# RECENT DEVELOPMENTS CONCERNING FREEDOM OF SPEECH AND PRIVACY IN THE CONTEXT OF GLOBAL COMMUNICATIONS TECHNOLOGY

The Honourable Frank Iacobucci*

## Introduction[1]

One of John Donne's immortal line is "No man is an island, entire of itself".[2] Like any phrase or sentence in literature, there can be many interpretations of it. To me, Donne was clearly saying that we human beings are interdependent and cannot live in some state of hermetic isolation.

History has proved Donne correct whether one looks to economic, political, social, or legal developments for support. In many ways, evolving global communications technology reflects both support for Donne's thesis and a challenge to it on which I wish to elaborate in discussing two of our most prized values: freedom of speech and privacy.

My choosing these values is not accidental but deliberate. My close friend, the Honourable John Sopinka, passed away a year ago on November 24th, 1997. On November 26th, 1994, John gave a speech on "Freedom of Information and Privacy in the Information Age", which he subsequently updated at Queen's University on November 26th, 1996 and in Calgary on September 15th, 1997, just two months before he died.

My comments today are an updating of John's remarks. But my main purpose in making these comments is to pay tribute to the life of a superb lawyer and judge whose "man for all seasons qualities" were taken from us far too soon and will not likely be replaced.

---

* Supreme Court of Canada. This is the text of a speech given at the Information Technology Law Conference in Toronto, October, 1998.

[1] I should like to express my thanks for the invaluable assistance of my law clerk, Wendy A. Adams, in the preparation of these remarks.

[2] *Devotions Upon Emergent Occasions* (1624), Meditation XVII: Nunc lento sonitu dicunt, Morieris.

## Freedom of Speech

*Conflicting Rights and Diversity of Regulatory Approaches*

Freedom of speech was established as an international human right, if only in aspirational terms, in 1948 with the proclamation by the United Nations of the *Universal Declaration of Human Rights*.[3] Since the inclusion of freedom of speech as a fundamental civil right within the *International Covenant on Civil and Political Rights*,[4] freedom of speech has arguably reached the level of an international norm. Domestically, freedom of speech is given explicit protection in most constitutional democracies, including Canada and the United States. However, in both the domestic and international contexts, as with other fundamental rights, sufficient flexibility exists for governments and courts to subject individual freedom of speech to such limitations as are thought necessary in democratic society to protect the rights and freedoms of others.

Accordingly, the permissible limitations on freedom of speech is a familiar issue in most legal systems. Legislatures and courts are faced with the difficult task of attempting to balance competing interests, namely the right to free expression, and the right not to be exposed to harmful or degrading expression which threatens inherent human dignity and equality. The advent of global communications technology, however, with its capacity for instantaneous dissemination of virtually unlimited amounts of information to a potentially universal audience, poses new challenges which threaten to disrupt the delicate balance that has been achieved to date in domestic legal systems.

The Internet, as the most visible structure of international communications technology, has fundamentally altered methods of accessing and disseminating information, with profound social, political and legal implications. Designed to support individual, autonomous access to a vast store of online information, the Internet provides global communications on a scale that previously could be achieved only by governments, businesses and organisations with sufficient resources to invest in the necessary infrastructure. Through a combination of public and private funding, the Internet puts worldwide communications within the reach of anyone who has access to a personal computer. It should not be forgotten, however, that in a world where only half the population has access to such fundamental technology as a telephone, increasing reliance on the Internet as a vehicle for information exchange and commerce by Western industrialised countries threatens to result in technological colonialism as developing countries remain isolated by their lack of access to technology.

---

[3] UNGA Res. 21 (III), UN GAOR, 3rd Sess., Supp. No. 13, at 71, UN Doc. A/810 (1948), adopted by vote 48-0, with 8 abstentions.

[4] *International Covenant on Civil and Political Rights*, 16 December 1966, Can. T.S. 1976 No. 47 (entered into force 23 March 1976; in Canada, 19 August 1976).

It is also necessary to come to terms with the essential and alarming paradox of this new communications technology. Decentralisation, which is the most important design feature of the Internet, has the potential to contribute significantly to the process of participatory democracy and the protection of human rights by expanding unrestricted access to information. The decentralised nature of the Internet, however, also has the potential to render superfluous government regulations and controls on either content or access which are considered desirable. While technological circumvention of domestic control allows citizens of authoritarian regimes an unheralded level of access to information and freedom of speech, it also renders democratic governments powerless in many ways to address the social harms of unlimited speech in the same manner as similar communications in other media.

The international political economy of information and technology reflects both the significance of economic development and social and political ideology in the diversity of regulatory approaches adopted to accommodate the challenges of global communications and commerce within existing legal institutions. One of the most significant distinctions underlying social and cultural values is the manner in which the persistent tension between liberty and equality is reconciled in terms of the limitations which are placed upon freedom of speech. While access to Internet communications technology and the accompanying dissemination of information is overwhelmingly concentrated in Western countries, particularly the United States, the relative homogeneity of political and cultural values does not equate to a uniform approach in balancing the rights of freedom of speech and protection from harm. At times, this cultural and legal diversity leads to interjurisdictional conflict as governments attempt to regulate access to and dissemination of information originating beyond their own territorial borders.

*Balancing Freedom of Speech and Protection from Harm in an International Communications Environment*

In many Western democracies, an acknowledged concern is that unlimited freedom of expression may result in exposure to harmful or degrading speech in a manner which abrogates or derogates from constitutional guarantees of equality. The United States and Canada, despite their analogous legal systems, represent in many ways two distinctly different ideologies in addressing this concern. The reasons for these differences are fascinating but beyond the scope of these remarks.

Both the Canadian and U.S. Constitutions enshrine and protect freedom of speech as a fundamental value which is essential to the proper functioning of a free and democratic society. Both Constitutions as well protect and promote basic equality as an inherent human right, essential to the dignity of all persons. Within the Canadian legal system, however, when these two values conflict in circumstances where freedom of speech threatens or results in harm to others, such speech is curtailed in order that

equality may prevail. Within the U.S. legal system, a limitation on freedom of speech in the name of equality is a solution which exists far beyond the doctrinal horizon. For the sake of discussion, I will refer to the Canadian approach as relativist and the U.S. as absolutist.[5]

Canadian courts have addressed the conflict between freedom of speech and protection from harm in two areas which are particularly amenable to global access and dissemination through Internet technology: pornography and hate speech. In *R v. Butler*,[6] the Supreme Court of Canada was required to balance the public interest in the constitutional guarantee of freedom of speech which extends even to obscene expression against an equally compelling public interest in protection from the harm that would result from exposure to such materials. The accused was a video store owner who was charged with selling obscene material contrary to the relevant provisions of the *Criminal Code* prohibiting the "undue exploitation of sex".[7] Through the pen of Mr. Justice Sopinka, the Court found the materials to be protected by section 2(b) of the *Canadian Charter of Rights and Freedoms*, which guarantees freedom of thought, belief, opinion and expression as fundamental freedoms.[8] Nonetheless, the Court concluded that the criminalisation of expression amounting to the "undue exploitation of sex" was a reasonable limit upon the right to freedom of speech, in accordance with section 1 of the *Charter*, as demonstrably justified in a free and democratic society. The Court recognised that materials which unduly exploit sex in a "degrading or dehumanising" manner may be prohibited on the basis that they are harmful to society in general and to the equality interest of women in particular.

In *R. v. Keegstra*,[9] he Court addressed a similar conflict between an individual's guarantee of freedom of speech and the public's right to be protected from harm. The accused, an Alberta high school teacher, was charged under the relevant provision of the *Criminal Code* with willfully promoting hatred against an identifiable group by communicating anti-Semitic statements to his students.[10] The Court concluded that hate

---

[5] That the U.S. approach is characterised as absolutist for the purposes of comparison is not meant to suggest that U.S. constitutional law does not contain qualifications or limitations upon the First Amendment right to freedom of speech. For example, speech which represents a "clear and present danger" in the form of inciting or producing imminent lawless action (*Brandenburg* v. *Ohio*, 395 U.S. 444 (1969)), or in the form of fighting words (*Cohen* v. *California*, 403 U.S. 697 (1974)) is not constitutionally protected from state regulation.

[6] *R. v. Butler*, [1992] 1 S.C.R. 452.

[7] *Criminal Code*, R.S.C. 1985, c. C-46, s. 163.

[8] *Canadian Charter of Rights and Freedoms*, Part I of the *Constitution Act, 1982*, being Schedule B to the *Canada Act 1982* (U.K.), 1982, c. 11, s. 2(b).

[9] *R. v. Keegstra*, [1990] 3 S.C.R. 697.

[10] *Criminal Code, supra* note 7 at s. 319.

speech is protected under section 2(b) of the *Charter*, but as with the circumstances occurring in *Butler*, this freedom is not absolute, particularly when the guarantee comes into conflict with other constitutional rights. The Court held that the relevant *Criminal Code* provisions constituted a reasonable limit upon freedom of expression in that protection from the harm flowing from hate propaganda which interferes with the basic human dignity and equality of targeted minority groups is an objective of sufficient importance to warrant overriding a competing constitutional guarantee.

Both of these cases dealt with limitations on speech produced and disseminated in traditional media. The challenge of addressing issues of pornography and hate speech in the context of the Internet is not that the nature of the expression itself has changed, or that the constitutional balance achieved between freedom and equality requires alteration. The Internet's definitive feature, its potentially unlimited capacity for access and dissemination, increases the magnitude of both the risk and the resultant harm from pornographic or hateful materials. The most serious challenge to domestic legal systems posed by the Internet is that this decentralised infrastructure requires universal enforcement in a world where domestic authority typically stops at the border. Legislatures and courts will be presented with troubling issues of jurisdiction in their efforts to impose domestic limitations upon speech which is essentially global in nature.

States which vary between absolutist and relativist in their approach to the right to freedom of speech will inevitably face both legal and technological conflicts where information that is perfectly legal in one jurisdiction can be accessed by those in a jurisdiction which prohibits such information. Early in 1996, a German prosecutor informed CompuServe, an American online services company with clients throughout the world, that allowing its German subscribers access to sexually explicit information would violate German law. Faced with growing competition in Europe in the provision of online services, CompuServe felt it had no choice but to block subscribers' access to the targeted information. The potential futility of national enforcement, however, is demonstrated by the fact that the same information could still be viewed computer users in Germany who had direct access to the decentralised Internet and did not need to rely on the gateway services provided by CompuServe. An additional complication is that it is generally not possible for Internet service providers to limit access with sufficient precision such that only prohibited material is denied. When Deutsche Telekom, a service provider for more than one million Germans, blocked access to a website based in California carrying the views of Toronto-based Holocaust denier Ernst Zundel, technical limitations forced it to block access simultaneously to **all** information originating from the same service provider.

These examples illustrate an important political and legal issue in terms of whether the United States, as a dominant Internet stakeholder, will be able to export successfully its libertarian and free-market ideological approach to Internet regulation to other countries, such as Canada, which currently adopt a different social welfare calculus. Both the "virtual export" and "involuntary import" of global communications results

from the decentralised nature of Internet communications: a decentralised network can adapt to local prohibitions by providing access from extraterritorial sites. The inability of domestic governments to regulate external sites could result in a *de facto* international regulatory regime established at the level of the lowest net regulatory burden.

An international defamation lawsuit that would have tested whether the absolutist American approach to free expression could prevail on the global Internet was recently settled by the parties involved. Dr. Laurence Godfrey, a British lecturer in physics and computer sciences, sued Cornell University and one of its former graduate students, Michael Dolenga, in the High Court in London, claiming that defamatory messages were posted on the Internet by the student.[11] Had the suit succeeded, the American Internet service provider and private individuals involved would have been held accountable not to their own domestic standards of free expression, but to the more rigorous approach of English libel law. On the other hand, had the suit failed, the result would be that England would be powerless to protect its citizens from what it views as the harmful effects of defamatory speech, disseminated not only in England but also available worldwide.

*Resort to Methods of Prior Restraint*

Faced with public demands to address the availability of unrestricted harmful speech on the Internet and the difficulty of enforcing national laws, governments are beginning to resort to technological rather than legal solutions, such as filtering software. Filtering software screens and limits material available on the Internet by blocking access to information based on a list of prohibited keywords contained in the software's database. This technology is presented as a viable alternative to overly broad governmental regulation, but the implementation of such forms of prior restraint is far from unproblematic. Existing filtration programs are blunt instruments of censorship, incapable of making contextual judgements as to content of information. For example, the inclusion of keywords with sexual connotations is ostensibly justified as a method of protecting children from sexually explicit materials available online, but the censored keywords also block access to sites with socially desirable information such as breast cancer research, assistance for victims of sexual abuse, and public health information relating to HIV and AIDS. Filtration software is also notorious for blocking access to lesbian and gay information services, notwithstanding that the censored sites contain no

[11] Carl S. Kaplan, "Suit Against Cornell Dropped in International Libel Case" *The New York Times* (6 November 1998). Professor Godfrey is apparently proceeding, however,With a defamation law suit against an Internet service provider carrying on business in England and Wales; see *Godfrey v. Demon Internet Ltd.*, [1999] E.W.J. No. 1226 (H.C.J.).

sexually explicit material, but simply provide information, education, resources and calendars of events.

The United States, with its absolutist approach to freedom of speech, is oddly enough the site of recent controversies wherein censorship of online information has been initiated by the state. In February 1996, a coalition of groups led by the American Civil Liberties Union filed suit to challenge the constitutionality of the federal Communications Decency Act of 1996 (the "CDA").[12] The CDA contained censorship provisions aimed at protecting minors by criminalising the "knowing" transmission of "obscene or indecent" messages through the Internet to any recipient under 18 years of age. In *Reno v. ACLU*,[13] the Supreme Court of the United States found the provisions to be an impermissibly vague limitation on the constitutional guarantee of freedom of speech, and further that a ban on transmitting indecent materials to minors also posed an unacceptable risk that socially valuable speech, such as information about birth control, sexuality and AIDS, would be restricted as well. The Court held that while Congress has a legitimate interest in protecting children from harmful materials, this interest does not justify an unnecessarily broad suppression of speech addressed to adults. A second challenge was recently filed in response to the subsequent Congressional attempt at online censorship, the *Child Online Protection Act*, which makes it a federal crime to "knowingly" communicate "for commercial purposes" material considered "harmful to minors".[14] On November 19th, a federal court in Philadelphia issued a temporary restraining order enjoining enforcement of the *Act*.[15]

Following the failure of the CDA, the United States Congress and various funded agencies have attempted to achieve similar results through indirect means. Congress has sought to condition the receipt by schools of federal funds on the installation of filtering software on computers available to students.[16] Libraries, under pressure from local boards, have begun to install filtering software on public access terminals available to library patrons. By installing technical means of prior restraint on library Internet terminals, however, public libraries may be engaging in an unconstitutional violation

---

[12] 47 U.S.C. §223 (1996).

[13] *Reno v. American Civil Liberties Union*, 521 U.S. 844 (1997).

[14] 47 U.S.C. §231 (a)(1)(1998).

[15] Order by United States District Judge Lowell A. Reed, Jr., in *ACLU* v. *Reno*, the United States District Court for the Eastern District of Pennsylvania, Civil Action No. 98-5591, November 19th, 1998.

[16] See for example the Children's Internet Protection Act, S. 1619, a bill introduced on February 9,1999, by Senate Commerce Committee Chair John McCain, (R-AZ), and approved by the Committee March 12, 1999. The proposed legislation would deny eligibility for telecommunications discounts authorized by the Snowe-Rockefeller provision of the Telecommunications Act of 1996 to schools and libraries that do not certify the use of a filtering or software filtering system.

of their patron's freedom of speech. In December 1997, a grassroots organisation filed a federal lawsuit in an attempt to stop Internet usage policy of the public library system of Loudoun County, Virginia. The policy required that filtering software designed to block access to pornographic sites be installed on all public access Internet terminals in the library system.[17] The threat of prior restraint has become so pronounced that the American Library Association felt compelled to issue an official statement of its position that filtering software blocks information which is protected in the United States by the First Amendment"s guarantee of freedom of speech, and is inimical to the basic function of libraries to provide public access to information.[18]

*Freedom of Speech as a Fundamental Human Right in Context*

In Western countries, our understanding of issues relating to freedom of speech on the Internet tends to focus on those concerns with which we are most familiar. We are fairly sophisticated in our appreciation of the tension between unlimited freedom of speech and the need to protect ourselves from the harmful effects of unrestricted pornography or hate speech. We may differ among societies, and even within societies, on the proper balance that legislatures and courts should attempt to achieve between the competing fundamental values that are engaged. In most Western democracies, however, we are fortunate to live in political systems that permit us the luxury of debate as to the degree of limitation which should be allowed; we need not advocate in peril for our right to freedom of speech itself. The same cannot be said of every other country.

As Western societies begin to cooperate to address the legal issues posed by global, unrestricted access to and dissemination of information on the Internet, we should be mindful that the international regulatory regimes and precedents we establish must protect not only the delicate balance between free speech and protection from harm in Western societies, but should also promote and protect an entitlement to free speech for those living under more repressive and authoritarian regimes. We need to proceed with caution and appreciate the necessity of a truly international perspective in dealing with an international communications medium. Without such a perspective, the potential exists that Western democracies, as the current dominant stakeholders of the Internet community, will establish domestic and international regulatory controls which achieve the objectives of our own domestic welfare calculus while simultaneously providing authoritarian regimes with the technical and legal precedents of online oppression.

---

[17] Carl S. Kaplan, "In Library Filtering Case, an Unusual Ally" *The New York Times* (2 October 1998).

[18] Statement of the American Library Association to the Senate Commerce, Science and Transportation Committee on Indecency on the internet, Hearing Record, February 10, 1998. Available on the Internet at the Association"s website at http://www.ala.org/washoff/mccain.html.

Unless we can be confident that regulatory controls are sufficiently contextualised, we should be aware that the same tools, whether doctrinal or technical, which protect us from harm can be used indiscriminately to withhold access from others.

## Privacy

### *The Implications for Privacy of Global Access and Dissemination of Information*

A right to privacy is recognised as a fundamental human right in all major international treaties and agreements on human rights. Nearly every written constitution also recognises privacy as a fundamental human right, either explicitly or implicitly. In both Canada and the United States, constitutional protection of an individual right to privacy has generally taken the form of restricting undue state interference with either behavioural privacy or the right of citizens to personal autonomy in making personal decisions and fundamental life choices. The increasing volume of personal information being collected by both governments and private commercial interests, however, along with the emergence of the Internet as a vehicle for worldwide communications and commerce, has shifted the focus of concern from behavioural to informational privacy, the latter being understood as the ability to control the collection and use of personal and intimate details of one's identity and life. New technology, particularly in the private sector, is beginning to erode this right of privacy, and neither domestic nor international law has kept pace with these developments.

Canadians perhaps initially considered the impact of wide-scale computerised record-keeping on individual privacy rights when the federal government adopted the social insurance number. We were assured that the number was not intended as a form of universal identification, and were instructed that we were legally required to submit our social insurance number for employment purposes only. The convenience of this unique identifier, however, was difficult for both governments and commercial organisations to resist. It appears that lack of awareness as to the implications has led to the current state of affairs whereby Canadians regularly provide their social insurance number on a wide variety of application forms such as licenses, video store memberships and credit cards.

While both federal and provincial governments in Canada have enacted legislation that places strict controls on the collection and use of personal information by the state, the private sector has been left largely unregulated. Prior to the advent of networked communications technology, the threat to privacy posed by commercial interests was relatively benign. The combination of mergers and acquisitions in the financial sector, however, along with technological developments which permit large, distributed databases to exchange information, has resulted in an increasing consolidation of personal information. More information is being collected than ever before, and is being aggregated and widely disseminated to a degree of which most Canadians are unaware. The collection of personal information, when confined to specific uses and

isolated within individual databases, poses relatively little threat to individual privacy. When communications technology permits this information to be consolidated, however, the result is a gradual buildup of intrusive personal profiles by private sector actors who remain largely unregulated.

Increasing use of the Internet also poses a serious threat to individual privacy, not simply owing to a lack of regulation in the private sector, but also because most users are unaware of the information that is collected during online sessions. A standard request for a World Wide Web document provides the name of the computer associated with the requester, the date and time of the request, the name and location of the requested file, and the last site the requester visited. Some websites also transfer information to the hard drive of the person viewing the site in a file known as a "cookie". Upon subsequent visits, this information on the requester"s hard drive can be viewed and modified by the operator of the website. In effect, a cookie functions as a passport issued by the website to each requester, which is viewed and stamped on subsequent visits. The cookie, or passport, typically contains a history of all of the Internet sites the user has accessed. Cookies were originally designed for the technical purpose of facilitating interaction between websites and viewers by providing website owners with the information necessary to increase the efficiency of website operations. Corporate website owners soon realised, however, that cookies could also be used to provide personal information concerning vistors' consumer habits, allowing companies to build a profile on each potential customer for marketing purposes.

The legal regulation of access to personal information, with its emphasis in both Canada and the United States on the public sector, has not kept pace with the increasing threat of privacy posed by online technology such as the Internet. Individuals have a dangerously naïve sense of privacy when they use these communications technologies, perhaps because access is conducted in the relatively anonymous environment of interaction between an individual"s own personal computer and an unseen, faceless communications server.

The vulnerability of personal privacy in this ostensibly anonymous environment was recently demonstrated in a situation involving the United States Navy's attempt to dismiss a gay sailor. Homosexuality is grounds for discharge from the United States military, but the recently implemented "don't ask, don't tell" policy presumably protects servicemen and women by prohibiting them to reveal their sexual orientation, and by prohibiting the military from making inquiries. Senior Chief Petty Officer Timothy R. McVeigh, who is no relation to the Timothy McVeigh recently convicted of the Oklahoma City bombing, served as the top enlisted man aboard a U.S. Navy submarine. He was threatened with discharge from the Navy when it was discovered that his member profile for America Online, an online service provider, contained the word "gay".

All America Online members are given "screen names" which identify them in online interactions without revealing their real identity. Each individual has the option of placing information about himself in a profile which members can use to identify other members of the online community with similar interests, hobbies or lifestyles. Timothy McVeigh identified himself in this profile as "Tim from Honolulu", and in the category of marital status, had written "gay". When Navy personnel contacted America Online and asked for the real identity of "Tim from Honolulu", America Online provided Timothy McVeigh"s name from its customer records, despite its' policy of protecting the privacy of its members. The Electronic Communications Privacy Act (the "ECPA"), however, prohibits any federal government agency, including the Navy, from seeking, and online service providers like America Online from releasing, any personal information to the federal government in the absence of appropriate prior authorization such as a warrant.[19] Accordingly, a federal court judge enjoined the dismissal of McVeigh after finding that the Naval investigators "likely" violated the ECPA when they requested and received the confidential subscriber information from America Online.[20]

The Alberta Court of Queen's Bench recently dealt with a similar situation in Canada in *R. v. Weir*.[21] The accused was charged with possession of child pornography after his Internet service provider discovered an e-mail message containing pictures of children in sexual positions. The Internet service provider released this information to the police, who then obtained a warrant to search the accused"s residence. A computer and disks containing further pornographic pictures of children were subsequently seized. The accused argued that e-mail carries an expectation of privacy, and that the police had conducted a warrantless search and seizure by requesting and receiving access to the initial e-mail message without prior authorization. While the court found that e-mail did carry a reasonable expectation of privacy, this privacy was less than could be expected with first class mail. The court accordingly ruled that the evidence was admissible and then accused was convicted.

*Private Sector Data Collection and "Creeping Surveillance"*

The potentially negative impact of communications technology on personal privacy derives not only from the increasing ease of global communications made possible by the Internet, but results as well from the manner in which networked communication permits wide-scale consolidation of the information contained in numerous databases in both the public and private sectors. In effect, the increased collection and consolidation of individual items of personal information results in a form of "creeping

---

[19] 18 U.S.C. §2701 et seq.

[20] See *McVeigh* v. *Cohen*, 983 F. Supp. 215 (Dist. D.C., 1998).

[21] *R. v. Weir*, [1998] A.J. No. 155 (Alta. Q.B.).

surveillance". The implications of this surveillance by installment are of particular concern in commercial transactions, given the almost total lack of regulatory controls in the private sector with respect to the permissible extent of information that can be collected, and the uses that commercial organisations can make this information.

In the absence of privacy legislation, companies are able to consolidate a large amount of information not only by maintaining their own transaction history databases, but can also augment this information by purchasing transaction histories and the associated personal details from other companies. It is almost impossible to proceed through one"s daily routine in a manner which avoids collection of personal information that is added to these corporate databases. Automated teller machines record the time, date and location of every transaction. If you rely on a magnetic stripe pass to enter the office, your location is automatically recorded as you move through the building. Every purchase of goods or services charged to a credit card is available in a database to which the police, among others, have access. Surveillance cameras in banks, government buildings and convenience stores record you image. If you use a company health plan to purchase prescription drugs, your employer (or even a potential employer) may have access to the details of your medication history. If all this information is consolidated, the result is a fairly complete electronic record of your day, available both for sale and purchase by others. A novel niche market has even developed whereby professional researchers will search online databases and the Internet to compile a dossier of personal information in response to requests from those interested in as much detail on others as possible, such as current and potential employers.

Perhaps the greatest threat to personal privacy in the commercial sector comes from a rather recent development, which is the use of pooled customer information by companies for marketing purposes. Companies have always collected detailed information about their customers in the form of transaction histories, but have only recently begun to consolidate transaction histories in data warehouses and to adopt sophisticated analytical techniques of "data mining" to identify trends and buying patterns that will provide them with a competitive edge. Companies soon learned that they could compile even more comprehensive information through the use of centralised reward programs, such as air miles, which provide them with a more complete data picture of consumer habits. Consumers who take advantage of rewards programs may not be aware that their statistical history is available to each and every commercial sponsor of the program, and that currently no legislation exists which would prevent the sponsors from selling this personal information to others. At present, no clear ethical or legal line has been drawn to distinguish between appropriate methods of data collection and analysis for marketing purposes, and excessive data collection that amounts to an unacceptable level of surveillance of the private lives of individuals. While information concerning an individual transaction may not pose much of a threat, most consumers would no doubt be somewhat unsettled to know that companies are compiling a complete statistical history of their consumer transactions over extended

time periods, and that they have no control over the manner in which companies use or distribute this information.

*Privacy, National Security and Domestic Law Enforcement*

The right to privacy is not absolute in that, in most domestic legal systems, the right must give way to a countervailing public interest in safety and security. Constitutional democracies such as Canada and the United States typically implement a prior authorization procedure whereby law enforcement and national security personnel are subject to strict due process requirements before a breach of privacy will be permitted. Authorities responsible for both domestic and international security, however, are increasingly concerned that criminals and terrorists can take advantage of technological developments to shield their communications and activities from surveillance. Private individuals, on the other hand, while concerned with public safety, also have a strong interest in limiting the manner in which the state can use surveillance technology on its citizens.

An essential component of the privacy of electronic information is the ability to keep the data secure from unauthorised access. Just as information in paper-based files and documents is kept secure in a physical medium through the use of locks, the security of information in an electronic communications medium such as the Internet can be protected by cryptographic methods which mathematically scramble the original text. Cryptography protects the confidentiality of information by using "digital keys", a unique combination of ones and zeros that an individual can use to encrypt and decrypt digital data. Without access to the correct key, data encrypted to ensure confidentiality can only be decrypted by the use of "brute force" decoding techniques whereby all possible permutations of the key must be tried. Cryptographic strength is therefore relative to the length of the cryptographic key. In July 1997, it took 78,000 computers working together on the Internet 96 days to crack a message encrypted with DES (the Data Encryption Standard), a key algorithm that uses a 56-bit key.

Prior to the advent of individual access to global communications networks such as the Internet, cryptography policy and technology were almost exclusively of interest to governments. Cryptography was used to protect military secrets and national security, and the current Canadian policy and legal framework reflects this orientation. Canada is a signatory, along with 33 other nations, to the *Wassenaar Arrangement* that was established to address regional and international security concerns with respect to the buildup of weapons of mass destruction and sensitive technology with military

applications.[22] The provisions of the *Arrangement* require states to adopt export controls on a long use of "dual-use" products, including cryptography technology. Canada has implemented these provisions in the form of export control regulations which restrict the export of customised encryption software or hardware. The export of mass-marketed encryption software is unrestricted, however, and there are no constraints on the import or domestic use of cryptographic software.

While the original focus of cryptographic policy may have been on national and international security and the threat of force from other states, a more pressing concern these days is the insistence by law enforcement authorities and national security agencies in both Canada and the United States that access to strong cryptography in the hands of individuals threatens public safety by limiting the surveillance capacity of the state over criminals and terrorists. In the United States, the Clinton Administration advanced what was known as the "Clipper Chip" proposal, a government-imposed encryption standard that would be embedded in all new forms of communications technology and would enable law enforcement authorities to have unlimited access to private communications, subject presumably to due process guarantees. Widespread opposition from both the public and the technology industry led to the defeat of the proposal.

While universal state access to technology used in private communications may no longer be a live issue in the United States, the surveillance capacity of law enforcement authorities continues to expand in an *ad hoc* fashion. In the 1980s, Congress determined that the legal protection of privacy had not kept pace with technology, and concluded that without statutory protection for rapidly expanding wireless and digital communication technologies such as e-mail, citizens faced a steady erosion of their privacy rights. Accordingly, in 1986, Congress enacted the ECPA, discussed above in relation to online privacy, prohibiting interception and disclosure of "electronic communications".

In response to FBI concerns, however, that technological developments were impending law enforcement's electronic surveillance capabilities, Congress subsequently enacted the Communications Assistance for Law Enforcement Act ("CALEA"), which generally requires a telecommunications carrier to ensure that its equipment, facilities or services are capable of interception pursuant to lawful authorisation and to provide access to call-identifying information.[23] In response to

---

[22] The *Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies* (WA), the first global multilateral arrangement on export controls for conventional weapons and sensitive dual-use goods and technologies, received final approval by 33 co-founding countries (including Canada) in July 1996 and began operations in September 1996.

[23] 47 U.S.C. §1002(a)(1)-(4).

CALEA proceedings initiated by an FBI petition, the Federal Communications Commission on November 5th, 1998 issued a statement expressing its initial approval of the technical requirements proposed by the FBI that would enable law enforcement authorities to determine the location of individuals using cellular phones.[24]

Canada recently initiated a review of its own cryptography policy as part of the initiative undertaken by Industry Canada's Task Force on Electronic Commerce. Industry Canada defines electronic commerce as "the conduct of commercial activities and transactions by means of computer-based information and communications technologies". The mandate of the Task Force on Electronic Commerce is both to study the implications of electronic business practices and to create policy for the so-called "information highway". Its primary objective with respect to privacy issues is to develop a national policy for protecting the privacy of personal information while still allowing for the flow of information necessary to participate in the global information economy.[25]

In February 1998, the Task Force tabled its report of cryptography policy, "*A Cryptography Policy Framework for Electronics Commerce – Building Canada's Information Economy and Society*",[26] listing possible scenarios for government regulation of cryptography.

Among the proposed alternatives was mandated law enforcement access to encrypted communications by prohibiting the use of products without key-recovery or key-escrow capabilities. Advocates in support of government restriction on the use of encryption technology include the Canadian Association of Police Chiefs, the RCMP, CSIS and the Communications Security Establishment, all of which have expressed concerns about losing the ability to intercept electronic mail or voice communications when conducting investigations. Apparently only a few countries, however, favour the development of key-escrow or key-recovery techniques. While unlimited access to strong cryptography is thought by some to compromise public safety by placing criminals and terrorists beyond the surveillance capacity of law enforcement authorities, others feel that key-escrow or key-recovery technology creates an inherent risk of unlawful interception of personal communications and financial transactions data, including the potential for unlawful access by state authorities.

On October 1, 1998, Minister of Industry, the Honourable John Manley, announced Canada's revised cryptography policy as an essential component of the Canadian

---

[24] A formal Notice, including the requisite request for public comment, was released on November 5, 1998. The Commission rejected other capabilities requested by the Bureau and deferred decisions on other issues, including surveillance of Internet communications.

[25] Information on the Task Force is available on the Internet at http://e-com.ic.gc.ca.

[26] The Policy is available at http://strategis.ic.gc.ca/crypto.

Electronic Commerce Strategy, designed by the federal government to position Canada as a world leader in the use of electronic commerce by the year 2000. The policy allows Canadians to develop, import and use whatever cryptography products they wish, and does not impose any mandatory key-recovery requirements or licensing regime. It appears that the government is seeking a balanced approach that will encourage the growth of electronic commerce while maintaining the capacity of law enforcement and national security agencies to ensure public safety. To this end, the government is proposing amendments to the *Criminal Code* and other statutes as necessary to deter the use of encryption in the commission of a crime, and to apply existing interception, search and seizure procedures to cryptographic situations and circumstances.[27]

*Regulatory Diversity and the Necessity of Cooperation*

In the current global communications environment, one can discern extensive regulatory diversity as states adopt different approaches to protecting the privacy of online personal information and the security of financial transactions. Each state will impose a regulatory burden on the private sector which is sufficient to achieve its own domestic welfare objectives in terms of balancing the right of privacy against the requirements of commercial activity for the free flow of information and the occasional but important need to breach personal privacy in order to protect public safety. Given the exigencies of international trade and finance, however, in combination with the decentralised nature of Internet communications, the question becomes whether regulatory arbitrage will result in a global standard of privacy being set at the level of the lowest net regulatory burden. In a classic "race to the bottom" scenario, states which initially pose a high net regulatory burden will be unable to maintain a position of comparative advantage in international trade and finance unless they decrease the available level of privacy protection to the standard of the lowest common denominator.

The first mover in the international arena in this area is the European Union. Europeans have benefited to a much greater degree than North Americans from strict and comprehensive privacy laws which protect personal information regardless of whether it is collected by the public or private sector. In contrast, in both Canada and the United States privacy legislation generally applies only to the public sector. What protection is available in the private sector is largely sectoral or self-regulatory rather than legislative in nature. The informal regulatory approach to the protection of personal privacy found in both the Canadian and U.S. systems, however, may soon be required to give way to more substantive measures in the face of increasing international economic pressure resulting from the provisions of the European Union's

---

[27] Information on Canada's cryptography policy is available on the Internet at http://e-com.ic.gc.ca/english/fastfacts/43d7.htm.

*Data Protection Directive* which took effect on October 25th, 1998.[28] The *Directive* is intended to protect personal privacy by prohibiting the improper collection, use and transfer of data relating to individuals. For EU member countries, the effect of the *Directive* is to harmonise the flow of cross-border information between member countries, replacing the previous confusing and conflicting standards imposed by multiple regulations and procedures.

The data law sets a standard of legal rights for EU citizens which far exceeds the level of protection accorded to either Americans or Canadians at this time. Article 25 of the *Directive* establishes rules to ensure that personal data is transferred to countries outside the EU only when the continued protection of the data is guaranteed, thus ensuring that the high standards of privacy protection introduced by *Directive* are not undermined. As a result, many U.S. or Canadian companies with European operations, or with significant trade relationships with European companies, could find their commercial activities disrupted. Depending on the economic strength of the EU in international trade and financial services, and the strength of its commitment to enforcement, the potential for regulatory arbitrage could be greatly reduced if other states respond by raising their own levels of privacy protection accordingly.

The EU has provided a safety valve, however, which takes into account the necessity of avoiding massive disruptions to commerce or initiating a trade war with strong trading partners such as the United States. While the basic rule of Article 25 is that data should only be transferred to a non-EU country if it will be adequately protected in the destination location, adequacy does not necessarily require a non-EU country to apply legislation similar to the EU *Directive*. In addition, Article 26 provides a practical system of exemptions and special conditions. Data transfer will be allowed to countries without adequate protection in given circumstances, such as when the data subject has consented to the transfer, or if the transfer is necessary for the performance of a contract between the data subject and the transferring entity. Aware of the international economic implications of the *Directive* and its possible adverse effect on international trade and finance, the Commission is involved in discussions with a number of non-EU countries in order to explore methods of avoiding possible interruptions in the flow of information. The U.S. Department of Commerce and the European Commission have discussed creating a "safe harbour" for U.S. companies that voluntarily adhere to certain privacy principles, based on the *1980 OECD Privacy Guideline*.[29]

---

[28] "Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data", *Official Journal of the European Communities* of 23 Nov1995, No. L. 281, p. 31.

[29] The text of the *Guidelines* is available at the OECD website at http://www.oecd.org.

Canada appears to have initiated reform of its own legislative framework much earlier than the United States. In May 1996, the Minister of Industry announced that the federal government would develop legislation to protect personal information in the private sector. This commitment was reiterated by the Minister of Justice in September 1996. In January 1998, Industry Canada and the Department of Justice released a consultation paper entitled "*The Protection of Personal Information – Building Canada's Information Economy and Society*", and solicited comments from the public.[30] Finally, on October 1st, 1998, the Honourable John Manley, Minister of Industry, supported by the Minister of Justice and Attorney-General of Canada, the Honourable Anne McLellan, introduced a new privacy legislation bill titled *The Personal Information Protection and Electronic Documents Act.* The bill contains measures to protect personal information in the private sector, as well as creating an electronic alternative for doing business with the federal government and clarifying the assessment of the reliability of electronic records used as evidence.[31]

The privacy provisions are based on the Canadian Standards Associations *Model Code for the Protection of Personal Information*, recognised as a national standard in 1996.[32] They address the manner in which organisations collect and disclose personal information, the requirement to seek consent of the individual concerned, the right of individuals to have access to personal information collected by others, and the right to have information about themselves corrected if necessary. The provisions will initially apply to the federally-regulated private sector, as well as trade in personal information that occurs inter-provincially or internationally. Three years after coming into force, the regulations will apply more broadly to all personal information collected, used or disclosed in the course of commercial activities. In circumstances where a province adopts legislation that is substantially similar to federal regime, as is the case with Quebec's existing privacy law, the organisations covered will be exempted from application of federal law.

Some might argue that the application Article 25 of the European *Directive* results in an illegitimate extraterritorial application of national privacy laws, but it would appear that the reality of integrated global communications is that a rough harmonisation process is inevitable. Strongly held legal values are exported through a

---

[30]The publication is available on the Internet at http://strategis.ic.gc.ca/SSG/pv01169e.html.

[31] Bill C-54, *An Act to support and promote electronic commerce by protecting personal information that is collected, used or disclosed in certain circumstances, by providing for the use of electronic means to communicate or record information or transactions and by amending the Canada Evidence Act, the Statutory Instruments Act and the Statute Revision Act*, 1st Sess., 36th Parl., 1997-98.Information on the bill is available on the Task Force's website at http://e-com.ic.gc.ca/english/releases/41d7.htm.

[32] The text of the Model Code is available from the Canadian Standards Association, Document No.CSA Q83096.

combination of first-mover status, political consultation, and at times, economic leverage. Multilateral give-and-take will eventually result in the progressive development of international privacy norms. The beginnings of an international consensus among Western states is evidenced by the results of the recent OECD Ministerial Conference held in Ottawa in October 1998. The Ottawa Conference was the second major international meeting within the overall OECD effort on electronic commerce. One of the outcomes of the meeting was *Ministered Declaration on Protection of Privacy on Global Networks*.[33] While the *Declaration* sets a tone that is more aspirational than obligatory in encouraging states to work in tandem with the private sector on privacy issues, it nonetheless reaffirms the importance of privacy protection and the original principles contained in the *1980 OECD Privacy Guidelines*.

**Conclusion**

Recent developments in global communications technology, particularly the Internet, have significant implications for the constitutional guarantees of freedom of speech and privacy. The decentralised nature of the global communications infrastructure presents both a challenge and an opportunity to states as they seek to integrate diverse cultural values and regulatory regimes to address the legal issues involved in protecting these fundamental civil rights in an online environment.

Technology alone does not change the nature of the balance between the competing interests of freedom of speech and protection from harm. Instead, the challenge is to achieve some degree of regulatory control over a global medium. The Internet's decentralised infrastructure frustrates traditional regulatory options, as communications which are prohibited locally may nonetheless be accessed and disseminated in another jurisdiction. While Western democracies deal with the jurisdictional challenges in attempting to preserve domestic trade-offs between liberty and equality in terms of freedom of speech in online environments, it cannot be forgotten that for many of the world's population, access to the Internet may be the first opportunity to speak freely to a wide audience. Nor can it be forgotten that the increased pace of global technological development threatens to leave behind those nations without the resources to build the necessary communications infrastructure. It would appear that existing stakeholders in the Internet environment should do everything in their power to encourage universal international participation in global communications technology.

The advent of electronic commerce has created a significant threat to personal privacy both in Canada and the United States. Privacy legislation covering the public sector must somehow be extended appropriately to cover commercial activities in the private sector. The sheer volume of personal information contained in commercial data

[33] The text of the *Declaration* is available at the OECD website at http://www.oecd.org.

warehouses places consumers under a form of "creeping surveillance" which may breach individual rights of privacy. Not only must the fundamental civil right of privacy be protected as a constitutional guarantee, but in practical terms, privacy protection is also essential to foster the growth of electronic commerce. For countries such as the United States which have yet to take the necessary steps to address privacy and security of information in the private sector, the pull of an international consensus within the context of global communications and international trade may soon alter domestic policy. Global communications and electronic commerce have initiated a multilateral dialogue that cannot be ignored, no more than John Donne's observation several hundred years ago can be forgotten.