Freedom of Speech and Privacy on the Canadian Internet
1993-1998

"Sorry, you can't download the new version of Netscape
until you view more Canadian content."
The Ottawa Sun

Abstract

This paper, the result of research conducted in 1998, takes an overview of a period of five years (1993-1998) on the Canadian Internet, looking for occurrences of controversial issues concerning free speech and privacy. A short historical review and a more detailed description of the theory behind free speech, as well as of the different actors interested in the development of the Internet, precede the actual overview of the issues at stake. As a rule, we can say that the intention of state institutions is to regulate the information flow on the Internet through censorship by limiting privacy. However, their attempts fail because of technological difficulties or simply the resistance of civil rights organizations specialized in Internet issues. Through the examples it presents, the paper wishes to provide guidance to the countries of the Central European region, who have yet to reach the stage of Internet development Canada knowns.

Résumé

Cette étude est le résultat d'une recherche effectuée en 1998, et passe en revue une période de cinq ans (1993-1998) sur la partie canadienne d'Internet, en cherchant des occurrences de polémiques concernant la liberté de l'expression et la vie privée. Un court aperçu historique et une description plus détaillée de la théorie sur la liberté de l'expression et aussi des différents acteurs intéressés dans le développement de l'Internet, précèdent l'examen concret des enjeux. En général, on peut dire que les institutions gouvernementales souhaiteraient réguler le flux d'information sur Internet à travers la censure ou bien en limitant le champ de la vie privée. Mais toutes leurs tentatives échouent à cause de difficultés technologiques ou simplement à cause de la résistance des organisations de droits civils spécialisés dans Internet. A travers les exemples qu'elle présente, cette étude désire montrer le chemin aux pays de l'Europe Centrale, qui n'ont pas encore atteint le niveau de développement d'Internet que le Canada a déjà connu.

Introduction

We have reached a stage in the development of the worldwide information network when scholarly papers or articles in the press dealing with it do not have to explain what the Internet and the various related terms mean and how important they are for the future of mankind. What needs to be specified in this introduction is rather the precise scope of this paper within this enormous and ever-growing subject matter. The
aim of this paper is to describe and analyse the forces that were at work in the development of the Internet in Canada between 1993 and 1998.

Today, in 2002, no country – with the possible exception of the poorest – can ignore the impact the Internet has on our societies. The world is discovering the controversial aspects of the new medium, in particular the questions of censorship and privacy. However, due to divergent levels of development, these questions arise in different places at different points in time. Having one of the best connectivity rates in the world (see section 4.4.), Canada has naturally been among the first to experience certain aspects of the related problems. In many respects, the countries of the Central European region are now approaching the point of Internet development Canada reached in 1998. In others respects, for example average connectivity rates, we are still lagging far behind. This analysis of the chosen period in Canada may thus prove to be useful in foreseeing and eventually preventing future problems, as well as in identifying current ones.¹

1. Prehistory in brief

Canada has always occupied a leading role in the field of communications. Many people are not aware that Bell’s telephone is in fact a Canadian invention, that Marconi sent his first wireless telegraph message from Newfoundland, and that Canada is the home of a number of apostles of the information age, among them Marshall McLuhan and William Gibson (Carroll, XII).

Jean Chrétien, Canada’s Prime Minister, has given a geographical explanation to this affinity to information transmission, which he considers inherent to the country.

> Considering our unique circumstances in Canada, our fascination with communication systems is easy to understand. With a small population thinly scattered across one of the world’s largest countries, spanning six time zones, surrounded by three oceans, and including incredibly diverse and often difficult terrain, our communication systems have served the critical role of bringing Canadians together and preserving our culture and identity. (Carroll, XII)

It is not surprising therefore that when computer networks emerged as a scientific experiment, Canada was quick to join in with the United States. As early as the beginning of the 1970s the first networks were set up in different parts of the country. However, it was not until 1982 that the Canadian and American defence services agreed to interconnect their networks, which was realized in 1985. From then on the future of the Canadian side of the network was intertwined with the development of the Internet (called ARPANET at the time). In 1987 the .ca top-level domain was created to refer to the Canadian side of the network. On 25 October 1990, CA*Net, the high-speed Canadian national research network, was launched, which interconnected the formerly existing regional networks. The first commercial dial-up accesses to the Internet (the ancestors of today’s ISPs) appeared in 1992. Government initiatives predominated in 1993 with the launch of the CANARIE and Schoolnet programmes, and also the first World Wide Web sites pointed up on the Canadian Net following the world premiere in Switzerland. This new way of handling information on the computer network led to its opening up to the public. In 1994 and 1995, most institutions created their own web sites, and for a time the increase in Canadian web addresses exceeded 100% per year.
A watershed came in 1995, in the sense that the notion of the Internet erupted on the public scene, people and authorities started to talk about it seriously and the first questions about controversial issues were raised. Also, by this time all the actors on the Internet scene were in place and ready to confront each other.  

2. An advocate of free speech

Before we look at the actors and the forces turning them against each other, let us first consider some general questions necessary to understand the approach adopted in the following article. As more and more people become aware of its potential, the Internet has been raising a number of controversial issues worldwide. The central question remains always the same: Should communication over the Net be controlled for any reason?

Initially, the underlying principle of the Internet – and this still remains widely applicable today – was total freedom in the opinions and material made public on it and their limitless availability to those who want to find them. It is important to underline this last point, because unlike traditional media like television and radio, and to a certain extent the print media, information on the Internet does not reach the public by itself. We have to go and get it intentionally.

These considerations must be taken into account when talking about censorship. For example, maintaining a pornographic website is essentially different from broadcasting X-movies on TV. I am not pretending to be neutral on this question; in fact I wholly accept the arguments of defenders of free speech on the Net such as Electronic Frontier Canada, a civil organization whose primary aims are to assure the liberty of opinions and the privacy of information exchange on the Internet, but also in other domains of modern telecommunications.

Similar organizations have work to do all around the world, because most of the countries sufficiently developed to make a nationwide communication tool of the Internet resemble each other in the sense that they are seeking ways to control what is going on online. It is the reasons for doing so that make the differences.

But even in countries which have liberal capitalist economies and are considered to be bastions of individual freedom like the US and Canada, control of the Internet is a high-priority issue on the political agenda. There are two main reasons for this. First, parents fear their children will be able to access inappropriate content (pornography, hate-sites and information on subjects like how to build bombs) through the Net, and so want to impose limitations on free speech. Second, law enforcement bodies fear that criminals will be able to communicate in complete secrecy if the 100% secure information encryption methods that are already available become widespread. These are powerful arguments, but those on the other side, relating to the technological impossibility of control without infringement of basic human rights, are no less forceful.

Since no satisfactory model of control has been found to work to date, the only reasonable solution, in my opinion, would be to accept free speech as a rule. After all, as mentioned earlier, Nazi and pornography sites will not bounce up on our computers by themselves: we have to go and seek them out them. The only regulation to be imposed is at parental level: do not let children surf the web alone in their rooms.
The issue of privacy is mainly concerned with the policies to be adopted with regard to encryption and the anonymity of the web-users. Today, standard messaging on the Internet is about as private as material contained on an on-line web site can be: nothing prevents a moderately skilled third party from reading our messages (not to mention our ISP). However, the currently existing encryption techniques allow a user to send a message to someone else in such a way that they will be the only ones to be able to decipher it. Law enforcement forces are concerned about the liberty in communication these techniques would give to criminals. They want to have control of encryption keys so that at least the police can intercept encrypted messages. On the other hand, civil rights advocates are worried that once the police can read our messages, it will not take long for criminals to do so (sometimes these will be simultaneous). So the question is what is better – enabling criminals to communicate or letting them watch everything we do? The future of electronic commerce is also at stake here, since only completely secure encryption would make it possible to communicate credit card data on the web (Riga, "If cops can read E-mail").

Having looked briefly at the general international issues of control over the Internet, we can now continue our exploration of the Canadian situation by presenting the different parties implicated. Those who are interested in a more detailed general discussion of these issues can refer to the website of Electronic Frontier Canada.

3. Actors on stage

3.1. The state

Realizing the potential advantages and dangers of the new means of communication, the Canadian government set up a number of institutions and programmes to help and control its development in the country. The programmes included SchoolNet, a federal government initiative to put all of Canada's schools on-line by 1998 and provide them with skills and learning content; CANARIE (Canadian Network for the Advancement of Research, Industry and Education), a business plan supported by both the government and the private sector to speed the development of key parts of the information highway; and finally, what is perhaps the most typically Canadian because deriving from the country's geography, the Community Access Programme, intended to enable people in remote rural areas such as the far North to join the Internet.

The Canadian government also made a point of showing a good example in the use of this new technology by building a network of websites for federal and provincial governments. However, these programmes had little to do with the controversial issues that form the centre of interest of this paper. They were developments of which no one questioned the necessity, motored by a clearly utopian vision of the society of the future as depicted in the final report of the Information Highway Advisory Council:

No longer will distance pose an obstacle to economic development, social intercourse, learning, voluntary action, adequate health care, business success or full participation in society and Canada's national cultural dialogue. Knowledge will become increasingly available to everyone, allowing us all to make wiser decisions in all aspects of our lives – from business to government to health care to education to work to our everyday existence. Everyone will be not only a consumer of knowledge and content, but also a creator. Canada's national cultural
dialogue and political discussion will take on a liveliness and depth that will strengthen national, regional and local communities. (IHAC)

The Information Highway Advisory Council operates in the framework of Industry Canada, giving advice to the government on the challenging issues that need to be resolved in order for Canadians to make the most of the technology of the Internet. The IHAC published two reports in the research period, one in September 1995 and a final one in September 1997. This latter outlined everything the government did, was doing and would do in this domain, so that it constitutes an excellent resource for researchers.

A number of already existing official bodies such as municipal governments, the federal Parliament and police forces are frequently forced to take sides in controversial issues related to the Internet. Nevertheless, we have to mention separately a problematic government organization whose existence is not the result of the Internet, but which controls a number of factors influencing its development and whose status in related issues was under debate in 1998. As stated on their website, the role of the CRTC (Canadian Radio-television and Telecommunications Commission) is “to supervise and regulate Canada’s broadcasting and telecommunications systems, balancing the interests of consumers, the creative community and distribution industries in implementing the public policy objectives established by Parliament”.

Apart from ensuring fair competition on the market by imposing economic regulations, the CRTC’s concern is also to keep out illegal or offensive content from the media and to make sure that the required proportion of Canadian material is being diffused.

In 1998, the mission statement was fortunately interpreted in a way that did not make the CRTC responsible for anything happening on the Canadian web, even if in previous years there had been voices from the organization alluding to regulatory intentions. What is startling sometimes is the degree to which people in key positions fail to understand the nature of the Internet.

When she became chairwoman of the CRTC in 1996, Francoise Bertrand announced her intention to make the organization control the viewed web content on both the ISPs’ (Service Provider) and the users’ sides. Fortunately, these ideas were quickly abandoned after it became evident that such a regulation would run up against the enormous technological, practical and moral difficulties inherent in regulating the Internet, some of which have been mentioned above. One of them was cleverly put by a journalist in a remark addressed to Bertrand:

[H]ow are you going to make ISPs responsible for ensuring that a surfer views the required 50% of content from a Canadian producer? Are ISPs now supposed to monitor where a user goes, and cut him off? Imagine a message telling you “Sorry, you can’t download the new version of Netscape until you view more Canadian content.” (Hall, “New CRTC boss”)

It is interesting to note that a similar debate burst out in October 2000 in Hungary, when the president of CRTC’s Hungarian counterpart gave voice to regulatory intentions concerning Internet broadcasting in the country.
3.2. Internet service providers

In 1996, Jim Carroll and Rick Broadhead used the following categorization to describe the 300 ISPs then existing in Canada (Carroll, 89-100).

- For-profit ISPs
- Non-profit networks: academic, institutional and community networks

In the following two years, the scenery became less varied, with more and more place going to for-profit ISPs, which sprang up like mushrooms all over the country, and with new national giants emerging (Ladner, “Web telephony”). The homogeneity also extended to their interests, which led to the formation of the CAIP (Canadian Association of Internet Providers) in March 1996. To date, no external regulation obliges Canadian ISPs to control what their clients store on their servers. The CAIP’s main achievement is to have taken a preventive step against external censorship by adopting a voluntary code of conduct in November 1996. The reasons for doing so are to be found in the Canadian legal system, based as it is on the Anglo-Saxon model of precedents. No ISP has ever been condemned in Canada for illegal content, and until this happens the law enforcement organizations cannot be certain when it is possible to strike. The code of conduct embraces the idea that it is better for the providers to restrict themselves before the police get grounds to attack in future cases (Hall, “Hunt on”).

Nevertheless, the adoption of the code is very much an anticipation of censorship, because according to critics Jim Carroll and David Jones from EFC it is much too vague on certain points and thus encourages a degree of cooperation with the authorities that already hinders free speech and privacy (Rowan and Friedman).

3.3. Academic community and Internet veterans

It is understandable that people who in 1994 were the sole inhabitants, legislators and creators of a new parallel world where free speech was the common denominator feel frustrated today as they witness not only the public and commercial appropriation of the Internet, but also the various attempts from different external official bodies at regulating the information flow on it.

This frustration has led to the creation of interest groups that believe they are acting not only in their own name, but for the future of everybody using the Internet. Electronic Frontier Canada took the lead as a general defender of free speech and privacy, backed by more specialized professional associations such as LoGIC (Legal Group for the Internet in Canada), a group of lawyers devoted to ensuring, as the association says on its homepage, that “new laws and regulations have no detrimental effects on the free and interactive communication of information.” These groups are radically against any hindrance of free speech on the Internet, which sometimes places them in situations where they find themselves opposed to official bodies and side by side with not very respectable individuals and organizations. However, they always stress that they do not necessarily agree with what is being said, but insist that there has to be a way of saying it. This is also my own position on the controversial issues to be discussed later.

There are also countless numbers of individuals who contribute to the maintenance of free speech through various actions, the most important being the mirroring of sites that were banned somewhere else.
3.4. The public

The best way to build a profile of Canadian Internet users is to rely on statistics. Many organizations carry out regular surveys all around the country, among them ACNielsen, Angus Reid Group, Statistics Canada, POLLARA, Ekos Research Associates, or at the provincial level, for example RISQ (Réseau Interordinateur Scientifique Québécois, Scientific Intercomputer Network of Quebec). Their methods vary and their results are diverse. Some achieve surprising levels of sophistication, so that one could devote an entire dissertation to their analysis (like the surveys of RISQ). For the sake of the present work, the following points can be made about the use of the Internet by the Canadian population.

Canada has always been among the countries with the highest proportion of connected population. In November 1997, 31% of Canada’s inhabitants had access to the Internet, outscored only by Iceland (45%) and Norway (32.5%). To put things into perspective, the US was at 30% in February 1998, the UK at 10% in August 1997, Germany at 7% in February 1998, Hungary at 1% in March 1997 and France at 0.69% in September (NUA, “How many online?”). One can expect that it is in countries with the highest number of people having experience with the Internet that problems will first arise concerning content control. Indeed, there is a growing general awareness of the Internet, shown by the fact that in 1998 42% of the Canadian population already had experience with it (ACNielsen), compared to only 18% in 1995 (Angus Reid Survey in Caroll, 490).

We can also observe a considerable shift in the composition of the connected users according to gender and age. The 68% / 32% male-female ratio of 1995 (Angus Reid Survey in Caroll, 490) moved to 53% / 47% in 1998 (ACNielsen), whereas the number of internauts aged 45 and over tripled during 1997 (NUA, “Statistics Canada”). According to the analysts of the RISQ survey (RISQ, Sept. 1997 “Le service d’Internet”), this could be the cause of the continuously growing popularity of e-mail: the increasing number of women and retired elderly people who join the Internet use it primarily for messaging, not surfing on the World Wide Web, which only comes second in the list of activities of all users.

The massive arrival of women and the increase in home access (almost doubled over the year 1997: NUA, “Statistics Canada”) emphasizes the growing family aspect of the Internet. A 1997 survey announced that 66% of all Canadians considered some kind of regulation should be applied to it, with the rate going up to 80% among women with young children (Cobb). Since regulation is technically difficult, these figures are alarming. However, EFC representative David Jones remained optimistic:

There is a difference between being on the Net for 6 months and 16 months. The more experience people have on the Net the more they appreciate its openness. They come to realize that they can make choices themselves and they don’t need some bureaucrat to decide what they can see or not. (Cobb)

4. Issues at stake

The following presentation relies on an in-depth study of the 450 press articles (dating from 1992 to February 1998) stored in the media archives of the Electronic Frontier
It is will hopefully provide information to people who want to look at how an Internet control related issue has been dealt with in Canada.

4.1. Inappropriate content

4.1.1. Revealing secret information

Historically, the issue of control over the Internet first emerged in 1993, when the development of the network in Canada was still restricted to the academic community and the average citizen had not even heard the name Internet ever mentioned. In July that year, the trial conducted in the Karla Homolka/Paul Bernardo serial murder case was ordered to be hidden from the eyes of the public. Radio, TV and the print media did comply with the publication ban, but the Internet newsgroup discussions of the University of Waterloo somehow got hold of forbidden documents and discussed them eagerly until the authorities of the university decided to ban the newsgroup in question. In practice, this meant that the discussion groups simply moved to American servers where they could not be bothered any longer, and the affair received more publicity than it could have ever achieved by itself. Public debate started on the rights of a university to determine what is being published on its server, and as an offshoot of the case Electronic Frontier Canada was founded in 1994 by a Waterloo University professor and other members of the academic community. In retrospect, it is clear that this affair marked the beginning of a long series of cases in which offended people complain about a certain content, authorities struggle in vain to snuff it out from the web, and civil rights organizations raise their voices in defence of free speech. (Lougheed).

Incidents similar to those arising from the Homolka/Bernardo case can have international effects, as demonstrated by the occasion when the author of a Canadian site in British Columbia was instructed by a British court to withdraw the mirror page of documents of a trial that had been banned in Britain. This time, the author complied with the demand, although it is hardly conceivable how he could have been punished if he had kept it online; (the British were attacking him on the basis of copyright violation [see section 4.4 below and Kapica]).

4.1.2. Hatred

Even in a liberal and seemingly peaceful country like Canada, there are hidden tensions ready to surface here and there. The Internet provides an excellent medium for groups and people who wish to incite these forces, not only because of the ease of communication that characterizes it, but also because the publication of a hate-site usually results in much greater fame through traditional media coverage than it would probably generate by its sole presence on the Internet.

The first and most persistent issue has been the Zundelsite, a hate-site against Jews maintained by Holocaust denier Ernst Zundel on a server in the United States. It started out back in 1995 as an international affair. German universities wanted to block access to the server in question, but their students found a way to get around the ban. They used a website in Toronto called The Canadianizer, where you could type in the address of any site in the world and it would appear enriched with Canadian content, like the anecdotal “..., eh?” ending of sentences in Canadian English (EFC press release, “Net Censorship Backfires”). Later on, in autumn 1997 the case became a national issue raising the delicate question whether Canadian courts could bring
decisions concerning a website situated in another country. When the Canadian Human Rights Commission got involved, they even dug up an old law stating that answerphone messages inciting to hatred were illegal and tried to compare the World Wide Web to answering machines. It is possible that they might finally succeed in putting Zundel in jail through reference to the terms of the Human Rights Act, but the procedure used would be outside the boundaries of the Internet and is not of direct interest to us here (Borovoy and EFC press release, "Electronic Frontier Canada").

When a site with controversial content is situated on a Canadian server, the debate gains another dimension. This is what happened with the Freedom Site, which had been banned by all but one ISP in the country. This site offers the bulletins of politically incorrect groups who aim at revealing the oppression that white Anglo-Saxons suffer from in Canada. Anti-immigration and anti-Jewish material is fairly common on them. Although their presence on the Fairview Technology Centre’s server in British Columbia had already been challenged as early as July 1996 (McCullagh), the Simon Wiesenthal Centre only launched its full offensive in January 1998 by naming Oliver (the hometown of the controversial ISP) as “hate capital of Canada”, as if the citizens of the peaceful town had anything to do with what was going on in the computers of a private company situated there. Feeling offended, the town of Oliver is now charging the Wiesenthal Centre with defamation (Pattison). Worse, according to David Jones from the EFC, there is nothing on these sites that is against the current Canadian law: if the same publications were being distributed on paper, authorities would not go to so much trouble over them (EFC press release, “BC Gov’t”). A good thing, however, is that in the true spirit of free speech, Yahoo.ca, the main Canadian Internet directory (organized on a thematic basis), does provide a link to the Freedom Site, with the relatively neutral comment “hosts Canada’s most controversial organizations”.

The issue is even more heated when it comes to the tensions existing between the Francophone and Anglophone parts of the population. The “Quebec North America’s Neo-Fascist State” site knew a brief, tormented but highly publicized life in August 1997. The site, drawing parallels between the current regime in Quebec and pre-war Nazi Germany, and going to such extremes as having Quebec Premier Lucien Bouchard’s photo morph into a picture of Hitler, was quickly withdrawn by its creator, a British Columbian ISP, under the joint pressure of internauts, Quebec and the Simon Wiesenthal Centre, only to reappear immediately on different servers in the United States. However, it was impossible to find it in March 1998 (Cauchon). But not in August 1997: one person got into serious trouble when creating a link to the incriminated site on his personal home page with the following comment and nothing more: “Here’s a site that the Quebec government wants banned.” Rather innocent, one would have thought. However, as a federal civil servant employed at Industry Canada, he was instructed to remove the link and an investigation was started to determine whether he was spending government money on propagating hate material about the province (Rupert).

Another similar chain of events had been provoked by a Lucien Bouchard hate-site a few months earlier (Guy). The EFC’s viewpoint on this question is that only inciting people to commit violence against others is illegal; simply hating them is not. They also consider the Canadian Association of Internet Provider’s voluntary code of conduct to be much too rigorous, as it makes the ISP responsible for the content that is situated on its server (Cauchon and EFC press release, “Plug Pulled”).
4.1.3. Language

The issue of language is all the more interesting since this kind of problem is typically bound to arise in Canada. Among the reasons for the unpopularity of Quebec among a number of Anglophone netizens are the attempts of the province’s authorities to control the language used on the websites located geographically within its boundaries. The controversial Office de la langue française (Office of the French Language) has the responsibility of enforcing the draconian measures of the Charter of the French Language, whose main aim is to ensure that the province’s first language maintains its predominant status versus English. To get an idea of the extent to which the language inspectors go in real life, it is enough to read the troubles of a hapless Anglophone Montreal computer storeowner. Among the different small details (one more ridiculous than the other) that were found to be offending the Charter in his shop, the most absurd one was that on his otherwise completely Francophone business card a small map had the text “Décarie Blvd.” instead of “Boul. Décarie”. In fact, a businessperson can give an English language business card to another only if he is specifically asked for it (Gatehouse).

In these conditions, it is not surprising that when in May 1997 another computer store owner published his shop’s home page, of which only two-thirds was translated into French, the OLF was quick to strike and requested him to remove the site, add more French or pay a fine. Personal web pages are fortunately free from language control, but commercial ones fall under the regulation on commercial brochures that requires them to be dominantly in French. The OLF’s step incited a heated debate, which went up as far as the federal government, as to whether a provincial authority has any power in legislating the language to be used on a section of an international territory like the Internet (Thompson).

For our part, we can only advise them to follow the recommendations of a Francophone journalist who suggests that the authorities propagate French not by banning material from the Web but by encouraging the creation of more French-language sites (Dubuc).

4.1.4. Child pornography

The online publication of standard pornography is a legal and accepted practice, on a par with the presence of printed pornography in newspaper stores, where you can walk in and browse through dozens of adult magazines. One issue in relation to the Internet is the ease of access to the porn sites; the debate in this area will be discussed in the section on libraries and public places (4.1.6 below). However, the category of pornography mentioned in the title of this section is a case apart: material depicting children in sexually explicit situations is simply forbidden by the law in any format. People whose sexuality is aimed at children have always existed, and the Internet has proved to be an excellent tool for them to come together and exchange material. This does not happen on publicly accessible websites, but on secret, hidden ones, in specialized newsgroups where they can post anonymous messages, and on private BBS servers that cannot be reached via the Internet but only by a direct telephone line. Ever since the Regina versus Butler case, which has served as precedent since 1992, and the widening of the definition of child pornography in August 1993, police raids have become frequent in homes and even offices where child pornography is stored on computers (“Regina v. Butler”). For this offence, unlike that of hate sites, the punishment is almost automatic, and can run to a maximum of five to ten years of
imprisonment, depending on whether the person only stored the obscene material on his computer or also distributed it ("Definition of Child Pornography"). Surprisingly, the offenders often include respectable people, teenagers or even women, which shows the gravity of the phenomenon (Hebbard, Barrick, McClintock).

Even though child porn collectors do not maintain public websites, it is rather easy to track down their activities on the Internet. In this respect, the police must be thankful to the Net, since it considerably facilitates their task. In fact, the police departments dealing with child porn have been overloaded with work since the Internet emerged (Szklarski). If the cause is undoubtedly fair, it is their methods that can give rise to controversies. In one case, it was not the police who discovered the infamous files but a technician doing a routine check on a computer brought in for repair. There was no evidence that the person who downloaded them to his computer did not do it from pure curiosity and was not going to erase them anyway. Nevertheless, the man was banned from the Internet for eight months (Cox).

In fact, even if somebody only views a child porn picture on his computer screen without voluntarily saving it to the hard disk, he might be breaking the law. In general, the currently used browsers always create a backup file of everything that the user views in a directory called "the cache", in order to avoid unnecessary downloading times should the user go back to the page in the near future. Can these automatically created and renamed backup files be considered child pornography stored on your hard disk? Physically, the answer is certainly yes. Although in the period under examination there was not any concrete case involving them, it could happen any day (Mentek). Lawyers are still looking into the legal status of backup files created by the web browsers, partly too because they also raise issues of copyright (Jannuska).

A rigorous civil rights defender might also find the definition of child pornography a little too wide in the sense that it also includes "any written material or visual representation that advocates or counsels sexual activity with a person under the age of eighteen years that would be an offence under this Act" ("Definition of Child Pornography"). One wonders how Nabokov's *Lolita* can be published in Canada with such a regulation. In fact, in October 1993 a young man writing short fictional stories about his sexual fantasies involving children and uploading them to the Internet was convicted under the terms of the new definition adopted in August that year. Before that, only cases involving real children were effectively pursued. His case served as precedent to many others, the most notable being the confiscation of the works of painter Eli Langer in 1993 (Skelton).

4.1.5. Elections

The 1997 elections in May were the most "wired" ones in Canadian history to date, and this fact caused two quite distinct types of new issues to emerge in public debate. Both disputed cases offended Canadian law, one by publishing too much information on the Net, the other by showing too little.

A complete media blackout is ordered by the Elections Act concerning preliminary survey and poll results during the 72 hours that precede the closure of the last polling booth, so that electors will not be influenced by anything in the last days of their personal decision-making. A lot of people find this regulation unnecessary and even absurd, to the point that one polling company exported his online poll results to a server in Florida where it is out of reach of Canadian jurisdiction (once again, the
ARPANET principle). Canadians eager to be up-to-date to the last minute just had to type a different address in their browser. Subsequently, newspaper groups and civil rights organizations decided to challenge this regulation (Riga, “Internet users”).

The other case was a conflict with advertising restrictions imposed on pre-election political campaigns. An individual put up a site supporting the Canadian Green Party on its home page, but did not name the sponsor of the site under the pretext that he wished to remain anonymous. Elections Canada threatened him with a fine of $1000 or one year of imprisonment if he did not name the sponsor or shut his site down. The author of the site opted for this latter solution; however, sixty "Vote Green" mirror pages – one as far away as Norway – sprung up on the web in no time. The EFC undertook the task of challenging the advertising restrictions with reference to the Charter of Rights and Freedoms. According to David Jones, setting up a personal home page promoting a political party is just like putting a supportive sign in the window of one's house (Riga, “Internet users”).

4.1.6. The Internet in libraries and public places

Even standard web pornography can become a serious issue if it emerges on the computer screens of a public library, as happened on an unfortunate occasion when a pornographic image left on the monitor of a Burlington Library computer was spotted by a five-year-old girl. Her father was further irritated by the nonchalance with which the library staff handled his complaint. The affair turned into a major debate after another parent joined in with similar problems, and the library had to look for different alternatives to prevent this from happening again. It quickly turned out that no filtering system could be applied to the computers because they banned sites containing useful information on, for example, breast cancer. In the end, the solution seems to be to adopt a mixture of measures including punishments to those who leave such material on-screen, the positioning of the monitors so that only those sitting in front get a view of them, and staff paying more attention to spotting and educating young people who try to access controversial material (Henderson). EFC spokesman David Jones's opposition to imposing restrictions on the Internet access of the library was thus rewarded by success (EFC press release, “Public libraries”). We can only hope that this case will serve as precedent for potentially emerging new ones.

As for schools, there have not been many reported cases; it seems the teachers are holding a firm grip on the Internet access from the classrooms. However, one incident could be noted, when the carelessness of a teacher led him to encourage his pupils to look at his personal website, where he had some spicy jokes he had forgotten about. The teacher was immediately fired (unsigned, “Teacher fired”).

4.2. Issues of privacy

4.2.1. Encryption

Encryption is a very hot issue indeed, because for once it is not a tiny group of defenders of free speech that are challenging official regulation and public opinion. Instead, the entire commercial and banking sector of the country is confronted with so-called national security interests. In Canada the issue has not been subject to as much debate as in the United States, because the law has been more permissive. In order for the FBI and other similar bodies to be able to crack into any message circulating on the
Web, the US until very recently imposed export and usage restrictions on software enabling 56-bit encryption and over. To put this into perspective:

Some cryptographers argue that, with little more than $200,000 worth of specialized computer hardware, a lucky and bright hacker could break a 56-bit key within hours. So far, there has been no public evidence of that being accomplished. Experts say it would take the 78,000 computers 67 years to crack a secret key algorithm using a 64-bit key and well over 13 billion times the age of the universe for those computers to crack a 128-bit key. Canadian banks that allow customers to complete transactions over the Internet use 128-bit encryption to hide customer data while it travels between the bank and the customer's home computer. (Akin, "Cracking the codes")

In March 2002 it seems that both countries have given up the idea of enforcing legislation on encryption, in order to facilitate the development of e-commerce.

4.2.2. Exploiting the lack of privacy

If business companies are intent on the privacy of financial exchange on the Web, they are less enthusiastic about the anonymity in personal information and in browsing, as mentioned earlier. Commercial data mining is taking the form of "cookies", little files that are sent to the user's machine to log his or her visit to a given site. American advertisement agencies using this technology started targeting the Canadian market in 1997 (Dutt). The use of electronically collected data was soon to be regulated (Camlot, "Ottawa to introduce"), not only in order to prevent excessive commercial data mining but also to hinder possible criminal activities (e.g. blackmailing) based on exploitation of databases (Lawton).

This is the place to note also that new forms of revenge are born on the Internet and make newspaper headlines: making somebody's personal information available on an undesired forum in a made-up context so that the person will get endless harassment. A woman in Vancouver irritated by a rival in a love affair posted the other woman's home address on a sex forum with an inviting message. The rival "received thirty phone calls within days and a letter from Egypt in response to the Internet sex ad". The woman who committed the crime was put on 18 months' probation and was banned from the Internet for that time (D'angelo).

4.3. Internet hysteria in the media

With the last news item, we have reached a domain of Internet-related issues that often make the headlines in tabloids. In fact, traditional media are doing a great job in spreading popular misconceptions about the new technology by mentioning only its offensive and obnoxious aspects. Instead of emphasizing the incredible variety of advantages that one can gain from using the Internet, they offer over-exaggerated coverage of cases like teenagers building bombs following instructions found online (Hann) or how two people who met in a newsgroup committed collective suicide (Mascoll). What these articles fail to indicate is that bomb-building instructions are available to anybody in public libraries and that every week several thousand happy relationships are initiated in Internet newsgroups and chatrooms between people who could not have met elsewhere. Also, a very sad example of media distortion about the Internet is described in the Internet Handbook: in 1995, a benevolent Canadian initiative advocating the right to euthanasia for the terminally ill on the Internet, the DeathNet site, was the victim of a hysterical press campaign based on the false
information that they were giving away suicide recipes (Carroll, 508-520). Typically, the beneficial aspects of the Internet get publicized only if the case is unique enough to draw attention. The incident when a young boy in Texas saved the life of a Finnish woman asking for help in an Internet chatroom in April 1997 got world publicity (unsigned, "12-year-old hailed"), but little attention was given to a similar case involving a woman in New Brunswick who alerted Interpol when her Scrabble playing partner in England suddenly lost consciousness (unsigned, "Injured Internet man"). Reports of this kind of thrilling news are unfortunately rare compared to the richness of spicy subject matter about the naughty Internet.

4.4. Copyright issues

The ease of reproduction of digital information and of its transmission on the Internet makes copyright an extremely important issue in the context of the global network. The main concern of authorities has long been software piracy, raging on the web to such an extent that it is possible to find publicly accessible websites in the world from which anyone can download free software worth several thousand dollars. In Canada, the department of the Royal Canadian Mounted Police responsible for the enforcement of copyright admitted in 1997 that it could not even attempt to follow up the individual pirates, because it lacked the personnel for it (Scott). However, copyright does not include only software, but also any kind of intellectual property. In an attempt to monopolize its position on the Internet, Hollywood ordered Canadian and US students to withdraw the pages devoted to their favorite TV series, like *The X-files* (Barker). A third aspect of copyright problems is related to the nature of the Internet: the attribution of domain names often happens on a first come, first served basis. In the US, this policy was so strictly applied by the company in charge of domain name registration (InterNIC) that it did not hesitate to give away names like “www.mcdonalds.com” to individuals who subsequently made fortunes by reselling the rights to use these names to the slow-to-react multinational giants (Akin, “The Name Game”). However, in Canada domain name registration has always been done on a non-profit basis, which would not allow such incidents to happen under the .ca top-level domain. Therefore there have been only minor clashes over domain names, like in August 1997 in Edmonton (MacDonald), but that involved an address registered at the United States registrar (who accepts international requests as well).

We have to mention that the times are changing with respect to these copyright issues. New technological solutions have emerged in Canada and in the US to make it possible to keep track of digital copies of intellectual property (Camlot, “New software”), and also laws have been modified so that illegal copying will not only be punished if the offender makes a profit from it but also if he distributes it for free.

4.5. A special sense of humour

To finish this review of the misuse of the Internet in Canada, I will show how misuse can be “misused” through the power of irony. In Canada, the first signs of this type of approach appeared with The Canadianizer site, described in the section dealing with hatred (4.1.2.). Canadians seem to appreciate self-irony if it exposes the traits that make them specifically Canadian, as in the case of the Canadian Internet Licensing Board site, an April Fool’s Day joke of Toronto marketing firm Hip Hype Inc’d. inaugurated in March 1997 and still online. The site imagines what would happen if the rules about the proportion of Canadian content in other media were applied to the Internet. The mission statement of the licensing board is as follows:
The Canadian Internet Licensing Board (CILB) is a special operating agency authorized to process and issue English Language Canadian Web Site Licenses under Canada’s new Information Highway Act. Under this Act, Canadian Web Sites are invited to apply for a license to operate by March 31, 1998. Applications will be reviewed and licenses will be issued by the CILB on a first-come, first-served basis to Canadian Web sites that meet the Information Highway Act’s Canadian Web Site Guidelines.

One can get an idea about these guidelines by looking at the License Application Form of the board. The origin of the creators, of the tools used and of the content (consisting of Canadian cultural clichés such as ice hockey or Leonard Cohen) all count in this hilarious site evaluation form. The absurdity of the page was however not enough to convince some people that the whole thing was just a hoax, the affair got to the police and Hip Hype Inc’d were finally instructed to clearly indicate the humorous nature of their site by adding the following sentence at the bottom of every page: “In case you’re wondering, it’s a joke, eh!” (Hoare).

5. Conclusion

Thanks to its inherent structure, the Internet has so far proved to be able to overcome difficulties and remain the guarantor of free speech and individual initiative that it has been from the start. It is certainly far from being a perfect system, but as always in human history the drawbacks and undesirable effects of a technology derive from the imperfectness of human nature rather than from the evil deeds of a mystical “ghost in the machine”.

Governments, civil organizations and individuals are facing the same problems in every country developed enough to build their local part of the global network. Having provided an overview of the controversies deriving from the working principle of the Internet through Canadian examples, this paper hopefully provides a set of ideas on how to react to the emergence of what we like to call today “the information society”. Its main intention was to hold up a Canadian mirror to us, one in which we can see the reflections of all that is bad and good in the Internet policies and attitudes of our respective countries.

Endnotes

1. A methodological note. My research was based on surveys, media archives and handbooks. However, in the collection of information I limited myself to what is known as the World Wide Web. Therefore newsgroups, mailing lists and chatlines were not my target, even if their content appears on Web pages. Their usually informal style and subject matter would be adequate only for a more specifically sociological approach. As for the format of referencing to Web pages and other Internet resources, I followed the recommendations of the Modern Language Association. For references to entire websites (not only documents contained in them), I underlined their names, which is the standard usage for links on real web pages.
2. In this short summary of the prehistory of the Internet in Canada, I have used the Canadian Internet Milestones list from Carroll, Appendix A.

4. For more information, an exhaustive review in Hungarian can be found at index.hu/tech/net/internet/.

5. For this last number, it should be noted that the French have had their national version of the Internet, Minitel (unfortunately incompatible in its philosophy and design), for about twenty years and have found it difficult to switch over.

6. By April 2001, NUA indicated that the Canadian connectivity rate was 45 % of the population, whereas Hungary still lagged behind with a modest 11.5 %, overtaken by France at 20 %. Other Central and Eastern European countries were further ahead, like the Czech Republic with 26 % and Slovenia with 33 % of their populations connected. This shows that the big leap forward in the region is either still ahead or currently happening (in March 2002), hence the relevance of this study.

7. Unfortunately, the Canadianizer site has disappeared since.

8. The address is www.yahoo.ca/Regional/Countries/Canada/Society_and_Culture/Cultures_and_Groups/White_Supremacists/

Works cited

References in the article contain only the author of the text cited, unless the author in question has more than one citation in this list; in that case the short title of the appropriate text is added. If the name of the author of the document was not provided, I either designated the nature of the document, or marked it "unsigned", or indicated the name of the organization that created the document. The web pages referred to in this list were all retrieved between 1-10 March 1998, so they reflect the state of the World Wide Web at that time. All the press articles in the list were downloaded from the media archives of Electronic Frontier Canada (www.efc.ca/pages/media/). I included all bibliographic information found there. For further information on the original newspapers, library files can be consulted.

Definition of child pornography * Criminal Code 163.1 * 1993 *
insight.mcmaster.ca/org/efc/pages/law/cc/cc.163.1.html


ACNielsen * Canadian Internet Survey * – * Fall 1997 *
www.acnielsen.ca/ACNielsen/cgi-bin/DisplayPage?SITE=ACNielsen&KEY= survey97fall&TRACKID=MC_

Akin, David * Cracking the codes * The Hamilton Spectator * March 2, 1998 *
www.efc.ca/pages/media/spectator.02mar98.html

---------. * The Name Game Gets Serious * The Hamilton Spectator * February 23, 1998 *
www.efc.ca/pages/media/spectator.23feb98.html

Asseo, Laurie * Congress can’t ban smut on Internet, Supreme Court rules *


Barrick, Frances * 17-year-old charged over child pornography * Hamilton Spectator * August 7, 1997 * www.efc.ca/pages/media/spectator.07aug97b.html

Borovoy, A. Alan * Culture, not the law, should muzzle * The Toronto Star *
November 6, 1997 * www.efc.ca/pages/media/toronto.star.06nov97b.html

Petersen, Klaus and Hutchinson, Alan C. ed. Censorship in Canada * University of Toronto Press * 1998 * catalaw.com/logic/dt-censor.html

Riga, Andy * If cops can read E-mail, so can the bad guys * The Montreal Gazette * September 24, 1997 * www.efc.ca/pages/media/gazette.24sep97.html

Rowan, Geoffrey * Internet group strikes conduct code * The Globe & Mail page B3 * November 2, 1996 * www.efc.ca/pages/media/globe.02nov96.html


Rupert, Jake * Internet web site compares Parizeau, Bouchard to Nazis * The Ottawa Citizen * August 29, 1997 * www.efc.ca/pages/media/ottawa.citizen.29aug97.html


Skelton, Chad * Child-less Pornography * id Magazine * January 25, 1996 * www.efc.ca/pages/media/id.25jan96.html

Szklarski, Cassandra * Porn traders trapped in own Net * Canadian Press * December 15, 1997 * www.efc.ca/pages/media/cp.15dec97.html

Thompson, Elizabeth * Quebec controls Web * The Montreal Gazette * June 20, 1997 * www.efc.ca/pages/media/gazette.20jun97.html


unsigned * Injured Internet man saved by N.B. woman * The Toronto Star * April 11, 1997 * www.efc.ca/pages/media/toronto.star.11apr97.htm


Sites Cited

Canadian Association of Internet Providers: www.caip.ca

Canadian Internet Licensing Board: www.cilb.com

Canadian Radio-television and Telecommunications Commission: www.crtc.gc.ca

CANARIE: www.canarie.ca

Community Access Programme: www.cap.ca

DeathNet: www.deathnet.com
Electronic Frontier Canada: www.efc.ca
Freedom site: www.ftcnet.com/~freedom/
Information Highway Advisory Council: strategis.ic.gc.ca/SSG/
Internet Society: www.isoc.org
Legal Group for the Internet in Canada: catalaw.com/logic/
Office de la language Française: www.olf.gouv.qc.ca
Quebec North America’s Neo-Fascist State: unknown address, cannot be found with search engines in March 1998
SchoolNet: www.schoolnet.ca
The Canadianizer: www.io.org/~themaxx/canada/can.html (address not responding in March 1998)
Word Wide Web Consortium: www.w3.org
Zundelsite: www.webcom.com/~ezundel