

Readers, note that emphasis has been added at certain points by Timothy Denton to assist a rapid reading of the text. My thanks to Mr. Justice John Sopinka for allowing it to be published here.

COGEL Conference

Edmonton, Alta.

September 15, 1997

Address by: The Hon. Mr. Justice John Sopinka

Supreme Court of Canada

FREEDOM OF SPEECH AND PRIVACY IN THE INFORMATION AGE

Freedom of speech and the right to privacy are two of our most cherished values. **Protection of these values under our legal system will be greatly complicated by the technological advances that have occasioned the greatest expansion in the communication of information in the history of civilization.** The medium, which is variously referred to as Cyberspace, the information superhighway or Internet, provides a means of global communication on virtually any subject. It is a potent democratic force which enables a far greater number of people to broadcast their views free of a publisher, broadcaster, editor or other gatekeeper's control to a greater audience, and at far less cost than by any other medium.

Along with the dramatic amplification in our capacity for communication with each other and the benefits that this brings come greatly amplified versions of old threats, and serious new ones also. The old scourges of defamation, obscenity, and hate propaganda on the Internet may cause greater personal and social damage than ever before. The availability of techniques by which messages may be posted anonymously makes civil recourse and criminal law enforcement virtually impossible in response to these abuses. Privacy is threatened by the collection of personal data, by the ease of surveillance and by the interception of communications on the Internet. One solution to the threat of privacy violation is the encryption (or encoding) of messages and data. However, a heated debate continues to rage over the issue of encryption, which may protect privacy but simultaneously shelter criminal behaviour such as the circulation of child pornography.

Recently, at the annual convention of Chiefs of Police, a session was devoted to Internet pornography. A 90-minute graphic video of excerpts was so upsetting that 175 officers left the room. One of the Chiefs was quoted as saying that "everything on the Internet is becoming bigger, better, badder, uglier, stinkier, nastier, more violent, more vile, more disgusting".

The result of this information explosion is that people have over-dosed on free speech. Law enforcement agencies and legislators are scouring the books to ascertain whether the existing laws can be used to curb the excesses. In some countries, new measures have been adopted. In the United States, in February, 1996, President Clinton signed the *Communications Decency Act* which imposed heavy punishment on anyone who transmits indecent or patently offensive material over a public computer network to minors or in a manner available to a minor. This legislation was heavily criticized and has persisted only briefly. In *Reno v. the American Civil Liberties Union*, the U.S. Supreme Court ruled on June 26th of this year that the *Act* was unconstitutional because, in the absence of any dependable way of screening interlocutors according to age so as to avoid minors, the *Act* was an effective ban on the transmission of "indecent" material between adults who have a constitutional right to receive and send such material to each other. In the U.S., indecent expression which is not obscene is protected by the First Amendment. The Court was not satisfied that the State had chosen the least restrictive way to achieve its objective as effectively as the *Act* would have done.

This legislation was found unconstitutional partly due to the existence of filtering software such as NetNanny or CyberPatrol, which allow parents to be assured that objectionable sites will be blocked. The existence of these programs contributed to the finding that the *Communications Decency Act* infringed the right to free speech, since they appeared to represent a less-intrusive means of protecting minors from indecent material. Ironically, they are now subject to the criticism that they themselves threaten free speech. Some critics fear that behind the secret lists of blocked sites, the software companies are using this censoring power to promote political agendas.

Another thorny problem is posed by the global nature of Cyberspace. Once a message is posted in Cyberspace it may be accessed from anywhere on earth. Different states balance individual freedom of speech and the collective good differently and present varying degrees of tolerance for obscenity, hate speech and defamation. However, Internet messages are oblivious of international political boundaries. An individual user who posts material on the Internet which is lawful in his own country, may unwittingly be offending the treasured values of another country. What can this offended country do about material on the Internet which infringes its laws? What should it do?

In December, 1995, a prosecutor in Germany caused CompuServe, a global on-line service provider, to shut down 200 of the net's sex-related news groups because they violated German obscenity law. Since the firm had no technical way to restrict Internet content only in Germany, it was obliged to impose the same restrictions on all of its 4 million world-wide subscribers. Surely this cannot be the solution, since it would have the effect of forcing Internet service providers to block all sites unless they conformed to the strictest law worldwide, in defiance of the rights of different societies to determine the worth of certain forms of speech for themselves. Nevertheless, one can understand the desire of countries to hold Internet service providers liable for unlawful postings on the Net since they are often the only entities within a country's legal reach.

Apart from problems of jurisdiction, should sanctions be applied to the Internet service providers? The service provider will pass the costs of sanctions or of attempting to meet the varied national laws on to the general public. It seems unfair that the general public must bear the costs of unlawful conduct by a limited number of people participating in obscene, defamatory or hateful speech. Furthermore, in order to curtail these forms of speech it is surely more efficient to apply legal pressure to those parties who are at the origin of such speech if their identities can be determined, rather than to another party for whom it may be most difficult to control that speech.

There have been suggestions that legislation aimed specifically at the Internet should be drafted. Many of the Netizens or Cyberians, as inhabitants of Cyberspace are known, are quite firmly against government attempts to "censor" content or to otherwise interfere with individual liberties on the Internet. The remarkable strength, diversity and dizzying growth of the Internet is thanks, in part, to the anarchic "state of digital nature" which exists there. However, as the Internet has exploded, so to have abuses on the Internet. Where legislation has been passed governing various aspects of Cyberspace there has been an angry backlash on the part of civil libertarians.

The libertarian culture of the Internet prefers self-regulation and self-help to any type of government regulation. In the absence of legislation, some have taken the law into their own hands by doing their own censoring. One Norwegian computer programmer was so incensed at a Phoenix law firm=s commercial advertisements on the Internet, that he wrote a program called "cancelbot" which automatically deleted every message sent out by the firm. The information age has the potential of allowing those few with the necessary expertise to censor any information they dislike. However, it is not clear that censorship by a small number of Netizens is preferable to governmental regulation.

[The "Virtual Magistrate" program](#), announced in 1996, and sponsored by two American groups, is one suggested means by which Cyberspace may be self-regulated. The Virtual Magistrate is a proposed arbitration system for the Net which could be of use in such things as electronic commerce where conflicts of law would abound. Others suggest that Cyberspace users form their own virtual courts, or that computer network service providers run an "alternative dispute resolution" mechanism for tort claims.

In any event, in the absence of both legislation directed specifically to the Internet, and an effective form of self-regulation, existing legal principles will have to adapt to the "brave new on-line world". Industry Canada commissioned [a study, published in February, 1997](#), which discusses the extent to which existing laws apply. To deal with defamatory statements, we might adapt and apply the laws of libel and slander which have recently been upheld as reasonable limits on free speech in *Hill v. Church of Scientology*. To deal with obscenity and hate messages, we have in place the provisions of the *Criminal Code*. The obscenity laws were upheld as a reasonable limit on freedom of speech in *R. v. Butler*. The hate laws were held to be constitutional in *R. v. Keegstra*. I propose to examine each of these tools in order to determine whether that are apt and, if not, how they can be improved.

Defamation

Any communication on the Internet which is defamatory is actionable against the person who made it and everyone who publishes it. If the person or other entity who made the statement can be identified, the party injured will have a remedy. But if the maker is impecunious or anonymous, the injured party will have an effective remedy only if he or she can sue the party publishing the statement. This is where difficulties arise in applying existing principles. Apart from the user, the other party playing a role in the dissemination of the defamatory statement is the Internet service provider. Does that party "publish" the statement so as to attract liability?

These issues have not been addressed in Canada but there are two decisions in the United States concerning the liability of on-line service providers for statements posted on their bulletin boards. In *Cubby v. CompuServe*, the on-line service provider did not maintain the bulletin board itself, but hired

another company to control it. When defamatory statements were posted on its bulletin board, the court classified CompuServe as a distributor who, like news vendors, book stores and libraries, is not liable for defamatory material in the U.S. if they neither know nor have reason to know of the defamatory statements. However, in *Stratton Oakmont Inc. v. Prodigy Services Co.*, the Court concluded that Prodigy acted as a publisher because it exercised sufficient editorial control over its computer boards to burden it with the same responsibilities as a newspaper. The court distinguished *Cubby Inc.* because Prodigy had held itself out as controlling the content of its bulletin boards and used a software screening program to monitor bulletin board postings.

Accordingly, under American law, it would seem that if an Internet service provider attempts to regulate the nature of the content on its bulletin board, even by a relatively automatic screening procedure (which would tend to pick up offensive words or topics rather than defamatory statements) it may be held liable as a publisher. However, if they do absolutely nothing they may avoid liability by being classed as a passive distributor, akin to a bookstore or news vendor. This latter strategy permits them to avoid liability for defamatory material but creates a "Catch-22" since they then risk damage to their corporate image resulting from the presence of unpleasant or offensive language on bulletin boards associated with them.

This state of affairs is far from satisfactory. The U.S. case law encourages Internet service providers to abdicate any control or responsibility for fear of being held responsible as a publisher of defamatory statements. By virtue of the vast number of communications that they would have to scrutinize, Internet service providers simply cannot closely monitor all the material for which they could be held liable as publishers. While they could use automatic software screening for certain words or topics, they are obliged to scrupulously avoid any screening at all in order to avoid being classed as a publisher. But surely whatever screening they may reasonably conduct should be encouraged?

Although it is difficult to be definitive with respect to the likely result under Canadian law, it would appear that a service provider cannot escape liability by the simple expedient of being classified as a library, bookstore or news vendor. Under English law, a library can be liable as a publisher unless it establishes the defence of innocent dissemination. This requires the defendant to prove that "he neither knew, nor ought to have known, on the assumption that he carried on his business properly, not that the paper was one which contained a libel but that the paper was one which was likely to contain a libel." The result will, therefore, depend on the facts of the case. Service providers cannot simply rely on the fact that they cannot be expected to vet the material that appears on their bulletin boards. **The defence of innocent dissemination is only open to an on-line service provider which was "operating its business properly"**. In appropriate cases, the Courts may be willing to impose some sort of screening responsibility as an element of the "proper operation of the business". **However, the use of a screening program should not, as in the U.S., inexorably lead to the conclusion that the Internet service provider was a publisher of the defamatory material.** To do so would be to place the Internet service provider in an impossible position since it is extremely difficult to pick up defamatory statements using automatic screening procedures, and screening using the subtler sensitivities of human employees would be a herculean task.

Obscenity

Our court decided in *Butler* that the prohibition on the undue exploitation of sex in s.163 of the

***Criminal Code* is a reasonable limit on the right to free speech.** We concluded that s.163 did violate the guarantee of free speech in s. 2(b) of the *Charter*, but was justified in the interests of preventing harm to society as determined on the basis of community standards. These standards are national standards that do not vary from one jurisdiction to another.

This has avoided, perhaps unwittingly, one of the problems that is troubling commentators in the United States. Under American law, local community standards are used to determine whether material is obscene. This enables prosecutors to shop around and pick the most conservative jurisdiction in which the material was received. The accused may then be punished on the basis of standards which were not applicable in the jurisdiction in which he posted the material.

In Canada this would not be a problem with respect to material that originated in any part of the country. We may have other problems. Section 163 creates two classes of offences. By virtue of s. 163(1), everyone commits an offence who distributes or has in his possession for a like purpose any obscene material. Under s. 163(2), everyone commits an offence who knowingly sells, exposes to public view or has in his possession for such a purpose any obscene material.

As in the case of libel and slander, the question arises as to the degree of familiarity with the obscene material that is necessary to implicate an Internet service provider. In *R. v. Jorgenson*, we decided that the term "knowingly" required the vendor to know of or be wilfully blind as to the characteristics that made the material obscene. If, therefore, the service provider is equated with a vendor of pornographic material, it would be difficult in most cases to prove knowledge or wilful blindness. On the other hand, a lesser degree of awareness is required under the first branch which deals, not with vendors, but with makers, publishers or distributors.

The categorization of large on-line service providers has not been considered in Canada, although the situation of a small bulletin board operator was considered in *R. v. Hurtubise*. In this case, the accused couple operated a pornographic computer bulletin board service which permitted subscribers to gain access to a CD-ROM of pornographic material, some of which was child pornography. The Court faced the issue of whether they were distributors subject to strict liability under s.163(1) or vendors guilty only on a showing of knowledge or wilful blindness under s.163(2). The Court held that the Hurtubises were distributors rather than retailers and that they had failed to exercise due diligence because they did not make inquiries into the content of their CD-ROM. This case deals only with small BBS operators who are relatively close to the service that they provide. It is difficult to know whether Internet Service Providers, who merely provide a connection to the Internet through which obscene materials are transmitted, or even those which run large unmoderated bulletin boards would be treated in the same way by the courts. This Court noted in *Jorgensen* that producers or distributors are presumed to be familiar with their material by virtue of creating or distributing it. It would seem that these presumptions would be misplaced in the case of Internet service providers, who, like vendors "would ordinarily not be aware of the specific nature of the contents of the material sold" due to the large quantity of communications passing through their systems.

There are, however, other problems. Much of the obscene material that appears on the Internet emanates from outside Canada, and in most cases, from the United States. Section 6(2) of the *Criminal Code* provides that no person can be convicted of an offence committed outside Canada. I have referred to the action taken by the German authorities against an Internet service provider with operations in Germany which had the result of imposing German standards on the whole world. Other countries have taken

similar measures. The answer appears to be international cooperation with a view to arriving at a convention similar to that in areas such as law enforcement and the enforcement of custody orders.

Hate Literature

Similar problems arise with respect to the provisions of the *Criminal Code* relating to the promotion of hatred. By virtue of s. 319(1), everyone commits an offence who, "by communicating statements in a public place incites hatred against an identifiable group where such incitement is likely to lead to a breach of the peace." Section 319(2) makes it an offence if the statement is communicated anywhere other than in private conversation but the Crown must establish that it was done wilfully. In *Keegstra*, our court held that to find "wilfulness" it was necessary to prove that the promotion of hatred was the conscious purpose of the accused or that this result was foreseen as certain to occur.

It is not likely that a service provider will be implicated by these sections by reason of their exacting requirements of *mens rea*. Since the Internet service provider, who merely facilitates the transmission of a message, is unlikely to even know of the content of the message, it would be unlikely to meet the *mens rea* standard necessary. The sender of the message is a more likely candidate. If a user posts a hate message on a bulletin board, is this a public place? Certainly all users have access. In an earlier version of this speech, I discussed the impact of our judgment in *Ramsden v. Peterborough* in which we struck down a city by-law that sought to ban posters on public property. That judgment stressed the public nature of posters in communicating ideas. I observed that the electronic media such as Internet may be the posters of the late 20th century.

Assuming that the bulletin boards or news groups are a public place, what should be done when the physical computer server on which a message is posted is located outside Canada? Does the Canadian *Criminal Code* apply to Cyberspace as a virtual "public space" or do foreign servers become "public places" subject to Canadian laws in some other way? This raises the same problems that I discussed in connection with obscenity. Where did the offence take place? Once again, Germany has faced this issue. In late January, 1996, Deutsche Telekom cut off access to all computers linked to the online server "Web Communications", fearing prosecution under German anti-Nazi laws because Web Communications rented Web space to Ernst Zundel. While this solution was not fully effective, neither did it have extra-territorial effect, although other entities such as Deutsche Bank Securities who rented space on Web Communications found themselves "thrown out with the hate speech".

Anonymity

All of the problems discussed above are complicated by the ability of Internet users to be completely anonymous. The identity of a person in Cyberspace may be discovered through the records of the Internet service provider where a person's true name and E-mail address may be matched. However, there is a means through which a person may remain truly anonymous. An "anonymous remailer" is a device which receives communications from individuals and strips away all headers which indicate the origin of a message. In some cases, the administrator of the remailer maintains records of the remailer users but there is no obligation to do so.

Anonymity promotes both unfettered free speech and the abuse of free speech. An anonymous speaker may speak freely without fear of governmental persecution or social ostracism. In fact, Johan Helsingius, a former anonymous remailer administrator, was motivated by his fear of totalitarian state control. In a 1994 interview in *Wired Magazine*, he stated that;

"It's important to be able to express certain views without everyone knowing who you are...Living in Finland, I got a pretty close view of how things were in the former Soviet Union. If you actually owned a photocopier or even a typewriter there you would have to register it and they would take samples of what your typewriter would put out so they could identify it later. That's something I find so appalling."

The value of anonymity in the promotion of meaningful free speech is clear. Anonymous remailers were originally created to allow victims of child abuse or AIDS to engage in private therapeutic discussion. However, an anonymous speaker may also indulge in the worst abuses of free speech, such as child pornography and hate propaganda, or other crimes such as extortion, stalking, threats or harassment with perfect impunity.

Accordingly, the benefits and risks of anonymity are clear. The challenge is to devise a regulatory system which keeps the social benefits of anonymity while controlling the excesses. Levine suggests that anonymous remailers be obliged to keep records of their users which would be available upon court order. He also suggests that remailer administrators should be subjected to liability only where they know of illegal acts passing through their service.

Privacy

The other societal value that is threatened by the new technology of the information age is privacy. The ease with which personal information can now be assimilated makes it possible for "big brother" to be watching us. **Unlike freedom of speech, there is no explicit right to privacy guaranteed under the Charter. However, s. 8, which provides everyone with the right against unreasonable search and seizure, is grounded in the right to privacy.** The test for its application against government surveillance is the existence of a reasonable expectation of privacy. The more accessible the information about an individual, the less is his or her expectation of privacy. In recent years, a story appeared in the Ottawa newspapers that police in the course of scanning bulletin boards detected a posting by a parolee which they believed showed that a parolee had travelled to the U.S. in breach of his parole. The subject had obtained gainful employment in a car dealership, but was fired when the police arrested him. It turned out the police had misinterpreted the information.

In order to make out a breach of s. 8, our parolee car salesman would have to distinguish *R. v. Plante*. In that case, we had to consider whether it was constitutionally permissible for the police to use its computer records of the electrical consumption at a specified address in order to determine whether or not it was likely that marijuana was being grown at the house, since this is often characterized by a higher than normal consumption of electricity. I observed that the "*Charter* should seek to protect a biographical core of personal information which individuals in a free and democratic society would wish to maintain and control from dissemination to the state". It could not be said that information revealing a pattern of electricity consumption would fall into such a category. However, each case must be decided on its own facts, carefully analyzing the extent to which respect for one's personal privacy and dignity has been violated.

But snooping by police is only one of the concerns. Perhaps of greater concern is the intrusion into our personal lives by private parties. One example emerged during the confirmation hearings of Judge Robert Bork for the United States Supreme Court. During the hearing, his video rental viewing habits were revealed after a reporter tracked down the computer records of his rentals.

The Internet is also a fertile collection ground for commercial marketing information. In 1995, a Seattle company began to sell an advertising mailing list of 250,000 E-mail addresses collected from public spaces on the Internet. The possibility of the collection of information about personal behaviour and interests is disquieting. Furthermore, there exist programs called "sniffers" which monitor passing communications to identify and save useful information, including credit card numbers, passwords or other confidential information.

These intrusions by private persons and entities are the more serious because they cannot be challenged as a violation of s. 8 of the *Charter*. Nor, it seems, is there any civil remedy available. Furthermore, no preventive measures can be taken because often, as in the case of Bork, we are not even aware that the information is being collated and stored.

It has been said that an unencrypted message on the Internet is as confidential as a postcard. Encryption refers to the encoding of data using a mathematical formula. Encryption technology is the subject of a current raging debate. If powerful encryption technology becomes widely disseminated, law enforcement agencies fear that they will not longer be able to use lawful wiretaps to monitor criminal activity, and national military agencies are afraid that they will be unable to decode the communications of unfriendly nations. Yet, encryption can protect law-abiding citizens from invasions of their privacy.

Conclusion

Freedom of speech, privacy, anonymity and encryption are all linked aspects of the same problem. **As anonymity and encryption are controlled and reduced in order that domestic laws may be enforced in the on-line world, individual privacy and free speech is threatened.** As more and more sensitive information is traded and commerce is conducted on-line, individuals are open, to an unparalleled extent, to the possibility of untoward governmental surveillance, the depredations of thieves or vandals intent on hacking into databases or using information in communications, the solicitations of commercial interests which have amassed marketing profiles from watching individual behaviour on the Internet, and even simple busybodies. While anonymity and encryption provide good ways of avoiding these dangers, they raise the spectre of Internet lawlessness. By removing any possibility of holding people accountable for defamation, obscenity, hate speech or other social ills, anonymity and encryption remove the deterrent effect of the law.

The information age has brought us a wonderful instrument which enables us to vastly expand our knowledge and comprehension of the world. It is not, however, an unmixed blessing. Society is struggling to attempt to curb the excesses and abuses. **We must be careful, however, that we not kill the proverbial goose. Hopefully, the *Charter* guarantee of free speech will ensure that this does not happen. I predict that only partial success will be achieved in eliminating the abuses. Some will remain. Some members of society will be left without redress. While this is to be regretted, it is the price we pay for the right to enjoy freedom of speech and the price we pay for the many benefits that we derive and will continue to derive from this powerful new medium.**