It will also allow a much larger segment of the community to take advantage of the educational opportunities provided by information technology.

Finally, information technology and its associated culture is evolving so rapidly that it is important that the University regularly review its policies and procedures in this area. Such reviews and any decisions which are made should involve consultation with the University community.

• Fundamental Principles Used by the Task Force

1. Those associated with the University are entitled to the best possible environment for working and learning.

2. Such an environment is not one in which those associated with the University are involuntarily exposed to pornographic, racist, homophobic, and similar offensive messages and images.

3. Therefore, no one associated with the University should be required to consume against his or her will offensive messages and images conveyed by information technology or any other means.

4. Those associated with the University should be entitled to communicate freely with one another and the wider community.

5. The Criminal Code of Canada, the Civil Rights Protection Act, the B.C. Human Rights Act, and the UBC Sexual Harassment Policy all apply to the use of information technology at the University, as they do to other aspects of life here, to limit completely free communication in order that the best possible environment be preserved.

6. The responsibility for establishing the best possible environment for working and learning is a shared one between the University administration and those associated with it.

7. The University should not ban the electronic communication between *willing* participants of messages and images which others might find offensive, since no such ban applies to other forms of communication.

8. Those associated with the University should be educated about the laws and policies applicable to this area, as well as about the need for everyone at UBC to treat one another with respect.

§ SPECIFIC RECOMMENDATIONS

1. The University should ensure that its efforts to create an environment in which all members treat each other with respect extend to facilities and activities associated with information technology.

2. The University should provide access to all newsgroups and, more broadly, the Internet as a whole, for all members of the University community. Other institutions, such as schools, which access the Internet through UBC accounts, should be informed of the possible existence of material that is inappropriate for their users. Such institutions should make their own policies regulating access to such material.

3. The University should make it clear that the user bears the primary responsibility for the material he or she chooses to access, send, or display on the network and other computing systems.

4. The University should educate the University community about the benefits of access to the Internet and information technology, as well as the form of and need for responsible use of these resources. In particular, before obtaining accounts, users should be informed of the culture and etiquette involved in the use of information technology such as newsgroups and electronic mail, the nature and impact of offensive uses of these facilities and associated penalties, the procedures for reporting abuses, and the Canadian legal context.

5. The University should instruct the administrators of units operating computing facilities to establish procedures for dealing with abuses involving information technology. An outline of recommended procedures is given in Appendix H. All administrators should be aware of the issues involved, and be prepared to deal with complaints in consultation with the Sexual Harassment Policy Office or Human Rights Office (once it is established). A single individual should be identified as the person to whom abuses should be reported in cases involving material that is potentially illegal, or sites outside UBC. This individual should be responsible for notifying the appropriate authorities external to UBC. The University should make it clear that, as in other contexts, all members of the community bear a responsibility to report instances where they feel abuses have occurred. Moreover, the University should ensure that there are non-intimidating mechanisms for doing so.

6. The University should establish Sexual Harassment and Human Rights policies in which victims need not bear the entire responsibility for initiating correction of offences under those policies. The policies should attempt to deal with causes as well as symptoms.

7. The Campus Advisory Board on Computing should be responsible for regularly reviewing the University's policies on the appropriate use of information technology. This body should be broadened to include representatives of graduate and undergraduate students.

8. The University should provide resources, information, and incentives to encourage the broadest possible participation in the use of information technology at all levels in the University community.

9. Changes in policies affecting information technology should involve significant consultation with the University community.

§ BACKGROUND MATERIAL

• History

In April/May of 1992 the availability of pornographic material on university computers became a very controversial topic with widespread media interest. UBC Associate Vice-President Bernard Sheehan and his computing staff worked on the issue for several weeks, collecting background information from other institutions worldwide. A package containing some of the most extreme material was made available to senior administrators at most Canadian universities through activities of the Women's Centre at the University of Winnipeg. Several members of faculty, staff and the student body at UBC, including the Advisor on Women and Gender Relations, the President of the AMS, and the Director of the Centre for Research in Women's Studies and Gender Relations, wrote to President Strangway protesting the availability of pornographic material on UBC's computers.

On July 30, 1992, President Strangway issued a letter (Appendix B) informing the University community that all pornographic material would be removed from the computer files belonging to University Computing Services and requesting that all UBC units be very vigilant that University property not be used to access, create or store pornographic material on University computing equipment. He announced that AVP Sheehan had taken steps to remove the newsgroups and would establish a Task Force on the Appropriate Use of Information Technology. On September 14, 1992 AVP Sheehan published the Terms of Reference (Appendix A) of the Task Force, instructing the Task Force that it should advise the President's Office on appropriate use of information technology in the context of the campus Sexual Harassment Policy.

• The Sexual Harassment Policy

UBC's Sexual Harassment Policy (Appendix F) came into effect in February 1988. The critical provision of that policy for present purposes is section 1.01, which reads as follows:

> *1.01 "Sexual Harassment" includes comment or conduct of a sexual nature, including sexual advances, requests for sexual favours, suggestive comments or gestures, or physical contact when any <u>one or more</u> of the following conditions are satisfied:*
>
> *(1) the conduct is engaged in or the comment is made by a person who knows or who ought reasonably to know that the conduct or comment is unwanted or unwelcome;*
>
> *...*
>
> *(5) the conduct or the comment is intended to, or has the effect of, creating an intimidating, hostile or offensive environment.*

In the university context sexual harassment often occurs between individuals of unequal status. However, sexual harassment can and does occur between individuals of equal status.

In practice, this policy has been applied to a single incident or a series of incidents. Clearly individuals who receive unwanted material of a sexual nature or are exposed to this material by means of information technology can seek the assistance of the Sexual Harassment Policy Advisors or any University administrator in order to remedy their situation.

• The Underlying Technology: The Internet

In understanding the issues, it is important to understand the underlying technology and how it is used. The Internet, a recent and rapidly growing phenomenon of high technology, consists of approximately one million computers, each being used by one or more people and connected to each other by telephone lines or their higher-speed equivalents. This computer network spans the globe. It is used to generate, communicate, and store information. In particular, the Internet serves as an alternative to the post office and a library, and permits its users to send messages and receive them from others connected to the network. It also permits, via newsgroups and bulletin boards, group discussions on, at last count, over 1500 separate topics.

The benefit of the Internet to those who use it regularly, of whom academics are a large percentage, is the quick and easy exchange of ideas and information. Many academic research communities rely almost entirely on the Internet for the communication of information (announcement of research results, conferences, job openings, etc.), and groups of researchers often use the Internet as the primary vehicle for collaborative research. Canada's Networks of Centres of Excellence, for instance, are centres in name only; without the Internet, the joint work done by the Centres would be impossible, as the researchers are spread across Canada.

Once a site is connected to the Internet, it is virtually impossible effectively to control or censor the information that can be accessed from that site. The volume of new material received by a site each day is so high that monitoring each item is simply not practical. The high degree of connectivity in the network and the ability to log on to remote sites ensures that users have many routes by which they can access material banned from their local site. For example, when a university removes some newsgroups, users can continue to access these newsgroups by connecting to other sites, as is currently the case at UBC. The only effective form of control would be to cut off all access to the Internet. Like cutting off our telephone system from the rest of the world, the benefit to UBC of doing this would be far outweighed by the drawbacks.

• Offensive Material: Nature and Impact

Computer communication is subject to many, if not all, of the problems of other media. It can be, and on occasion is, used to communicate material and information that objectifies and effectively dehumanizes both individuals and groups. Abuses range from the use of sexual imagery as computer background screens in labs and other shared computing environments, to widely disseminated messages containing hate material. Offensive background screens create work environments which are extremely unpleasant for many individuals, while hate material implicitly and sometimes explicitly justifies and advocates actions and policies, including violence, which limit the freedom and opportunity of targeted individuals. UBC is not exempt from such abuses. During the month of November 1992 alone, there were

episodes of pornographic background screens appearing in UBC undergraduate computing labs, and UBC users posting newsgroup messages which were both inappropriate to the newsgroup topic and highly offensive.

Offensive materials range widely in their nature and preoccupation. Jokes and off-hand dismissals of legitimacy and authority exist at one end of the continuum, advocacy of rape, lynching, and genocide at the other. While most material is of the milder variety, at its core, too often, lie assumptions about the inferiority of others and the superiority of the messenger. Women, children and all groups perceived as "the other" (in the West these are usually non-Christians, people of colour, persons with disabilities, and lesbian and gay individuals) have always been favourite, sometimes interchangeable and often overlapping, targets for media overwhelmingly controlled by white men. Much of the material is merely silly and unpleasant but there also exist regular examples of extreme misogyny, racism, and homophobia. Whether voiced publicly or privately, such hate material, whether in the form of pornography which links violence and degradation with sexuality, or approval of Hitler's "final solution," threatens and disempowers its targets. The result compromises any free society.

Substantial debates rage about the impact of material along this continuum. Free speech advocates and censors exist simultaneously among conservative and progressive, including feminist, groups. Efforts at solution also vary by jurisdiction. Canada, for example, has taken a much more proactive legislative role than the United States. The problem of how to identify and deal with "hate material" distributed through computer systems now confronts the UBC community, and has been the major focus of our Task Force.

• Actions by Other Universities

Universities have responded to the situation in which pornographic and other offensive materials might be accessed from the Internet through their computing facilities in a variety of ways. Some institutions have decided to retain access to all newsgroups because they view censorship as ineffective and inappropriate. Some have always carried only an approved subset of available newsgroups, and others have deleted access to specific newsgroups in response to the recent controversy and complaints.

Those institutions which have deliberately chosen not to censor newsgroups include the University of Toronto, Stanford University and the University of Waterloo. In fact, both Stanford University and the University of Waterloo reversed earlier decisions to remove the newsgroups as the result of community feedback and reports from *ad hoc* committees. The Waterloo report recommended that "the University adopt and widely publicize the principle that it is the user, not the University, who is responsible for his or her decision to read a mail message or an article posted to an electronic newsgroup ... and in sending E-mail or in posting an article to a newsgroup... assumes responsibility for its contents." It also recommended appointing a person to help users deal with objectionable electronic news or mail.

Of those who have censored newsgroups some, including Simon Fraser University and the Universities of Alberta and Victoria, acted unilaterally on the advice of computing centre management. Others, such as the University of Manitoba and Queen's University, referred the matter to committees similar to UBC's Campus Advisory Board on Computing for a

review of their decision to delete the newsgroups. Most of these universities made an attempt to block whatever material they had received complaints on, as opposed to actively censoring the relevant newsgroups, and made allowances for private feeds of the material if requested in writing. Common reasons given for censoring included "inappropriate use of University resources for material that is not in support of the University's mission of teaching and research," lack of computing resources and disk space, and liability issues concerning illegal material and accessibility by minors.

In researching policies on the appropriate use of computing resources at other universities, we found very few which described effective procedures for dealing with offensive material. Most institutions are still studying how to modify their existing policies, which usually cover topics such as confidentiality, copyright, privacy, and unauthorized access. Excerpts from some of the relevant policies which express sentiments with which the Task Force generally agrees include:

- "Unmannerly conduct, including mailing obscene or abusive material is unacceptable behaviour." (University of Waterloo)

- "Respect the rights of other users; for example you shall comply with all University policies regarding sexual, racial and other forms of harassment." (University of Michigan)

- "Sending rude, obscene or harassing material via any electronic mail or bulletin board is strictly forbidden." (Iowa University)

In addition to appropriate use policies, many institutions are investigating procedures which can be used to deal with incidents of offensive material or harassment. Again, there are very few models of established working procedures.

• The Canadian Context

A number of people who made submissions to the Task Force invoked, in support of the positions they took, arguments grounded in either the experience or the socio-political traditions of other countries. Prominent amongst these were arguments grounded in the American free speech tradition.

Grateful as the Task Force was to be told about the approaches taken in other jurisdictions to the problem with which it has been asked to deal, and important as it is to examine that problem from a broad range of perspectives, the Task Force is strongly of the view that the best approach to take to this problem at UBC is one which reflects the Canadian context, including our socio-political traditions. These traditions, which are finding clear expression in the judgments of the Supreme Court of Canada under the Canadian Charter of Rights and Freedoms, include a greater willingness than exists in the United States to acknowledge that the abuse of private power can be as much a threat to freedom in a modern liberal democracy as the abuse of state power; a greater sensitivity to the harmful effects of pornographic and racist messages and images; and a greater emphasis on the need to attend, not merely to freedom and equality in their formal senses, but to freedom and equality in their substantive senses as well - that is, to recognize that, in a society in which real inequalities exist

between individuals and groups, a policy of inaction is not always going to promote the cause either of freedom or of equality for society as a whole.

To insist upon an approach which is sensitive to these socio-political traditions is neither to denigrate the importance of freedom of expression nor to ignore the dangers of heavy-handed action on the part of the University in this area. It is simply to say that, in the Task Force's view, it is not enough if one is arguing for a hands off approach to wave the flag of "free speech". At least in Canada, the issue is more complicated than that.

• The Legal Context

Resolution of the issue of how the University can best deal with the problem of pornographic and other offensive messages being communicated on the Internet and through other information technology media on campus necessarily requires that account be taken of the broader legal context within which the University and those who work and study here function. There are three aspects of that broader legal context which are especially relevant to this task.

Criminal Code of Canada

The first is the Criminal Code of Canada, which contains prohibitions against both obscenity and hate propaganda. The prohibition against obscenity makes it an offence *inter alia* "[to print, publish, distribute, circulate, or have in one's possession] for the purpose of publication, distribution or circulation any obscene written matter, picture... or other thing whatever," with the term "obscene" being defined in terms of a publication "a dominant characteristic of which is the undue exploitation of sex, or of sex and...crime, horror, cruelty and violence." There can be little doubt that individuals who send obscene messages and images through the Internet are vulnerable to prosecution under this provision of the Code. It is possible that individuals who store obscene messages and images in their computers with the intention of showing them on their screens or otherwise communicating them to others would be vulnerable to prosecution. It is even conceivable that the University itself would be vulnerable to prosecution if it stored such messages and images and made them freely available to users of its systems.

The Supreme Court of Canada has recently revisited the question of how the definition of "obscene" should be understood. It indicated that (a) the combination of sex and violence will almost always be considered obscene; (b) explicit sex which is degrading and dehumanizing may be so considered; and (c) explicit sex which is not combined with violence and is neither degrading nor dehumanizing will generally not be so considered unless children are involved. However, it went on to add that, if the portrayal of sex is essential to a wider artistic, literary or other similar purpose, then even if, absent such a purpose, it would be obscene, a court should not hold it to be obscene. Integral to this approach to obscenity was a willingness on the Court's part to attribute harm to at least some pornographic messages, with harm being understood in terms of encouraging or predisposing people to act in socially harmful ways. But the Court also recognized that sometimes society must be prepared to endure such harm in the interest of freedom of expression.

The Code provision dealing with hate propaganda makes it an offence for anyone, "by communicating statements, other than in private conversation, wilfully [to promote] hatred

against any identifiable group," with "identifiable group" being defined to mean "any section of the public distinguished by colour, race, religion or ethnic origin." Persons charged with this offence have available to them a number of affirmative defences, including truth and "[relevance] to any subject of public interest, the discussion of which was for the public benefit... if on reasonable grounds [they] believed [the statements] to be true." Because of the way in which this offence is worded, very few people have been charged with it and even fewer convicted. However, it clearly has the potential to be relevant to the communication through systems such as the Internet of messages designed to promote hatred against racial and religious minorities.

It is worth noting that both the obscenity and the hate propaganda provisions of the Criminal Code have recently been held by the Supreme Court of Canada to be "reasonable limits" on the freedom of expression protected by the Canadian Charter of Rights and Freedoms. Hence both provisions remain intact even though they have been challenged under the Charter.

Civil Rights Protection Act

The second relevant aspect of the larger legal context is the Civil Rights Protection Act. This statute, which appears to be unique to the province of British Columbia, creates a civil cause of action for the targets of "conduct or communication... that has as its purpose interference with the civil rights of a person or class of persons by promoting (a) hatred or contempt of a person or class of persons, or (b) the superiority or inferiority of a person or class or persons in comparison with another or others, on the basis of colour, race, religion, ethnic origin or place of origin." The Act explicitly authorizes the courts to award punitive damages in cases brought under it, and to grant injunctions prohibiting the continuation of the offensive conduct or communication. Again, the language of this legislation is such as to make it difficult for those who would use it to succeed in bringing claims. Again, however, the potential is clearly there for it to be used to deal with at least some of the problematic messages and images which can be communicated through information technology.

B.C. Human Rights Act

The third and final aspect of the broader legal context which has special relevance to this Task Force is human rights legislation, specifically the B.C. Human Rights Act. Human rights legislation, which exists within the federal sphere and within each province and territory, is designed to eliminate discrimination on a range of different grounds in a range of different contexts. One of those contexts invariably is employment, and sex is one of the prohibited grounds within that context. The Supreme Court of Canada has recently made it clear that sexual harassment directed at persons of the opposite sex is to be considered a form of sex discrimination. Hence, any female employee who can satisfy the B.C. Human Rights Council that she has been a victim of sexual harassment at the hands of a male employee is entitled to a remedy of some sort, including damages, from that employee. Moreover, and this is particularly important insofar as the University in its capacity as employer is concerned, such a female employee will also, as a rule, be entitled to relief from the employer. While the law relating to the employer's liability in such circumstances has yet to be firmly settled, indications are that the nature and scope of that liability will be a function of the efforts taken by the employer to deal with the problem of sexual harassment in that particular workplace. An employer who is aware of a problem of sexual harassment and does nothing to remedy it can expect to pay a heavy price for its failure to act. Similar rules are

applicable in cases in which the harassment is based on race, religion, disability or any other prohibited ground of discrimination.

Another context in which human rights legislation prohibits discrimination is housing. Here again, sex is one of the prohibited grounds, and it is safe to assume that in this context, too, sexual harassment will be considered to be a form of sex discrimination. Although the potential for information technology to be a source of sexual harassment in the housing context would seem to be remote, it is conceivable that a problem could arise through the use of personal computers in university residences. Again, similar rules would be applicable in cases in which the harassment is based on another prohibited ground.

Yet another context in which discrimination is prohibited by human rights legislation is in the delivery of "services, facilities and accommodation customarily available to the public." As the law stands at present in British Columbia, the educational services and facilities provided by the University to persons who have been accepted as students are NOT considered to be services and facilities "customarily available to the public." Hence, students on this campus cannot now avail themselves of the B.C. Human Rights Act to seek relief from the University in the event that they are victims of sex discrimination or any of the other forms of discrimination prohibited by the relevant provision. It should be noted, however, that the decision in which this ruling was made is currently on appeal to the Supreme Court of Canada. If that decision is overturned, then students as well as employees will be able to make use of human rights legislation to deal with complaints of sexual and other forms of harassment arising from the misuse of information technology. In this context, too, the University might find itself being held to account if it were found not to have taken appropriate steps to deal with the problem on its own.

• Input Received from the UBC Community

After the July 30, 1992 letter from Dr. Strangway and the removal of the newsgroups, he and AVP Sheehan received a variety of responses, both positive and negative, to these actions. The Task Force on Appropriate Use of Information Technology began its meetings in September. During October, the Task Force advertised electronically and in print, seeking input from the campus community.

Approximately twenty submissions were received. Of these, only one was supportive of the University's decision to remove the newsgroups. Of the remaining submissions, almost all objected to the decision based on an opposition to censorship. Many others included additional reasons for their opposition. Several cited the usefulness of the Internet and the necessity for a university to respect the concept and tradition of academic freedom and the free flow of information. Others pointed out the difficulty of defining offensive material and the impossibility of totally removing offensive material from UBC's computers. The self-policing nature of the newsgroups was mentioned frequently as a reason why no action should be necessary, as was the observation that individual users had to take specific steps to view offending material. Solutions other than removing newsgroups -- such as educating people on responsible and ethical use, encouraging more widespread use of electronic news, and instituting procedures to deal with incidents of inappropriate use -- were mentioned in a few submissions.

It is worth noting that the majority of the submissions did not perceive any major problems. We received no input from individuals who felt they had been victimized. Rather, the submissions were from people who feel empowered by the existing system.

In addition to these submissions, the Task Force requested presentations from the following people to aid them in their deliberations:

- Dr. Peter Danielson, Centre for Applied Ethics
- Dr. Richard Rosenberg, Computer Science Department

The Task Force is grateful to all members of the University community who took the time to express their views.

§ DISCUSSION

• Fundamental Principles

The terms of reference given to this Task Force call for it "to advise the President's office on the appropriate use of UBC information technology and facilities in the context of the campus Sexual Harassment Policy." The principle underlying the latter policy is that those associated with the University are entitled to "the best possible environment for working and learning," and the policy itself represents an acknowledgment on the University's part that an environment in which sexual harassment occurs fails to deliver on that promise.

This Task Force accepts this first principle as fundamental. Moreover, it accepts that an environment in which members of the University community are involuntarily exposed to pornographic, racist, homophobic and similarly group-related offensive messages and images fails to deliver on that promise. For the members of those groups at which such messages and images are targeted - women, racial, ethnic and religious minorities, persons with disabilities, gays and lesbians - such an environment is clearly a hostile one, and one in which both working and learning can for them be exceedingly difficult.

The Task Force also, of course, accepts as fundamental the principle that those associated with the University, and particularly faculty and students, should be entitled to communicate freely with each other and the wider community. Commitment to such a principle is integral to the very nature of a university, and certainly, in the view of this Task Force, of UBC. Any form of constraint on this freedom to communicate is inconsistent with this principle.

It is apparent that, in some circumstances, these two fundamentally important principles come into conflict. The question is how that conflict should be resolved. To a significant degree, that question has already been answered by legislation by which members of the University community are clearly governed. Messages and images which are offensive to the Criminal Code provisions relating to obscenity and hate propaganda are subject to criminal sanction. The Civil Rights Protection Act renders messages and images caught by its terms subject to civil claims. And to the extent that the B.C. Human Rights Act can be said to apply to communicative activities on campus which amount to sexual, racial, and other forms of harassment, it too exposes those who engage in such activities to civil claims.

In the context of forms of communication which amount to sexual harassment, that question has also been answered for members of the University community by the campus Sexual Harassment Policy. Such forms of communication are effectively prohibited by that policy, and those who engage in them can be subjected to discipline by the President.

It is clear from these legislative enactments and this policy that it has been thought appropriate in at least some circumstances to impose constraints on freedom of communication in order to protect other interests, including the interest in a working and learning environment in which people are free from uninvited pornographic, racist, homophobic and similar offensive messages and images. Moreover, it is also clear that these constraints operate, either by necessary implication or by design, on the campus of this University.

This answer to the question of how the conflict between these two principles should be resolved commends itself to the Task Force when members of the University community are involuntarily exposed to such messages and images via information technology. In such circumstances, the principle of freedom of communication must, in the Task Force's view, give way to the principle of a positive working and learning environment for all. This is true not only when such messages and images offend one of these legislative enactments or the Sexual Harassment Policy but more generally. No member of the University community should be required to consume against his or her will offensive messages and images conveyed on information technology. There is little if any benefit to be gained and much to be lost by protecting the freedom to communicate of those who would convey such messages and images to those who, because they find them offensive, do not wish to be exposed to them.

With the exception of those messages and images proscribed by the obscenity and hate propaganda provisions of the Criminal Code and the Civil Rights Protection Act, the Task Force is not persuaded that it is necessary or appropriate at this time to recommend that the University ban the communication between willing participants of messages and images which others might find offensive. To do so would be to recommend that information technology should be singled out for special and more restrictive treatment on this campus than other methods of communication - for example, the telephone, private conversations conducted in person, the Library system - and that the Task Force is not prepared to do. As a medium for communication information technology has much in common with the telephone and the printed word; our Task Force feels it should be governed by similar policies. Printed materials which would be viewed as offensive to some people are available in the UBC Library; they are not in the stacks but must be requested specifically by the borrower. Likewise, a potentially offensive discussion on the Internet generally must be sought out by the reader: it is rarely inflicted on him or her unknowingly. The telephone system is open to abuse by those who would make harassing phone calls, but this potential for abuse does not result in restriction of access to telephones. Rather, the harasser is dealt with by social and legal sanctions. The same should be true of the Internet.

The Task Force does, however, recommend that it be considered a serious abuse of information technology to communicate to anyone messages and images which offend the provisions of these special enactments. Situations in which such messages and images are communicated should be no less a concern to the University than they are to society as a whole, and it is important that the University be prepared to take steps on its own to deal with them.

Before leaving this discussion of fundamental principles, mention should be made of two others which featured prominently in the thinking of the Task Force. One is the importance of educating the members of the University community not only about the specific laws and policies which are applicable in this area, but also about the need for all of us to treat each other with respect. The kind of working and learning environment that we are seeking to establish here - "the best possible environment" - is one in which there would be no call for the enforcement of such laws and policies because the atmosphere was one in which we all respect and take into account the interest of others. The University must take steps to ensure that this message is communicated consistently and in a range of different ways.

The other additional principle, which flows out of the first, relates to the issue of responsibility. This Task Force is firmly of the view that the responsibility for establishing "the best possible environment for working and learning" is a shared one. The University, as we have already made clear, bears a significant amount of this responsibility, but so too do individual members of the University community, faculty and administrators certainly, but staff and students as well. They too can participate in the educational process, and they too can take steps to ensure that the applicable laws and policies are enforced.

• Restoration of Banned Newsgroups

The Task Force recommends restoring access to all Usenet newsgroups because of their importance to the teaching and research missions of the University, and because of the difficulty and inappropriateness of attempting to censor material accessed via the Internet. We were not convinced by arguments that computing resources should be restricted to the research and teaching activities of the University, since it is extremely difficult to determine the boundaries of such activities. Moreover, the additional costs associated with maintaining access to all newsgroups versus maintaining access to a subset of newsgroups are negligible. Since the University makes no attempt to prevent the use of its other resources (buildings, telephones, etc.) for other activities so long as the costs incurred by the other activities are minimal, it would be inconsistent and undesirable to apply such restrictions to computing resources.

• Education for Appropriate Use of Information Technology

It is essential that all users of UBC facilities, including faculty, staff, students and others, be educated in what constitutes abuse of information technology and what to do if abuses occur. Specifically, in addition to distributing copies of the relevant legislative enactments, the UBC Sexual Harassment Policy and the pending Human Rights Policy to all of those at UBC, training sessions should be conducted by qualified instructors wherever possible.

There are two places where training in this area is particularly important. One is in classes of courses which use computing resources. Instructors should brief their students on what is considered appropriate and inappropriate use of the resources, and tell them what to do if abuses occur. The departments offering the courses must be prepared to follow up on complaints in an expeditious and sensitive manner.

Secondly, providers of information technology on campus such as University Computing Services, the Department of Computer Science, and other departments which issue accounts for use on computing equipment, should include a statement of what is regarded as appropriate use in their account application forms. Sample wording for such a statement is given in Appendix G. The penalties for inappropriate use should be made clear. Specific recommendations are made in Appendix H.

• Procedures For Dealing With Inappropriate Uses

Even with better education of the UBC information technology user community about issues concerning offensive material, incidents in which people are offended are likely to occur.

Procedures on handling offensive material are needed, as well as an educated and sensitive environment. All relevant UBC authorities, from lab supervisors to Deans and administrators, must be aware of their responsibilities with respect to the issue. They must know to whom complaints can be referred, but also deal with specific cases and general problems. In appropriate cases, complaints should be dealt with in consultation with the Sexual Harassment or Human Rights offices and the appointed individual in UCS.

We specifically recommend the identification of a single individual in UCS to whom abuses should be reported in cases involving material that is potentially illegal, or sites outside UBC. This individual should be responsible for notifying the appropriate authorities external to UBC. Moreover, all members of the community should be aware of their responsibility to report instances where they feel inappropriate incidents have occurred, and the University should ensure that there are non-intimidating mechanisms for doing so.

Although complaints will be the primary means of identifying problems, authorities should also be prepared to deal with abuses of which they are aware but about which complaints have not been made. Additionally, complaints should serve as a spark to action: if a complainant prefers not to pursue the matter, or the specific complaint is resolved while leaving a larger issue open, further action may still be necessary. Not only the victim but the University and its administrators have responsibility for initiating correction of abuses.

There are a number of different means of dealing with specific incidents, and the Task Force feels that all of the following are valid:

1. Taking direct personal action. The simplest (but sometimes not feasible) procedure is for those who have been offended to deal with the source of the offending material directly. This only works when the source is identifiable (either as an individual or group), accessible, and willing to listen, and when those offended feel comfortable with approaching the source of offense.

2. Notifying an appropriate authority. It must be made clear that there are people within the academic or administrative unit concerned who are responsible for addressing incidents which occur. There should be a number of such people identified, in case the most obvious person (e.g. a lab supervisor) is unsympathetic or unavailable.

3. Moving up the supervisory hierarchy. If the problem cannot be resolved at the level of the obvious authority, Department Heads or other such administrators should be informed and should be available to deal with incidents. Additionally, Heads or equivalent administrators should be made aware of incidents occurring within their departments, and should have the responsibility of seeing whether internal policies or procedures can be implemented to prevent similar incidents from occurring in future.

4. Using alternate avenues. If the problem is not resolved in a way satisfactory to the complainant, or if the complainant wishes to pursue the issue in a parallel manner, other avenues should remain open and be made clear. Examples include the Sexual Harassment Office, any new Human Rights Office, the UCS resource person mentioned below, the AMS Ombudsoffice, and, depending on the nature of the incident, police, human rights agencies, and the courts. Referral to another avenue of complaint should not excuse the previously mentioned authorities from trying to reach

a resolution or dealing with larger problems while a specific case is pursued through other means.

Once action has been taken at any level other than that of direct personal communication, i.e. by any authority, the incident and the resolution should be publicized by whatever means are convenient and appropriate. The user community should be informed of the outcome of incidents where sanctions were applied in departments which have computing facilities.

• Broadening The Community Of Users

The media is the voice of the community, allowing it to express its interests, concerns, and prerogatives. This applies to information technology as much as to any other media, and many of the issues concerning offensive material on the Internet may be related to the relative narrowness of its community of users. The community tends to be male, of European descent, middle-class, scientifically-oriented, and North American and European in location. Thus the culture that has evolved does not include a large part of the wider diverse community. Inevitably, the preoccupations and prejudices of the largest group of users have coloured the character and development of information-technology-based media. Fiat will not change this orientation, although it would undoubtedly bring about some degree of subterfuge. What is needed is an end to the effective monopoly over a powerful medium.

Information technology will better serve the entire community if its users represent the community's diversity. Women, those of non-European origin, those trained in the arts, social sciences and humanities, and others presently without a voice in information technology media must be empowered to contribute to electronic exchanges. Here the University can take leadership by taking steps to bring in otherwise excluded groups. Institutional initiatives should begin with education, both within and without the classroom, and with practical assistance in linking into computer-mediated debates. Without such initiatives, the Task Force fears a continuing and growing division between those who use and control a powerful medium and those who for one reason or another are excluded. The costs of refusal to address this imbalance are substantial, and the benefits of broadening the community of users are enormous.

§ APPENDICES

- **APPENDIX A**
  Terms of reference for Task Force and list of members

- **APPENDIX B**
  Dr. Strangway's July 30, 1992 letter

• **APPENDIX C**
Submission to Task Force by Dr. Peter Danielson, Applied Ethics

Ethics & Computer Mediated Communication[1]

by
© 1992 Peter Danielson[2]
Senior Research Fellow
Centre for Applied Ethics
University of British Columbia

Introduction

The Task Force on Appropriate Use of Information Technology is charged with examining some of the most important and difficult questions facing an ethically sensitive university community committed to using computer mediated communication (CMC)[3]. I am happy that you asked me to appear before you, as these issues are central to my reseach, and very interesting as well.

I also realize that the features of the problem -- ethics and CMC -- suggest that you will likely encounter too *much* input. So I will try to be brief and focus on those facets of the problem about which I have something special to say as a moral philosopher and as a professional applied ethicist. I will organize my remarks under three headings. First, I sketch the structure of the moral problem at hand. Second, I shall sketch our experience at the Centre for Applied Ethics in ethics and computer mediated, communication indicating some practical risks of censorship to our work. Third, I sketch some practical proposals.

2. A Conflict of Values

We face a conflict of two values: the value of freer communication due to computer mediated communication (especially networking) and the harms caused by offensive messages. Those unaffected by either value will not have our problem. (Those who do not wish to participate in the Internet's technological adventure do not share our ethical problem and those morally less sensitive to the harms of technology can let the technology take them where it may.) To focus my presentation, let me specify the conflicting value assumptions that I see structuring the problem:

---

1 Notes for a Presentation to The Task Force on Appropriate Use of Information Technology, U.B.C.

2 Comments welcome. Author's address: 1866 Main Mall, E-162, Vancouver, B.C. Canada, V6T 1Z1. Email: danielsn@unixg.ubc.ca, , FAX (604) 822-8627 (604) Tel: 822-4658. This document is available in machine readable form; contact artmoral@unixg.ubc.ca.

3 I will use CMC as my most general term and the Internet as a narrower term to refer to the interconnected system of university computing equipment including thosethat provide access to many other computing sites.

Assumption 1: *CMC is a valuable new communication medium which comes under the prima facie case for mininal constraints on free speech within a university community.*

Assumption 2: *Some find the content of some messages objectionable posing a prima facie case for censorship.*

2.1 Specifying the Assumptions

Notice two things missing from these Assumptions. First, `pornography' is not mentioned. I do not limit my discussion to pornographic messages because the terms of reference for the Task Force are not so limited, but refer generally to "materials from the Internet [others have] seen as objectionable." Since I have not seen the supplied examples, I cannot assume that they are all pornographic. Also, pornography is a strongly contested term, so an important policy issue will be defining what is to count as pornographic. It would seem more expeditious to focus directly on the more general problem of offensive communication.

Second, I make no special mention of the technology involved. In most of my conversations about this issue, in classes, at conferences and over several Internet-based colloquia, I have found that many participants rush to the `technological gambit', taking the problem to be a technical one. For example, people often think that the solution is simply denying certain newsgroups disk space, "because this costs the University money". But there is nothing special about CMC technology -- paper also costs money.[4] We need a general solution to the problem of offensive communication, which we can then apply to various technologies: books, newspapers, newsletters, mail, posters, phone, e-mail, bulletin boards, IRC-chat, and so on.

Finally, I note that we are raising the question in the context of a Canadian university. I stress *Canadian* because much of the discussion in the wider Internet community assumes the US. legal framework.[5] But more important, I stress *university* because quite different policies may be appropriate in institutions, such as businesses, or indeed the public realm at large, not predicated, as ours is, on the centrality of the value of open inquiry and communication of results, some of which are likely to be offensive to some of us and to the larger community.[6]

---

[4] This strategy can also backfire in several ways. The largest, and therefore more expensive newsgroups tend be computer binary groups; smut is fairly compact, except in the form of images. Also the cost objection can be met in ways that will not eliminate the offensive material. Pornographic images can be compressed, the info-mac archivists have recently raised money from the Internet community for a gigabyte disk drive, and alt.censorship has a home financed by a millionaire patron. Finally, if full environmental cost accounting is used, newsprint may be more costly that disk space.

[5] For example, the list, "Banned Computer Material 1992" (archived at ftp.eff.org) of campuses practicing censorship, on which UBC appears, contains 7 Canadian and 13 U.S.

2.2 Resolving the Conflict?

Having set out the conflict, what can be said about resolving it? My own inclination would be to develop a libertarian defense of the freest communication in the special setting of the (research) university campus. Several well-known lines of argument agree here.[7] On the one hand, Mill's famous utilitarian defense of free inquiry has its clearest application in our setting, as the university and CMC are settings which support intellectual and critical feedback. On the other hand, Scanlon's lesser known complementary account of the limitations on the rights of censors has special application in a university setting, where the authority of the censor presumably must be *intellectual* and *moral*, not political, and therefore the grounds for the decision must be accessible to the judgment of the university community, arguably the best informed community on matters intellectual and moral. But I do not propose that we should try to settle these issues, so central to our ethical tradition, here. I would contend that the wider university community must be engaged on these issues -- but this is simply to reiterate Mill's emphasis on the educational value of free speech, and Scanlon's on the right of autonomous agents to make up their own minds about moral and political matters. (See Proposals for one means to open up this discussion.)

2.3 Relieving the Conflict

A more modest goal is to reduce the conflict between free communication and offensiveness. One established liberal technique to reduce this conflict is to distinguish private from public realms, and stress voluntary exposure to what consenting adults do in their private realms. Taking this perspective, it is surprising that CMC should be the focus of our current problem, since it tends to be governed by a high degree of voluntary exposure. Even the most offensive newsgroup requires that I log on to a computer network, execute a newsreader, select that newsgroup, and allow particular messages to appear on my screen long enough to read them. Even at that point they are still less invasive than the graphic dailies displayed in the newspaper box at my bus stop. This suggests a general recommendation.

General Recommendation: *Stress voluntariness of Exposure***.**

There are many different ways to categorize the conflict between the harm of offensive content and communicative values. I propose that we stress the degree to which the exposure to offense is voluntary. This yields a ranking of some recent and hypothetical cases of offensive computer mediated communications in the following order:

---

institutions, a disproportionate ratio that likely reflects the legal differences between the two countries.

6 For a stronger statement, see “On Freedom of Expression and Campus Speech Codes of Expression”, The American Association of University Professors, archived as academic/speech-codes.aaup at ftp.eff.org.

7 The relevant selections from Mill and Scanlon are reprinted in (Stewart 1986).

Best case for intervention:	involuntarily receivable
	Unsolicited e-mail without informative header;
	posting to ubc.general (e.g. Burkholder's sex slave ad)
	Plan file
Weaker case for intervention:	publicly accessible to minors
	alt.sex; IRC-chat; tinysex M.U.D.
Weaker case for intervention:	publicly accessible to adults
Weaker case for intervention:	accessible to restricted group
	CBPENet; Thick/Thin
Worst case for intervention:	private files
	The Japan that Could Say No

2. Network Research Projects at the Centre for Applied Ethics

The Centre for Applied Ethics is the home of three research projects using university computers and the Internet. I sketch them to indicate the range of our involvement and also to suggest the risks of a censorial policy to the type of research in which we engage.

2.1 Canadian Business and Professional Ethics Network (CBPENet)

The Canadian Business and Professional Ethics Network, whose principal investigator is Michael McDonald, Director of the Centre for Applied Ethics, offers its members a convenient, private, and secure means of discussion, some topics of which may involve ethically sensitive material. CBPENet is a private network; the co-investigators and the initial invitees, representing a broad spectrum of the Canadian business and professional ethics community, are the original members. We have created democratic procedures for adding new members and spawning sub-networks.[8] This project has received some notice among granting agencies for its ability to draw together constituencies both within and without the university community. This trustbuilding task is not trivial when different disciplines and professions as well as a new technology are involved. I have studied it, both from the theoretical side (Danielson 1992) and in a review of the literature of the sociology of computerization [9] We included in the design of CBPENet an initial face-to-face meeting in Vancouver, both to build trust and personal relations prior to the introduction of CMC and also to make democratic decision on network governance the practical norm.

What are the risks of policy change here? Privacy and -- of course -- freedom from censorship is part of the appeal of CBPENet, which has discussed sensitive issues effecting both the members and their clients. There are also broader questions of interfering with the democratic self-governance of a new virtual community. (Will the censors ask to join CBPENet or regulate it from without?). More legalistic questions arise whether the university, claiming `ownership' of equipment purchased with grant monies for a particular purpose, may interfere with that purpose, in this case a private, self-governing network.

---

[8] A more detailed description of The Canadian Business and Professional Ethics Network is attached as Appendix A, with details on the first sub-network.

[9] See (Danielson 1991); (Dunlop 1991) is an important collection of sources.

2. 2 Computer Ethics through Thick and Thin

Computer Ethics through Thick and Thin, of which I am the principal investigator, is an international and interdisciplinary experiment in the effects of different parameters of CMC on ethical discussion and decision-making. Participants from most continents, and from many disciplines and organizations meet in a pair of colloquia, one under conditions of full information and one under continuing pseudonymity. This experiment, which was launched at the First National Conference for Computers and Values, in August 1991, has been underway for almost a year, using software under development in my Group.[10]

This project involves ethically sensitive material and is committed to protecting the privacy of its members, half of whom are shielded by their use of pseudonyms. This project indicates some of the difficulties facing censorship policies in a research institution. When I was searching the enormous resources of the Internet for software to implement pseudonymous communication, I was directed to alt.sex.bondage, which is a leader in this area. More recently, rec.games.mud has been the source of innovative software for constructing multi-user dialogues. Unfortunately the first of these groups is among the first to be removed as offensive pornography and the second might be at risk when someone reads about the possibilities of tinysex discussed there.

2.3 The Ethics of Environmental Modeling

I have recently formed the Computer Modeling & Communication Group within the Centre to pursue research initiatives. We have recently been awarded a contract, in connection with a large NSF grant, to provide ethical consulting to the North Carolina Supercomputer Group. which builds environmental models for the Environmental Protection Agency in the U.S.A. Part of my plan is to provide principled ways to decide what features of a model should be public and which should not. Since environmental models are one of the most controversial subjects in politics just now, we had to assure our client that we could provide the required privacy. Yet some will be offended by assumptions made by some of these models and some will charge that some of these assumptions should not be kept from the public. I also plan to develop a remoted whistle-blowers network for this client. All this information will be kept on university computers.

2.4 Risks

The direct risks of censorship are fairly obvious. We have promised various constituencies privacy and anonymity. It is not clear that we will be able to provide this under new policies. It is not clear who the censors will be, what they will censor, who they will share the contents of which files with, and so on.

---

[10] A more detailed description of Computer Ethics through Thick and Thin is attached as Appendix B.

Indirect risks are more difficult to foresee. Censorship "chill" is probably the most insidious. Will we be reluctant to take on projects on "poisonous" subjects. Will clients on the "wrong" side of these topics even approach us under the new policy? How will U.B.C's reputation be affected? I will probably be better able to answer this last question when I present my paper on Philosophical Research and Networks at the American Philosophical Association's panel on The Electronic Philosopher, as that audience has, in the past, been keenly aware of censorship as a philosophical issue.

3. Some Proposals

You have asked for proposals that are practical in three respects: (1) they should implement the Sexual Harassment Policy, (2) they should be acceptable to the university community and (3) they should be readily communicated to the campus information user community. My proposals will fall short on (1), stress an educational version of (2) and satisfy (3) best.

A leading thread of my research on ethics and technology -- and CMC technology in particular -- has been the inadequacy of attempts to regulate emerging technology by applying prior moral intuitions. To this somewhat skeptical and negative claim, I add a constructive and hopeful conjecture: CMC has potential to be an ethically progressive medium. This is not the place to defend a conception of ethical progress, but the point is simple. If we get better at solving our moral problems by wide, open, non-coercive intellectual discussion, then within the technological community, CMC should be morally progressive, since this plastic medium allows us better to model ideal moral communication. I am, however, not a technological *utopian.* For example, I stress *within the technological community*, because, of course, not everyone, not even every academic or intellectual, has access to the Internet. Nor is the medium always or even usually used in the critical, morally sensitive way that it might. But these are things that we can do something about. Therefore I suggest:

Proposal 1. *We should open a forum for discussion of ethics and sexual harassment on the UBC node of the Internet.*

Some of the best discussion of our problem I am aware of takes place on the Internet itself. For example, I found the discussion of President Strangway's letter of 30 July `92 in ubc.general to be quite enlightening.[11] And the Computer and Academic Freedom News (in alt.censorship, ironically often one of the first groups to be censored) and the associated archives at the Electronic Freedom Foundation (ftp.eff.org) to be rich sources of primary materials, such as a transcript of the seminal CITY-TV broadcast and full text of various universities' policies in this area.

I further propose that this be a professionally moderated newsgroup, staffed by someone with training in ethics and CMC. Comp.risks, under Peter C. Newman's extraordinary fine editorship, is a model that we might aim.

---

[11] Even though I was visiting UCLA at the time, I could read netnews remotely here. This should remind us that the Internet is technologically biased against effective censorship.

Proposal 2. *Open access to the Internet to a larger subset of the university community.*

At present, access is severely restricted. Even the privileged find access difficult. (My grants can't seem to buy me ethernet connectivity!) But it is a fairly obvious truism of moral sociology that the mores of a community excluding most humanists and social scientists will be less humanized and civil thereby. (A motto: Humanize the Internet -- Wire the Arts Faculty.)

Proposal 3. *Moral support for users*

Open access is not enough. We need to support users in the use of the critical and filtering tools that make CMC the progressive ethical instrument that I claim it might be.[12] Users need to know how to filter out offensive messages[13] and to answer postings appropriately. Perhaps they need anonymity or pseudonymity. I would also suggest that they need continuing network addresses to foster responsibility and community.

Proposal 4. *Encourage A Variety of Experiments*

Not everyone uses published media, mail, telephone, radio, or television in the same way. Surely we need to experiment even more with a less conventionally settled medium like CMC. Therefore it would be a mistake to apply restrictive policies at too broad a level. There are relevant differences between a widely available server in a teaching department and a research machine in a research group. Lumping these all together as "university computing equipment" seems to be a mistake that will curtail interesting experimentation.[14]

Conclusion

In sum, I propose that we deal with our problem as befits a university, that is by addressing it as a serious intellectual problem that it is. Further, I hope that we take this problem as an intellectual challenge rather than a purely political problem, and try to deal with it by the means that we deploy best: intelligence, discussion, trial and error mediated by open comment on results, playfulness and rigor. U.B.C., with its tradition of technological

---

[12] The Report of the Advisory Committee on Network News, The University of Waterloo, May 30, 1991, is a model.

[13] CMC usually provides caller-ID automatically but the filter built into our mailer is neither supported nor currently working, so far as my assistants can determine.

[14] Policies that put one political agency in charge of the means of communication have not historically been friendly to open inquiry and communication, because, even in the best case, that agency becomes responsible for what should, properly, be a matter of dis-trituted responsible, and acts more restrictively than would the varied set of distributed responsible agents/

leadership, strong humanities and social sciences, and commitment to applied ethics, should be a leader in the task of civilizing this technological frontier.[15]

References

Danielson (1991) Review of M. David Ermann, Mary Williams and Claudio Gutierrez, eds. Computers, Ethics & Society. *Canadian Philosophical Reviews.*

Danielson (1992) *Artificial Morality*. London: Routledge.

Danielson (in press) Personal Responsibility, in T. Hurka and H. Coward, ed, *The Ethics of Global Warming.*

Dunlop (1991) and Kling, ed. *Computerization and Controversy*, San Diego: Academic Press.

Stewart (1986) *Readings in Social and Political Philosophy* New York: Oxford University Press.

[15] I discuss the ethics of a frontier in (Danielson, in press).

• **APPENDIX D**
Submission to Task Force by Dr. Richard Rosenberg, Computer Science

Free Speech, Pornography, Sexual Harassment, and Electronic Networks

Richard S. Rosenberg
Department of Computer Science
University of British Columbia
Vancouver, B.C. V6T 1Z2
E-mail: rosen@cs.ubc.ca
Tel: (604) 822-4142

A Presentation to the Task Force on Appropriate Use of Information Technology
October 23, 1992

A. Basic Principles

- Do not treat electronic media differently than print media, or traditional bulletin boards, merely because they can be more easily controlled.
- Do not censor: Use sexual harassment guidelines.
- Issues will proliferate beyond the ability of organizations to control them by rigid policies.
- Organizations do have a responsibility with respect to the uses and misuses of their facilities. However, they should not use cost of services as an excuse to censor and limit access.
- Occasional offensive postings do not deter from the benefits of electronic networks.
- Trust and educate people to be responsible.

B. Relevant Issues

1. Networks and Electronic Media

- Electronic Media vs. Print Media.
- Information Networks - Current State, Importance, Growth.
- Networks Are International - There are no universal standards of good taste. What are community standards? [C3, C13]
- Usenet - Rapid growth in number of newsgroups, readership, topics, and services provided. [C4, C11]
- Benefits of Networks in the Information Age: Access for millions, open marketplace of ideas, anonymity of users, instantaneous access to a variety of information sources, multimedia, online books, graphics, and sound. [E1, E2]
- Responsibility of Information Carriers and Providers - networks (Internet, Bitnet, Cdnet), videotex (Prodigy, Compuserv, The Source), local carriers (e.g. Universities, BBS's, Libraries, Bookstores, Videostores). [E4, F2]

2. Pornography and Censorship

- Impact of Pornography on Shaping Attitudes and Behaviour. [D2, D3]

- Access by Young People - An issue to be explored by concerned off-campus institutions as well. [C8]
- Free Speech vs. Censorship - U.S. First Amendment and Supreme Court decisions, Canadian Charter of Rights and Supreme Court decisions. [C6, D1]
- Disagreement Within the Feminist Community on Censorship. [C14]
- Censors and Censorship Criteria - Which groups to monitor and on what basis: It's not just alt.sex.* and alt.binaries.pictures.* (Currently, Oct. 5, 609 alt groups. 9 new ones on Oct.13 including alt.comedy.british and alt.comedy.lnh) [C1, C2, C5, C7, F3]
- Sexual Harassment, or Threatening, Offensive Behaviour - This is the best route to explore to deal with the present problems. [C10, C12]

3. Ethics and Responsibility

- Ethical Uses of Computers and Computer Networks - Require reading of, and signature on, official use forms and regular reminders and discussion of what constitutes acceptable computer use. Removal or revoking of access privileges may be an appropriate non-legal measure. Guidelines should be clear about what constitutes non-acceptable use, e.g., private profit-making activities. However reading or viewing available material is not *a priori* an offense. [C9, C15, F1]
- Organizational vs. Individual Responsibility - Organizational: Given that universities must pay for computer and telecommunications hardware, software, and employees to support networks, they clearly have a voice with respect to usage. Individual: Use of killfiles to control offensive postings from identified individuals; headers and explicit warnings permit skipping possible offensive postings by subscribers; encrypted messages convention. [E4, E3, F4]

4. Other Issues

- Other Network and Computer Systems Issues: Offensive E-Mail; obscene .plan files and file names; racist messages: anti-Black, anti-semitic, anti Arab, revisionist history; fascist political groups; copyright violations; software piracy; "crack" programs that can perform the illegal activity of discovering passwords.

C. Information Gleaned From the Net

1. History of Alt . Groups - Everything is anecdotal but it appears that the System Administrators (SA) of the Net "backbone" were apprehensive about permitting clearly non-technical and non-moderated groups to be included. A group of women voted to create comp.women and supposedly this action created so much discord among among the SA's that eventually the backbone broke up and leaving the present distributed, and weak, administration. It also seems that an additional component was what do with alt.sex and alt.drugs among others. As one person noted: (Chris Lewis, alt.comp.acad-freedom.talk, Feb. 27, 1992) "The prevalence of such groups as 'censorship', 'civil-liberty', 'acad-freedom' and the like in alt is because the people who tend to want to create such groups think that having to vote for a news group is fascist."

2. In a note from Switzerland (10, Article 1 of alt.comp.acad-freedom.news, April 17, 1992), the system manager at Ecole Polytechnique Federale de Lausanne, presents a classification of newsgroups into 4 categories:

   Category 1: Required newsgroups (exceptions: see Category 3) bionet.*, bit.*, ch.*, comp.*, etc.

Category 2: Optional newsgroups (exceptions: see Category 3) alt.*, clari.*, misc.*, rec.*, soc.*, talk.*, etc.

Category 3: Prohibited newsgroups: alt.binaries.pictures.erotica, alt.drugs, alt.fax.bondage, alt.personals.bondage, alt.politics.homosexuality, alt.psychoactives, alt.satanism, alt.sex* (6 groups), alt.sexual.abuse.recovery, alt.tasteless, bit.listserv.gaynet, de.talk.sex, clari.news.group.gays, clari.news.law.crime.sex, clari.news.law.crime.violent, clari.news.law.drugs, clari.news.sex, clari.news.terrorism, rec.arts.erotica, soc.bi, soc.motss, sub.sex, talk.abortion, talk.bizarre, talk.politics.drugs, talk.politics.guns, talk.rape [my underlining.]

Category 4: Not available newsgroups: eunet.*

Further, he notes, "The situation is such that I have users who use news servers in the US (Hawai! [sic]) and Germany (over slow and saturated links!) and who knows where else to read the newsgroups they want.)

3. From Article 2 of above, (a person in Ireland, where abortions are illegal), "The computer/censorship issue is related to the fact that only crosspostings to the group talk.abortion appear here. If a posting to such a group has information on how to procure an abortion, are we any more liable than a library with an English telephone directory which has the phone number of an abortion clinic?."

4. From (21, Article 3, alt.comp.acad-freedom.news) the following statement of Chip Salzenberg, in a monthly article in news.announce.users, with the title, "What is Usenet?" we read the following:

> "Usenet is not an academic network. It is no surprise that many Usenet sites are universities, research labs or other academic institutions. Usenet originated with a link between two universities, and the exchange of ideas and information is what such institutions are all about. But the passage of years has changed Usenet's character. Today, by plain count, most Usenet sites are commercial entities.
>
> Property rights being what they are, there is no higher authority on Usenet than the people who own the machines on which Usenet traffic is carried. If the owner of the machine you use says, "We will not carry alt.sex on this machine," and you are not happy with that order, you have no Usenet recourse. What can we outsiders do, after all?"

5. This is a reposting from University of Waterloo, October 3, 1991 (23, Article 7, June 25, 1992, as above). In May 1991, a committee appointed to study the question of newsgroup availability reported, "what you would expect them to report - that is to paraphrase, a University administration should not make non-financial decisions about what people can and can't read on campus. They recommended restoration of all banned newsgroups." These included rec.humor.funny, alt.sex.bondage and others. Note that John McCarthy of Stanford spoke at Waterloo and also played an important role in reversing a short-lived ban at Stanford.

6. From Article 10, above, Laurence Tribe, a distinguished Harvard Law professor and a leading constitutional scholar, has proposed a Constitutional Amendment:

> "This Constitution's protections for the freedoms of speech, press, petition and assembly, and its protections against unreasonable searches and seizures and the

deprivation of life, liberty or property without due process of law, should be construed as fully applicable without regard to the technological method or medium through which information content is generated, stored, altered, transmitted or controlled."

7. (29, Article 10, July 28, 1992, alt.comp.acad-freedom.news) David Sadleir, University of Toronto, vice-president, computing and communications, is quoted in an article in The Bulletin, June 8, 1992, by Karina Dahlin as follows: "I am not a censor." His view is that if a recipient has to actively select information, there is no need for the U of T to take action. If, on the other hand, the messages are flashed across the screen without user consent, his response would be "very aggressive" regardless of the content.

8. (35, Article 11, September 8, 1992, alt.comp.acad-freedom.news) The following is taken from Virginia's Public Education Network (PEN) Acceptable Use Policy for K-12 classroom, teachers, students, parents, and school administrators:

   It is therefore imperative that members conduct themselves in a responsible, decent, ethical, and polite manner while using the network.

   Each individual's judgment of appropriate conduct must be relied upon. To assist in such judgment, the following general guidelines are offered:

   I. Any use of VIRGINIA'S PEN for illegal, inappropriate, or obscene purposes, or in support of such activities, is prohibited. . . . Obscene activities shall be defined as a violation of generally accepted social standards for use of a publicly-owned and operated communication vehicle.

   From the Guidelines for Student Accounts on Virginia's PEN:

   5. Generally, students are not permitted to enter professional Virginia's PEN or Usenet discussion groups. Under certain conditions, posting privileges to specific newsgroups may be granted.

   From the Public School Student Application for VIRGINIA'S PEN Account:
   SPONSORING PARENT or GUARDIAN (Required)

   I have read the Acceptable Use Policy and Student Guidelines for VIRGINIA'S PEN. I understand that although administrators of the VIRGINIA'S PEN network have taken reasonable precautions to ensure that controversial material is eliminated on Virginia's Education Network, I will monitor my child's daily use of the VIRGINIA'S PEN and his/her potential access to the world-wide Internet, and will accept full responsibility for supervision in that regard if and when my child's use is not in a school setting. I hereby give my permission to issue an account for my child and certify that the information contained on this form is correct.

9. One user's view of the banning of alt.sex.* newsgroups: (July 13, 1992, alt.censorship, alt.sex)
   In response to a posting that taxpayer's money should not be spent to transmit and store "illegal material" over Usenet, one reader posts the following:

A quick look at the Arbiton stats'll show that alt.sex is one of the most popular groups on usenet. In other words, we have met the perverts, and we are them.

What does that mean? A waste of money? hardly, son. A huge savings, instead. Know what'd happen to my site's disk space if alt.sex was killed, assuming that I'm the only person reading it? Nothing. I could, can, and will find a way to gate the newsfeed into my e-mail. . . .

10. From the 199 -1993 Guidelines for use of Campus and Network Computing Resources at Princeton University (47, Article 7, October 6, 1992, alt.comp.acad-freedom.news, also on comp.admin.policy , September 8, 1992):

    Those who avail themselves of the campus and network computing resources are required to behave in their use of the technology, in a manner consistent with the University's code of conduct. As stated in Princeton's University Rights, Rules, Responsibilities:

    "Respect for the rights, privileges, and sensibilities of each other is essential in preserving the spirit of community at Princeton. Actions which make the atmosphere intimidating, threatening, or hostile to individuals are therefore regarded as serious offenses. Abusive or harassing behavior, verbal or physical, which demeans, intimidates, threatens, or injures another because of his or her personal characteristics or beliefs is subject to University disciplinary sanctions . . . ."

    [A list of the responsibilities users accept if they chose to use a University computing resource or the network access which the University provides.]

    . . . .

    6. You must be sensitive to the public nature of shared facilities, and take care not to display on screens in such locations images, sounds or messages which could create an atmosphere of discomfort or harassment for others. You must also refrain from transmitting to others in any location inappropriate images, sounds or messages which might reasonably be considered harassing.

    . . . .

    11. Messages, sentiments, and declarations sent as electronic mail or sent as electronic postings must meet the same standards for distribution or display as if they were tangible documents or instruments. You are free to publish your opinions, but they must be clearly and accurately identified as coming from you, or, if you are acting as the authorized agent of a group recognized by the University, as coming from the group you are authorized to represent. Attempts to alter the "From" line or other attribution of origin in electronic mail, messages, or postings, will be considered transgressions of University rules.

11. USENET Readership Reports for June 92 (Article 3724, July 3, 1992, alt.comp.acad-freedom.talk), July 92 (Article 3944, August 2, 1992, ibid) , and September 92 (Article 4550, October 3, 1992, ibid):

Month	Newsgroup	Readership	% of sites	Cost ratio	%Share
June	Misc.jobs.offered	280,000	83	0.01	12.2
	Misc.forsale	250,000	83	0.01	10.5
	alt.sex	220,000	67	0.04	9.4

	rec.humor.funny	220,000	81	0.00	9.2
	. . . .				
	alt.comp.acad-freed'm.t	27,000	57	0.03	1.2
July	Misc.jobs.offered	300,000	84	0.01	12
	Misc.forsale	250,000	83	0.01	10.5
	News.announce.new's	240,000	89	0.00	9.8
	rec.humor.funny	220,000	81	0.00	9.0
	alt.sex	220,000	67	0.04	8.9
	. . . .				
	alt.comp.acad-freed'm.t	29,000	57	0.02	1.2
August	Misc.jobs.offered	160,000	83	0.02	11.5
	Misc.forsale	160,000	82	0.02	11.1
	News.announce.new's	150,000	89	0.00	10.3
	alt.sex	120,000	68	0.07	8.4
	news.answers	120,000	84	0.00	8.4
	rec.humor.funny	120,000	81	0.00	8.2
	. . . .				
	alt.comp.acad-freed'm.t	14,000	59	0.04	1.0

Readership: Estimated total number of people who read the group, worldwide.
% of sites: Propagation: how many sites receive this group at all.
Cost ratio: $US/month/reader.
%Share: % of newsreaders who read this group.

12. At least one posting from Carl Kadie, of the Electronic Frontier Foundation and a staunch defender of absolute freedom of speech, is necessary. Mr. Kadie maintains extensive archives of court decisions, legal opinions, psychological papers on the impact of pornography on male behaviour and perceptions of women, university codes of behaviour, etc. These are made available by ftp or e-mail. In article 4641, October 9, 1992, alt.comp.acad-freedom.talk, Mr. Kadie responds to the following, self-posed question:

    What should sys admins do about nude pictures and displays of nude pictures in public terminal rooms? Is a special rule banning such pictures and/or displays needed?

    The problem is not the pictures themselves but rather their display. By way of analogy, your library likely contains thousands of nude photos (many academic libraries, for example, subscribe to *Playboy*). The existence of these pictures is not harassment because no one is compelled to keep looking at the pictures.

    If at the same time *Playboy* pictures, however, were *displayed* in a university office or lab where employees or students must work, the person displaying the pictures might be guilty of sexually harassing a person in the office or lab. Likewise the *display* of nude pictures in a public terminal room (or university office) might be found to be sexual harassment.

    . . . .

[So what can you do? Basically, use available "sexual harassment" policy after the fact. Of course notices can be posted in appropriate locations reminding people of this policy.]

13. Australian action (Article 4671, October 11, 1992, alt.comp.acad-freedom.talk): " About two years ago, AARNet (Australian Academic Research Network) ceased to receive alt.sex* and alt.drugs, and although some of those groups have at times come in on alternate paths, the official ban is still in place. Please note that this is not a case of censorship based on content, but a matter of economics. At that time the Aus-US satellite link was running at saturation point and as a result, according to kre@cs.mu.oz.au (Robert Elz).

    [What about now?]
    "Despite upgrades within the last two years, the AARNet Business Plan of September 1992 described the situation as follows: 'this link is now (August 1992) running at 95% utilization levels for 4-6 hours per working day, and it is anticipated that critical congestion and subsequent performance collapse will be experienced well before the end of 1992.' I certainly agree that it is a pity we can't read these groups, but I do agree that if a choice has to be made then non-academic traffic should be sacrificed in order to ensure that academic traffic can be carried." (Elizabeth M. Reid)

14. Various postings from "Feminists Against Censorship" and "Women Against Censorship" are available in Article 27388, August 8, 1992, alt.activism and Article 11055, August 31, 1992, alt.censorship.

15. Without including the policies of a wide sampling of universities (presumably already available to the Task Force), it may be useful to conclude this section with the following items taken from 48, October 19, 1992, alt.comp.acad-freedom.news:

    (i) From Article 8, Geoff Bronner, Dartmouth College responds to some previously posted questions about computing policy: Dartmouth receives all newsgroups. rec, news, soc, alt, etc. We also gateway a number of listserv mailing lists through news as well. If the general alt* traffic isn't enough Dartmouth affiliates can use local dartmouth.alt.* groups as well. Here it appears to be a departmental decision made by Computing Services. But if a major problem developed the Dean's or Trustee's [sic] might get involved. It has never really happened. A few years ago there was a short period where freshman were printing questionable things to the public printers but Computing Services decided that they would not get into the censorship business. After a while the novelty wore off and that was that. [my underlining] In my opinion alt.* groups and similar things can be a source of problems but nothing really serious. I don't really object when a site rejects alt.* traffic to try and reduce costs, that's reasonable. But if they can afford a full news feed they should allow it.

    (ii) From Article 9, Marshall G. Flax, Princeton University, writes. If the problem is displaying "offensive" images in public computer clusters, then you might want to start a policy that people should view images only in private. If you have a problem with people printing "offensive" images on laserprinters, then you might want to restrict printing to text and academically-related graphics. There's no need to restrict what people read privately or store in their account as long as you make clear to users that they should behave politely in public.

D. Other Sources on Pornography and Free Speech

1. Ronald Dworkin, "The Coming Battles over Free Speech, " *The New York Review of Books*, June 11, 1992, pp. 55 - 64. (Mr. Dworkin is Professor of Jurisprudence at Oxford University and Professor of Law at New York University. He is a staunch defender of free speech and is critical of the MacKinnon-Dworkin approach. He is also very critical of a recent decision by the Supreme Court of Canada which argued that "the proliferation of materials which seriously offend the values fundamental to our society is a substantial concern which justifies restricting the otherwise full exercise of the freedom of expression." Dworkin: "That is an amazing statement. It is the central , defining, premise of freedom of speech that the offensiveness of ideas, or the challenge they offer to traditional ideas, cannot be a valid reason for censorship; once that premise is abandoned it is difficult to see what free speech means." (p. 61)

2. Robert M. Baird and Stuart E. Rosenbaum (Eds.). *Pornography: Private Right or Public Menace* (Buffalo, NY: Prometheus Books), 1991. (A valuable collection representing a variety of viewpoints by very articulate and persuading writers including Susan Brownmiller, Andrea Dworkin, Ronald Dworkin, Gloria Steinem, and George F. Will).

3. John Stoltenberg. *Refusing to Be a Man*. (Portland, Oregon: Breitenbush Books, Inc.), 1989. Mr. Stoltenberg strongly supports the Catherine MacKinnon - Andrea Dworkin view that anti-pornography legislation should be based on a civil-rights approach (as a civil law with pornography defined according to harm and claim based on injury to the victim) rather than on obscenity law (as a criminal law with obscenity defined by arousal as a crime based on offense to public morals).

E. Other Sources on Networks

1. John D. H. Downing. Computers for Political Change: PeaceNet and Public Data Access. *Journal of Communications* 39(3), Summer 1989, pp. 154-162. Abstract: By "constructing an alternative public realm," two computer communications projects - one devoted to peace issues, the other to making U.S. government information more broadly available - demonstrate the potential of new technology for grass-roots political movements. This is just one of many examples of the importance of networks, in this instance for political action.

   [Surely as such systems continue to grow and diversify, care must be taken not to impose restrictions that prevent them from reaching their full potential.]

2. Eric A. Abbott. The Electronic Farmers' marketplace: New Technologies and Agricultural Information. *Journal of Communication* 39(3), Summer 1989, pp. 124-136. Another example.

3. Carol C. Gould (Ed.). *The Information Web: Ethical and Social Implications of Computer Networking*. (Boulder, CO: Westview Press), 1989. A collection of papers by some well known "computer - ethicists" including Deborah G. Johnson, James H. Moor, John W. Snapper, and Donn B. Parker. This book is interesting in the present context for what it does not include. Except for one relatively brief comment by Deborah Johnson, there is

nothing included about pornography, free speech, or censorship. There is a great deal about privacy, ownership, computer conferences, access, and cooperation. For example the editor, Carol Gould, concludes her introductory chapter with a proposal for a general principal of network ethics: "Maximum sharing of information and maximally equal access compatible with the preservation of the value of privacy, as protected by the requirement of free and informed consent." What has happened in the past three years to suddenly elevate the issue of pornography to such a level of urgency and publicity?

In Deborah Johnson's chapter she presents three cases for purposes of discussion. One case is taken from a collection of scenarios developed by Donn Parker and associates at SRI International (Donn B. Parker, Susan Swope, Bruce N. Baker. *Ethical Conflicts in Information and Computer Science, Technology, and Business*. (Wellesley, MA: QED Information Sciences, Inc.), 1990.) In this collection, some fifty-four scenarios were presented to a panel of experts for discussion. As far as I can tell only the one selected by Ms. Johnson bears any relation to the issue at hand. The scenario and associated discussion will be include at the end of this document. (Note that since Parker et al.'s study was funded by the U.S. government, the results can be copied without copyright violation.) Let me quote from Ms. Johnson's comments about this scenario:

> "The student who ultimately got in trouble with his university administration seemed to be treating the forum as public. That is, he did not bring the pornographic material into the forum itself, which would have, in some sense, forced students to see it who did not choose to do so. Rather, he informed students of it availability so that only those who wanted to see what they knew was pornographic, would see it. This approach seems to agree precisely with how we handle noncomputerized pornographic literature. We do not allow public displays or advertisements or distribution by mail to consumers who did not request the literature, but we do allow those who so choose to have access. . ."
>
> There is more and Ms. Johnson does grant universities the right to censor information on campuses if they believe it is the right thing to do.

4. The July/August issue of *EDUCOM Review*, Vol. 27, Number 4, is devoted to the theme Legal, Social, and Ethical Issues Operating in the '90s. EDUCOM is a nonprofit consortium of approximately 600 colleges and universities with 85 corporate associates. Four papers appeared under the advertised theme:
   (i) Sally Webster. Dispatches from the Front Line: Computer Ethics War Stories. pp. 18-21.
   (ii) Virginia E. Rezmierski. Ethical Dilemmas in Informational Technology Use: Opportunity Bumps on the Road to Civilization. pp. 22-26.
   (iii) Susan F. Stager. Computer Ethics Violations: More Questions Than Answers. pp. 27-30.
   (iv) Marilyn A. Van Bergen. Copyright Law, Fair use, and Multimedia. pp. 31-34.

   Webster presents one relevant case: "One of your staff tells you that a young male student, X, has been receiving harassing mail messages from another user threatening to expose that he's gay, that his e-mail account has been broken into, and that sexual solicitations have been sent to others. After presenting other cases, Ms. Webster notes, "The time has come to demystify 'computer abuses,' to strip away from the act the tool with which it is committed, and to concentrate on the abusers and what they have done to

each other. 'Computer abuses' should carry the same sanctions and consequences as the same misbehaviors committed with more ordinary tools." This position is consistent with the first of my basic principles.

Dr. Rezmierski includes the following among several incidents mentioned as examples of what has been happening recently across campuses: "(a) A student collects hundreds of files of pornography. Using the network, the files' availability is advertised, complete with cost. (b) A staff member allows her teenage child to help read electronic mail. Instead of just reading, the teen decides to scare people and broadcasts a threatening message to specific international students on campus." She discusses an educational process developed at the University of Michigan to deal with such problems.

Dr. Stager includes the results of a survey of 63 computer center directors on incidents occurring at their institutions over a 12 month period as well as their views of a number of statements dealing with many of the issues discussed above. These results are included in this report. She also makes the following statement on Freedom of Speech on Computer Bulletin Boards:

> "One of the most difficult management questions is about computer bulletin boards. Should Computer Centers take on the task of monitoring bulletin boards?
>
> It has been established that students at public institutions have protected, First Amendment constitutional rights to free expression. Institutions have the right to reasonably regulate expression as to its time, place, and manner so as to avoid disruption of the educational process and to avoid placing persons or property in danger. However, it remains unclear to many computer center directors whether this right of expression extends to university-operated computer bulletin boards. Many are hoping that Cubby *v.* Compuserv, Inc. will provide some guidance on whether the university can be held liable for the contents of these bulletin boards.
>
> Central to the issue of regulation of expression is the issue of obscenity. Of those directors surveyed, 68 percent agreed or strongly agreed that university-operated bulletin boards are subject to restrictions when material is clearly libelous or obscene. However, only 44 percent of those surveyed stated they have a general understanding of what their campus considers obscene."

In a letter to the Editor in this same issue, Marcia Lin, Director of the Instructional Technology Program and professor of mathematics, science, and technology education at the University of California at Berkeley expresses her concern about barriers to women in computing. Her final point is given as follows:

> "Fifth, resort to respect. For example, recently, computers shipped with background screens of nude women were installed in a laboratory at the university. Females felt degraded, but males argued that removing the screens would threaten their right to free expression. Eventually, a standard of mutual respect was established, and all the screens were deleted. I call on all of us to take action against these barriers as well as to identify and address other barriers to equity in computing."

One final excerpt from this magazine will be included. CNI is the Coalition for Networked Information, a group concerned about networks and management policy for networks, including NREN (National Research and Education Network). The Working Group on Legislation, Codes, Policies, and Practices, one of eight CNI working groups, identified a number of issues as top agenda items, including the following:

• Providing model principles, policies, and practices to protect freedom of expression in networked environments, especially when asocial behavior exists, by asserting and testing the hypothesis that the issue is to promote an environment that favors freedom of speech rather than one that restricts distasteful expression.

F. Other

1. Scenario IV.8 from Parker et al. (1990, pp. 121-124, 218-219.
2. Tables 1 and 2, from Stager (1992, pp. 28-29).
3. Article 4753 of alt.comp.acad-freedom.talk, October 22, 1992.
4. ACM Code of Ethics and Professionalism, Draft, February 12, 1992. *Communications of the ACM* 35(5), May 1992, pp. 94-99.

• APPENDIX E
Other submissions to Task Force

(not included here because of their bulk)

• APPENDIX F
UBC Sexual Harassment Policy

PART I DEFINITIONS

1.01 "Sexual Harassment" includes comment or conduct of a sexual nature, including sexual advances, requests for sexual favours, suggestive comments or gestures, or physical contact when any one or more of the following conditions are satisfied:

(1) the conduct is engaged in or the comment is made by a person who knows or who ought reasonably to know that the conduct or comment is unwanted or unwelcome;

(2) the comment or conduct is accompanied by a reward, or the express or implied promise of a reward, for compliance;

(3) the conduct or comment is accompanied by reprisal, or an express or implied threat of reprisal, for refusal to comply;

(4) the conduct or the comment is accompanied by the actual denial of opportunity or the express or implied threat of the denial of opportunity, for failure to comply;

(5) the conduct or the comment is intended to, or has the effect of, creating an intimidating, hostile or offensive environment.

1.02 "Complaint" includes a complaint respecting:

(1) sexual harassment;
(2) retaliation for the lodging of a complaint;
(3) breach of an undertaking as to future conduct.

PART II: APPLICATION OF THE POLICY AND PROCEDURES

2.01 (1) The policy and procedures apply in all cases where there is a sufficient nexus between the conduct or comment in issue and the functioning of the University.

(2) There is a sufficient nexus for the purposes of subclause (1) if the conduct or comment interferes, or could reasonably be regarded as being capable of interfering, with:

(a) the proper functioning of the University; or
(b) an individual's dignity or privacy in respect of matters connected with the individual's work or study at, or other relationship with the University.

2.02 The procedures for the imposition of discipline are inapplicable to the extent that they may be incompatible with any express provisions to the contrary in existing agreements between the University and its faculty or staff.

2.03 A complaint made under these procedures can be pursued, even though there are contemporaneous court or other proceedings related to the incident or incidents in question, unless:

(1) it would be unlawful to pursue the complaint; or

(2) the President's Permanent Advisory Committee, upon application, orders that the complaint be stayed.

2.04 All persons involved in the handling of a complaint shall hold in the strictest confidence all information of which they become aware.

2.05 The President's Permanent Advisory Committee may, on application and submissions from interested parties, vary in any given case any of the time limitations or any minor procedural steps provided for in these rules if the committee is of the opinion that it is desirable to make the variation and that to do so will not be unfair to any of the persons involved.

PART III: COMPLAINTS

3.01 A person who believes that he or she has been subjected to comment or conduct falling within the definition of a complaint in section 1.02 ought to discuss the matter with a sexual harassment officer.

3.02 The sexual harassment officer shall provide the complainant with advice and assistance on how to deal with the situation (including referring the complainant to the appropriate support or professional services), on the policy and procedures, on the apparent validity or seriousness of the complaint, and on what action might be taken.

3.03 A complaint may not be pursued by the complainant unless the complaint is specified in writing in reasonable detail and lodged with a sexual harassment officer by at the latest one calendar year after the event, or in the case of a series of events, the last event in the series, on which the complaint is based.

3.04 Subject to sections 5.01 and 5.04, a decision to pursue a complaint under these rules rests with the complainant, and having made a complaint the complainant may withdraw it at any time.

3.05 Events that take place after the giving of written notice may, without the filing of a further complaint but with due notice to the complainant or respondent, be the subject of mediation, investigation or formal hearing.

3.06 If a written complaint is not lodged within the prescribed time limit, the sexual harassment office shall seal all records that may have been compiled, and no person shall have access to those records, unless with the consent of the President's Permanent Advisory Committee. The sexual harassment office may however publish statistical information as to the number of complaints made and information as to the general types of complaints, including information on whether the complaints were made by or against faculty, staff or students.

3.07 If a written complaint is lodged within the prescribed time limit, the sexual harassment officers shall, within five working days of receiving the complaint:

(1) deliver to the respondent a copy of the complaint and a copy of the policy and procedures, and shall explain the procedures to the respondent;

(2) advise the respondent of the desirability of obtaining independent advice, and that, if the respondent so wishes, the Chairperson of the President's Permanent Advisory Committee will nominate a member of the committee to provide advice to the respondent;

(3) deliver a copy of the complaint to the Dean of the Faculty or the Head of the non-academic unit to which the respondent is attached.

3.08 (1) The respondent may, if he or she wishes, respond in writing to the complaint.

(2) Any response in writing under sub-section (1) shall be delivered to a sexual harassment officer within 15 working days of the receipt by the respondent of the written complaint of the complainant.

(3) Within five working days of receiving a written response from the respondent the sexual harassment officer shall deliver a copy of that response to the complainant.

(4) The sexual harassment officer shall also deliver a copy of any response to the Dean of the Faculty or the Head of the non-academic unit to which the respondent is attached.

PART IV: MEDIATION

4.01 (1) Within 30 working days of the delivery of the complaint to the respondent, either the complainant or the respondent may notify the sexual harassment officer in writing that he or she is prepared to resolve the matters in dispute through mediation.

(2) If no such notice is given to the sexual harassment officer then it shall be presumed that mediation will not take place.

4.02 On receipt of notice in writing from either the complainant or the respondent that he or she is willing to consider mediation, the sexual harassment officer shall immediately deliver to the chairperson of the mediation panel:

(1) a copy of the complaint by the complainant;
(2) a copy of the response, if any, of the respondent;
(3) a copy of the written notice or notices indicating a willingness to consider mediation.

4.03 (1) The chairperson of the mediation panel shall, on receiving the material referred to in section 4.02, enter into consultations with the complainant and the respondent in an attempt to secure their agreement to a mediator and the terms of reference for the mediation.

(2) An agreement on a mediator and on the terms of reference for mediation shall be reduced to writing and signed by the complainant, the respondent and the chairperson of the mediation panel.

(3) The mediator shall be responsible for arranging the mediation.

(4) If an agreement in writing is not arrived at within 10 working days of the receipt by the chairperson of the mediation panel of the material referred to in section 4.02, it shall be presumed that mediation will not take place.

4.04 At the mediation a complainant or a respondent may each be accompanied by a person of his or her choice.

4.05 (1) The mediation shall be completed with 15 working days of the signing of the agreement referred to in section 4.03(2). If it is not completed within that period, the mediation shall be presumed to have failed.

(2) If the mediation fails, the mediator shall notify in writing the parties, the chairperson of the mediation panel, the sexual harassment officer, and the administrative head of the faculty or unit to which the respondent is attached.

4.06 If mediation is successful, the agreement arrived at between the complainant and the respondent shall be reduced to writing, signed by the complainant and the respondent and counter-signed by the mediator. If the agreement contains undertakings as to future conduct on the part of either the complainant or the respondent, the agreement shall also be signed by a representative of the University.

4.07 A copy of any agreement reached under section 4.06 shall be provided to each of the parties, to the sexual harassment officer, and to the administrative head of the faculty or unit to which the respondent is attached.

4.08 (1) Whether or not the mediation is successful, and subject to section 4.07, all records and notes created in the course of the mediation and which are in the control of the mediator shall be destroyed.

(2) No person shall give evidence or introduce documents during any subsequent proceedings under these procedures or in any other University proceeding where that evidence or those documents would disclose that any person had agreed or refused to agree to mediation or, if mediation occurred, what took place during the mediation.

PART V: INVESTIGATION

5.01 (1) If the complainant or the respondent does not agree to mediation, or if mediation is unsuccessful, the complainant or the University may notify the President's Permanent Advisory Committee that he, she or it wishes the complaint to be investigated. Such a notification shall be in writing and shall be delivered to the chairperson of the President's Permanent Advisory Committee within five working days of the date on which it is known mediation is not to take place or on which mediation failed. If notification is not received within this period, it shall be presumed that neither the complainant nor the University wishes to pursue the matter further.

5.02 Within five working days of receiving the request for an investigation, the chairperson of the President's Permanent Advisory Committee shall appoint two persons (one of whom may be the chairperson of the Committee) to conduct an investigation.

5.03 The investigating committee should make every effort to interview the complainant, the respondent, and such other persons as it sees fit, and to examine any documents it may think relevant, and it shall report its findings to the President's Permanent Advisory Committee within 15 working days of the date of its appointment.

5.04 (1) The President's Permanent Advisory Committee shall consider the report and shall decide, within five working days of receiving it, if there is any evidence which would warrant the complaint being referred to a Hearing Committee; in which case the University shall be obliged to initiate proceedings before a Hearing Committee;

(2) If the President's Permanent Advisory Committee is not of the opinion that there is any evidence which would justify a hearing, the complainant may nonetheless initiate proceedings before a Hearing Committee.

5.05 Within five working days of reaching its decision, the President's Permanent Advisory Committee shall inform the following persons in writing of the decision:

(1) the complainant;
(2) the respondent;
(3) the sexual harassment officer;
(4) the appropriate administrative officers; and
(5) the chairperson of the Hearing Panel.

5.06 When the President's Permanent Advisory Committee decides that a hearing is not warranted, the complainant shall, within 10 working days of receiving the decision of the Committee, notify the chairperson of the Hearing Panel in writing if it is his or her intention to initiate proceedings before a Hearing Committee.

PART VI: HEARING

6.01 The President, with the advice of the President's Permanent Advisory Committee, shall nominate a Hearing Panel and shall designate one of its members as the chairperson of the panel.

6.02 On being notified that a hearing is to take place, the chairperson of the Hearing Panel shall:

(1) appoint three persons as a Hearing Committee, of whom one may be the chairperson of the Hearing Panel and of whom one shall be a non-University member of the Hearing Panel;

(2) designate the non-University member the chairperson of the Hearing Panel;

(3) within 10 working days of being informed that a hearing is to take place, notify the complainant, the respondent and the University of the composition of the Hearing Committee.

6.03 Subject to a ruling to the contrary by a Hearing Committee, where two or more complaints have been lodged against the same respondent, the complaints shall all be dealt with at a single hearing.

6.04 (1) Challenges for cause to the composition of the Hearing Committee may be made in writing to the chairperson of the Hearing Panel within seven working days of the receipt of notification of the composition of the Committee.

(2) Challenges for cause may be made at a later date to the chairperson of the Hearing Panel, or, at the commencement of the hearing, to the Hearing Committee only if the information on which the challenge is based was not available in order to make a timely challenge under sub-section (1).

(3) The chairperson of the Hearing Panel, or the Hearing Committee, shall make a ruling in writing on any challenge for cause. If the challenge for cause is upheld the chairperson of the Hearing Panel shall appoint a replacement member of the Hearing Committee.

6.05 The chairperson of the Hearing Committee shall make arrangements for the hearing with all reasonable dispatch.

6.06 (1) Where the University initiates the hearing, the parties shall be the University and the respondent; and the complainant may attend the hearing as an observer.

(2) Where the complainant initiates the hearing, the parties shall be the complainant and the respondent; and the University may attend the hearing as an observer.

(3) Each of the parties shall be entitled to be accompanied or represented by a person of his or her choice. An observer may be accompanied by a person of his or her choice, and may participate in the proceedings when and as permitted by the Hearing Committee.

6.07 The Hearing shall be conducted in a manner consistent with the requirements of natural justice, so as to give those involved a full and fair hearing.

6.08 (1) Subject to sub-sections (2), (3), (4) and (5) the hearing shall be held in private.

(2) A sexual harassment officer, the chairperson of the Hearing Panel, and the chairperson of the President's Permanent Advisory Committee may attend a hearing, subject, on application, to a contrary ruling by the Hearing Committee.

(3) A representative of the professional association, union or student body of the complainant shall, at the request of the complainant, be entitled to attend a hearing.

(4) A representative of the professional association, union or student body of the respondent shall, at the request of the respondent, be entitled to attend a hearing.

(5) The Hearing Committee, on application, may exclude from the hearing someone provided for in subsections (3) and (4), but in such a case an alternate representative may be named.

6.09 The Hearing Committee may admit such evidence as it deems necessary and appropriate, and is not bound by the rules of evidence that apply in judicial proceedings; though in deciding what evidence it will admit the committee may take those rules into account.

6.10 The onus of proof shall rest on the party seeking to prove that the conduct or comment alleged has occurred or been made, and that it falls within the definition of a complaint in section 1.02; and the standard of proof shall be on the balance of probabilities.

6.11 The Hearing Committee shall have 20 working days from the date of the conclusion of the hearing to reach its decision.

6.12 The Hearing Committee shall give reasons in writing and it shall send copies of its reasons to the following:

(1) the President;
(2) the administrative head of the faculty or unit of the respondent;
(3) the complainant;
(4) the respondent;
(5) the sexual harassment officer;
(6) the chairperson of the President's Permanent Advisory Committee.

6.13 The Hearing Committee shall (1) make findings of fact; (2) decide if on the facts the complaint is justified; and (3) make recommendations as to discipline to the appropriate University Officer. The findings of fact and a decision on whether or not the complaint is justified shall be binding on the University, the complainant and the respondent.

6.14 The appropriate University officer shall, in imposing discipline, take into account, but shall not be bound by the recommendations on discipline made by the Hearing Committee.

TIMELINES FOR PROCEDURES

Procedure	Number of Days*
Submission of written complaint	365
Advisor notifies respondent and Dean or Faculty or Head of non-academic unit	5
Respondent's written response to complaint	15
Advisor delivers response to complainant and Dean of Faculty or Head of non-academic unit	5
Mediation to be considered by both parties from date of delivery of the original complaint	30
Agreement reached regarding mediators and terms of reference	10
Mediation to be completed	15
Request for investigation to Chair of PPACSH**	5
Chair of PPACSH assigns investigators	5
Investigators complete investigation and submit report to PPACSH	15
PPACSH decides whether U.B.C. will initiate hearing	5
PPACSH notifies all parties of decision	5
If U.B.C. does not initiate hearing, complainant may request hearing	10
Chairperson of Hearing Panel notifies all parties as to composition of Hearing Committee	10
Challenges for cause to the composition of the Hearing Committee	7
Hearing Committee renders decision after conclusion of the hearing	20

* Days are interpreted as working days, i.e. days the University is open.
** PPACSH is the President's Permanent Advisory Committee on Sexual Harassment.

• **APPENDIX G**
Recommended wording for computer account applications

The University of British Columbia is committed to ensuring a working and learning environment in which all persons treat others with humanity and respect. The computing facilities at **[department name, e.g. University Computing Services]** are primarily intended for teaching, research, and administrative purposes. Their use is governed by the University's Human Rights and Sexual Harassment policies, by the Criminal Code of Canada, by the B.C. Civil Rights Protection Act and by the B.C. Human Rights Act. The user bears the primary responsibility for the material that he or she chooses to access, send, or display. The computer facilities may not be used in any manner to send or display material which contravenes the above policies or statutes.

Those who do not adhere to these guidelines may be subject to the suspension of computing privileges. More details on the guidelines are available in the package "The Appropriate Use of Information Technology," available with this application form.

Abuse of these computing facilities should be reported to **[contact person]** in **[department name]** by phone (**[campus local]**) or by electronic mail (**[e-mail address]**).

Signature of this application form denotes that the applicant has read and understands the package of material and also denotes acceptance of the above-stated terms of use.

• APPENDIX H

Recommended University-wide procedures related to inappropriate use of information technology

1. Ensure that application forms for computer accounts include the wording indicated in Appendix G.

2. Ensure that before obtaining accounts, users are informed of the culture and etiquette involved in the use of facilities including newsgroups and electronic mail, the nature and impact of offensive uses of these facilities and associated penalties, and the procedures for reporting abuses.

3. Establish as a penalty for inappropriate use suspension of computing privileges for a period of time. The length of the period should be proportional to the significance of the abuse as well as the number of previous abuses.

4. Ensure that all staff, faculty and administrators connected with a computing facility (either in a support/management role or through the teaching of courses using the facility) receive training on what constitutes appropriate and inappropriate use of the facilities, and on what to do if confronted by or notified of inappropriate usage.

5. Establish the procedure that on becoming aware of inappropriate use, a user should notify any of the staff, faculty or administrators connected with a computing facility. Once notified, this person must, in consultation with the appropriate UBC office (Sexual Harassment, Human Rights, etc.) and others responsible for the facility, address the problem. If the problem involves material that is potentially illegal, or sites outside UBC, this person must also notify the UBC individual responsible for handling such cases.

• APPENDIX I

Recommended additional actions by UCS

1. Identify a staff member of UCS as the person to whom abuses should be reported in cases involving material that is potentially illegal or sites outside UBC. This individual should be responsible for notifying the appropriate authorities external to UBC. This individual, in consultation with the appropriate UBC offices, would also prepare an annual report to CABC regarding the number, nature and outcome of abuses.

2. Make available one or more staff members of UCS to provide training for staff, faculty and administrators connected with computing facilities at UBC on what constitutes appropriate and inappropriate use of information technology facilities, and how to handle abuses.

3. Prepare a package of material covering the culture and etiquette involved in the use of information technology facilities including newsgroups and electronic mail, the nature and impact of offensive uses of these facilities and associated penalties, and the procedures for reporting offences. Make this material available to all users of UCS systems, and distribute the package to the other UBC computing facilities.