24

The politics of privacy on the global information highway

Richard S. Rosenberg
Department of Computer Science, University of British Columbia, Vancouver, B.C. Canada, V6T 1Z4
Phone: +1 604 822 4142; Fax: +1 604 822 5485
Email: rosen@cs.ubc.ca

Abstract

In this paper, we will explore a number of political issues associated with the debate over privacy concerns on the information highway. Among the approaches that have been proposed for protecting personal privacy, especially in North America, the four main ones are government legislation, self-regulation, security, and education. In this paper, a position in support of government legislation for privacy protection is adopted and defended over voluntarism and self-regulation. Most of the sources used are reports, proposals, and statements, produced or commissioned by government agencies in Canada, the United States (US), and the European Community. Given that governments have political agendas that are shaped by a combination of forces, it is a necessary and important exercise to identify the items on these agendas and to evaluate their relative strengths in order to anticipate the likelihood that personal privacy will be adequately protected in the future. Current privacy policies in Canada and the US are similar and differ substantially from those of many European countries.

INTRODUCTION

> 'If you're worried about privacy in the emerging electronic age, you're not alone. I'm worried too ... The need for explicit policies and appropriate laws arises from the efficiency of information technology. As long as it was impractical for large amount *[sic]* of personal information to be collected and distributed, only modest regulation of privacy was needed. But once gathering and sharing information became easy, the need for explicit guidelines will be evident' (Gates, 1995).

An Ethical Global Information Society J. Berleur & D. Whitehouse (Eds.)

It will be assumed that the term privacy is reasonably well understood, although considerable debate exists about an acceptable working definition. The following definitions are useful for the present purposes:

> Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others (Westin 1967, p. 7).
>
> Privacy refers to the social balance between an individual's right to keep information confidential and the societal benefit derived from sharing information, and how this balance is codified to give individuals the means to control personal information (*Information Security and Privacy in Network Environments*, 1994, Footnote 11, Chapter 1).

Note that both of these definitions refer to the ability and indeed the right (claim?) of individuals to control personal information. The growth of commercial activity on the Internet is creating vast amounts of such information.

The technological assault on personal privacy continues to accelerate on many fronts. Whether it is the video camera monitoring virtually every banking activity as well as other financial transactions or indeed ubiquitous closed circuit systems in public squares or the increasing use of smart cards that capture enormous amounts of transactional information, virtually every action in the marketplace adds to the growing databases of personal information. On the horizon are smart cards with microchips that can store such information and much more in a distributed fashion. For network *aficionados* there are web browsers that download information to most web sites visited. Microsoft's Windows 95 has the facility to scan a user's system to determine the kinds of application programs present and then to transmit this information when the Microsoft network is accessed, unless the user actively declines to participate. Commercial networks such as America Online and Prodigy monitor the activities of their clients to make sure that certain questionable words are not being used in chat rooms, where individuals can discuss arbitrary topics in a closed environment. This list could easily be extended.

In what follows, the policies of the governments in the US and Canada will be compared with the policies adopted in the European Community. Current privacy policies in both of these countries are generally similar, with certain important differences. However, they both differ substantially from those of many European countries. These differences and similarities will be explored later as well as the social and political implications. As a preview of the choices that could be made with respect to privacy concerns, consider the following list provided in a discussion paper (*Privacy and the Canadian Information Highway*, 1994) released early in October 1994 by the Information Highway Advisory Council (IHAC) in Canada, a government appointed body: legislation and regulation, voluntary codes and standards, technological solutions, and consumer education. (See Appendix A for more detail.) In one way or another, these four approaches, individually or in concert, underlie the range of discourse in North America. Of course, the European Community has decided that the first approach is the appropriate way to proceed and has done so by virtue of the Privacy Directive adopted in June 1995, to become effective in 1998.

Some threats to privacy

One fairly insidious example, on the Internet, is the use of cookies or 'client-side persistent information' by Netscape's browser as well as Microsoft's Internet Explorer. These browsers gather information about your shopping habits and make it available for subsequent perusal by downloading it without your knowledge onto your hard drive. Of course the official Netscape line is that, 'cookies are beneficial to the Web ... shopping done via the Web could be gradually gathered in the cookies file, and then paid for (as if at a supermarket checkout) when the user enters the appropriate page. The concept can also be used to create a permanently customized view of a site - if you regularly have specific needs from a search engine, for example' (*Netscape's Cookies Crumble*, 1996). There is more, 'a Cookie program can be built to track the user's every move while connected to a particular server. This information can then be fed into a database to keep statistics on site usage so Webmasters can tailor a site to a particular user's interests ... Combine Cookie with JavaScript and a site's administrator could launch a very effective direct mail campaign without ever having asked the user for permission ... In more malevolent hands, these new tools can do far worse. For example, a Webmaster could pretend to be a particular site in order to retrieve a user's Cookie data without authorization. "If you use a server that does not encrypt its information, there is a real problem."' (Yang, 1996).

InfoSeek, a web search engine, plans to track information stored in users' cookies files to figure out where on the web they have been and anticipate what information they want. The feature will also help the company sell advertisements at a premium by letting it identify users to advertisers. 'If you type in "chicken stock", it knows you're not talking about gumbo because you've been searching through financial sites' (Fogarty, 1996). The service will also target surfers with advertising tailored to their interests (Note 1).

In October 1996, three US senators were so concerned by the gathering of personal information in a typical commercial transaction that they wrote to the Federal Trade Commission, requesting it to, 'conduct a study of possible violations of consumer privacy rights by companies that operate computer data bases. We have received calls and letters from constituents who are greatly disturbed about the compilation, sale, and usage of these data-bases. They, as well as consumers in general, are concerned about the potential intrusion upon, and violation of, individual privacy rights. There also is concern about the potential abusive and unlawful usage of the data' (Letter from Senators Bryan, Pressler, and Hollings, 1996). More specifically, they asked for the probe to include the following questions and issues:

1. Is the non-consensual compilation, sale, and usage of databases a violation of private citizens' civil rights?
2. Are the databases subject to unlawful usage? Do they create an undue potential for fraud on consumers?
3. Are the compilation, sale and usage of consumers' personal data consistent with the Fair Credit Reporting Act and federal telemarketing regulations?
4. Are there ways consumers can prevent database service companies from including their personal background information in commercial databases absent from their content?

There is reason to be concerned, and the question to be addressed next is how have various nations responded to the ongoing attacks on personal privacy.

PRIVACY LEGISLATION OR LACK THEREOF

United States

The constitutional protection of privacy in the US has been much debated with legal opinion divided as to the degree to which privacy represents a fundamental right. Surely nothing exists as explicitly as the constitutional guarantee of freedom of expression (The First Amendment of the Bill of Rights), itself a topic of endless and ongoing concern. In the case, Griswold v. Connecticut (381 U.S. 479, 484 1965), Supreme Court Justice William O. Douglas described 'zones of privacy' that are protected by the Bill of Rights (as quoted in Blackman 1993, p. 439):

> 'The right of association contained in the penumbra of the First Amendment is [a zone of privacy]. The Third Amendment in its prohibition against the quartering of soldiers "in any house" in time of peace without the consent of the owner is another facet of that privacy. The Fourth Amendment explicitly affirms the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures. The Fifth Amendment in its Self-Incrimination Clause enables the citizen to create a zone of privacy which the government may not force him to surrender to his detriment. The Ninth Amendment provides: The enumeration in the Constitution of certain rights shall not be construed to deny or disparage others retained by the people.'

Thus, if it can be established that threats to privacy do exist, it is incumbent on the government to take appropriate steps to deal with such threats and included in these steps may be legislation, as was the case with the Fair Credit Reporting Act of 1970, the Privacy Act of 1974, and the Electronic Communications Privacy Act of 1986, among others. Indeed as Blackman (1993, p. 446) argues, 'Congress has recognized the need for and demonstrated a desire to protect personal privacy and commercial access to information, but has thus far failed to enact legislation that accomplishes both purposes in a comprehensive, effective manner. Satisfaction of Congress' intentions requires *a law that establishes a privacy standard for all industries to follow, and a mechanism to ensure its enforcement*' [emphasis added]. However, neither Congress nor the President has shown any interest in enacting legislation to protect personal privacy.

Canada

Canada is similar to the US in that there is no federal government legislation that applies comprehensively to the private sector. The Canadian Privacy Act applies only to the activities of the federal government, although in distinction to the US Privacy Act there is a federal Privacy Commissioner (as well as a Freedom of Information Commissioner). However, this position has limited powers and serves primarily as a mediator, a facilitator, and an early warning monitor. At the provincial level, there exists a wide diversity of approaches, with some provinces having limited privacy legislation while others, especially Quebec, have much

more power. Indeed, Quebec is the only jurisdiction in North America whose privacy law applies to both the public and private sectors and, in this regard, is comparable to many of the laws that exist in western Europe. Note that, in the Canadian political system, federal responsibility is limited in many areas, and serious jurisdictional barriers would prevent general acceptance of federal sovereignty in the privacy area. Nevertheless, the Quebec Privacy Law (Quebec Act respecting the protection of personal information, 1993) could provide a model for appropriate legislation. (See Appendix B for more detail.)

In recognition of the importance of the Internet and the anticipated information highway, the Canadian government appointed the Information Highway Advisory Council (IHAC) in 1994 to explore a wide variety of social, political, commercial, and legal issues in order to provide necessary advice for future policies. IHAC's membership reflected many diverse interests and it produced a number of studies in such areas as intellectual property rights, access, content, education, and of course privacy, as mentioned above, prior to a final report issued in September 1995 (*Connection, Community, Content*, 1995) that contained a number of recommendations with respect to the protection of privacy on the information highway. Although the information highway is still in the future the current technological approximation, the Internet provides some of the features that are expected to make it so exciting.

Recall the four approaches presented at the outset of this paper to serve as a concise set of possibilities for dealing with privacy problems on the information highway. In brief, they are legislation and regulation, voluntary codes and standards, technological solutions, and consumer education. Let me argue that these approaches are not alternatives and their presentation tends to suggest, for example, that consumer education, as well as 'a fundamental need to educate business about the need for more enlightened approaches to the handling of personal data', will help alleviate major impending challenges to personal privacy. This statement is either naive or disingenuous. To support this position as well as the voluntary codes and standards approach would require evidence that historical examples exist in which companies have voluntarily curtailed certain activities, thereby foregoing profits in order to take the ethical high ground. The general tone of the argument in favour of voluntarism is that privacy issues are complex, government jurisdiction is a problem, the private sector is responsible, consumers need to be educated, and all in all the Canadian government is very concerned.

However, in its final report (*Connection, Community, Content*, 1995), after referring to the usefulness of voluntary codes and standards, the IHAC came down very strongly on the side of legislation, or in its own words, 'The Council believes strongly that there should be national legislation (Rec. 10.2) to establish fair information practices on the Information Highway' (p. 50). It further urges the government to continue to cooperate with the Canadian Standards Association and other organizations to 'implement the code (*Model Code for the Protection of Personal Information,* 1995) and develop effective independent oversight and enforcement mechanisms' (Rec. 10.1 and 10.2). In the end, IHAC has come to the conclusion that government legislation is necessary and will work, given an extensive consultation process with the private sector and consumer groups. So, the operating procedure that has emerged and that might also be effective in the US context is a preliminary period of industry consultation to develop an acceptable

privacy code that is comprehensive and effective, followed by national legislation with regulatory, oversight, and enforcement teeth, based on this code.

Europe

Given that the US is a major world trader and enmeshed in international trading agreements, the issue of data protection of transborder data flows (TBDF) is of prime importance. The Basic Principles of National Application of the Organization for Economic Cooperation and Development (OECD) have influenced the privacy guidelines of many countries (Clarke 1989). However, with the prospect of a global information infrastructure (GII) on the horizon, it will be necessary to establish privacy principles that have worldwide application. Members of the G7, the world's leading industrial countries, met in Brussels between February 24 and 26, 1995, to discuss a host of issues related to the GII. Much of the meeting was devoted to technical issues, but social issues including privacy and data protection were also on the agenda.

Prior to the meeting, the US government produced a position paper that included the following with respect to privacy concerns (*The Global Information Infrastructure: Agenda For Cooperation,* 1995):

> The United States and other countries around the world are re-examining existing privacy policies to ensure that they apply comprehensively to the transfer of personal data over global networks. A balanced privacy policy - preserving the individual's right to privacy while maintaining the free flow of information across national borders - is important to the development of global networks and services. Working together, nations should ensure that the transport of personal data adequately takes into account the following agreed-upon international privacy principles:
>
> - Personal data should be collected only for specified, legitimate purposes;
> - The dissemination, sharing, and reuse of information should be compatible with the purposes for which it was originally collected;
> - Personal data should be accurate, relevant, and up-to-date;
> - Individuals should be informed how personal data will be used and should be allowed to examine and correct this information; and
> - Transmission of personal data should not be unduly restricted or subject to burdensome authorization procedures.

The first four points are clearly taken from the US Code for Fair Information Practices, currently being updated after some twenty years, to reflect the needs of a much more advanced information society. (See Appendix C.) The last point is directed towards perceived attempts by Europe, in the form of OECD directives subsequently amended by the European Parliament, to strengthen the privacy requirements for TBDF.

The 1992 Privacy Directive, as amended, was adopted by the European Community in June 1995. The significant part of this Directive (Directive 95/EC, 1995) for the present purposes is Chapter IV, Transfer of Personal Data to Third Countries, Article 25, Principles, which reads in part:

1. Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the

national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in those countries.

The simple version of the first point is that no personal data can be transferred, from any member state of the Economic Community, to a third country unless that country's level of protection is adequate, where adequate means equivalent to that offered in the Economic Community. Since there are no national privacy laws for the private sector in existence in North America, it would seem to be the case that a confrontation is looming, but the Directive allows the possibility that adequate 'professional rules and security measures' may be sufficient or that satisfactorily agreed upon procedures, that could be generalized, may do as well. Thus, it is possible that the Privacy Directive may serve to spur the development of federal privacy laws or, what is more likely, special arrangements will be made between US companies and the Economic Community for the protection of personal information. In the present US political climate, there appears to be little inclination to enact comprehensive privacy legislation.

Possible North American responses to the privacy directive

The question now looms as to what impact it will have on traditional modes of privacy protection in the US and Canada and how it will influence the role of government. For probably no other reason would data protection legislation be enacted in the US today, and such a demand by the Economic Community may yet fail to have this effect, given a universal reluctance for US legislators to be seen as bowing to foreign demands. Although the US could possibly take a go-it-alone stance, such an option is probably not available to Canada. It is also possible that the acceptance by US industries of a voluntary code that meets the requirements of the European Privacy Directive may satisfy the European Community. Where this leaves the individual is up for debate, given that individual companies or industries will be the final arbiters in privacy disputes. If nothing else, however, the Privacy Directive will serve to isolate the US and focus on the inadequacies of legitimate protection of personal privacy in the private sector.

In Canada, the federal government has announced that it will move towards privacy legislation based on the Model Code for the Protection of Personal Information of the Canadian Standards Association (*Model Code for the Protection of Personal Information*, 1995). Although this code was expected to be voluntarily adopted by Canadian businesses, it requires legislative teeth to meet the standards of the European Directive. In its response to the privacy recommendations contained in the Final Report of the Information Highway Advisory Council, the Canadian government noted that, 'As a means of

encouraging business and consumer confidence in the Information Highway, the ministers of Industry and Justice, after consultation with the provinces and stakeholders, will bring forward proposals for a legislative framework governing the protection of personal data in the private sector' (*Building the Information Society*, 1996, p. 25). Canadian Justice Minister, Alan Rock, has promised that such legislation will be in place by the year 2,000.

VOLUNTARISM AS A SOLUTION

United States

The Information Infrastructure Task Force (IITF) Working Group on Privacy notes that the National Information Infrastructure (NII), the Clinton Administration's term for the information highway will, by its very nature, raise the privacy stakes beyond anything that has so far existed and therefore require more comprehensive privacy principles. Consider the following comments (*Privacy and the National Information Infrastructure,* 1995):

> 6. While guidance to government agencies can be found in existing laws and regulations, and guidance to private organizations exists in principles and practices, these need to be adapted to accommodate the evolving information environment. This changing environment presents new concerns:
> (a) No longer do governments alone obtain and use large amounts of personal information; the private sector now rivals the government in obtaining and using personal information. New principles would thus be incomplete unless they applied to both the governmental and private sectors.
> (b) The NII promises true interactivity. Individuals will become active participants who, by using the NII, will create volumes of data containing the content of communications as well as transactional data.
> (c) The transport vehicles for personal information - the networks - are vulnerable to abuse; thus, the security of the network itself is critical to the NII's future success.

Thus, although a set of updated privacy principles for the Information Highway is the goal of this report, the working group argues that they should not be implemented as legislation. In the report, it is stated that the purpose of these principles is to provide a 'guide' for any groups, institutions, or governments that need to design privacy regulations or laws but that these principles do not have 'the force of law'. This position is certainly consistent with the long-standing attitude of the US in opposition to broad and comprehensive privacy legislation and in favour of a piecemeal or sectoral approach, often resulting in legislation enacted under crisis situations or in response to a wellspring of public indignation. Thus, the federal Privacy Act of 1974 seems to have been enacted as a result of the Watergate events with the basic intent to reassure the public that government would respect personal privacy only if specific legislation were in place. The Fair Credit Reporting Act (1970) can be seen as a response to public opinion concerned with the accuracy and misuse of credit records by credit bureaus, banks, insurance companies, and other institutions that depend on personal credit reports.

Such narrowly-based legislation is clearly at odds with the history of privacy legislation in western Europe. Countries such as Germany (then West Germany), Sweden, and the United Kingdom have established Data Protection boards to oversee and monitor any public or private institution that collects and uses personal information. Space does not permit additional discussions of the European approach but Flaherty (1989) and Bennett (1992) are excellent references. The following two paragraphs are quite revealing (*Privacy and the National Information Infrastructure*, 1995):

> 9. Moreover, the Principles are intended to be in accord with current international guidelines regarding the use of personal information and thus should support the ongoing development of the Global Information Infrastructure.
>
> 10. Finally, adherence to the Principles will cultivate the trust between individuals and information users so crucial to the successful evolution of the NII.

Paragraph 9 states that the Principles are 'intended to be in accord with current international guidelines ...' but given that they do not have the force of law it is not clear that a mix of voluntary guidelines will satisfy the countries of Europe that have adequate legislation in place. Paragraph 10 offers the plaintive hope that 'adherence to the Principles will cultivate the trust between individuals and information users ...' What evidence is there that voluntary codes work? How will individuals know which voluntary code is in effect and how its provisions differ or are similar to other voluntary codes? What recourse will they have if they feel that their privacy has been compromised? Must they depend upon the goodwill of the 'information user'?

In October 1995, the National Telecommunications and Information Administration (NTIA) issued a White Paper (*Privacy and the NII: Safeguarding Telecommunications-Related Personal Information,* 1995), by which it hoped:

> to contribute to the broader privacy debate by addressing the privacy issues related to a specific sector - the telecommunications sector. Specifically, this paper focuses on the privacy concerns associated with an individual's subscription to or use of a telecommunications or information service. The overall purpose of the paper is to provide an analysis of the state of privacy in the United States as it relates to existing and future communications services and to recommend a framework for safeguarding telecommunications-related personal information (TRPI).

Note that this paper is a product in part of the comments received as a result of the circulation of the February (and April) 1994 NTIA 'Inquiry' paper. Forty-six formal comments were received from 'industry, the press, academics, privacy advocates, and individuals ... supplemented by consultations with stakeholders in the privacy debate, feedback from experts, and independent research'.

It is noted that the 'United States currently has no omnibus privacy law that covers the private sector's acquisition, disclosure, and use of TRPI (telecommunications-related personal information)'. But, not surprisingly, its bottom line is not to recommend such legislation, at least not yet. Instead, the White Paper hopes for the following:

> As stated above, NTIA's proposed framework draws upon the IITF's Principles and has two fundamental elements - provider notice and customer

> consent. Under NTIA's proposed framework, each provider of telecommunications and information services would inform its customers about what TRPI it intends to collect and how that data will be used. A service provider would be free to use the information collected for the stated purposes once it has obtained consent from the relevant customer. Affirmative consent would be required with respect to sensitive personal information. Tacit customer consent would be sufficient to authorize the use of all other information.
>
> This approach, if embraced by industry, would allow service providers and their customers to establish the specific level of privacy protection offered in a marketplace transaction, *free from excessive government regulation*, so long as the minimum requirements of notice and consent are satisfied ... For these reasons, NTIA believes that it is in the private sector's interest to adopt the privacy framework outlined in this paper, *without waiting for formal government action* [emphasis added].

Formal government involvement in the marketplace regulation of privacy via appropriate legislation is not on the cards, even though western Europe, Canada, and other countries have chosen this strategy. The NTIA paper recommends a modified contractual approach to dealing with privacy concerns. Under such an approach, 'companies would inform their customers about what sorts of personal information the firms intend to collect and the uses to which that information would be put. Consumers could then either accept a company's 'offer', or reject it and shop around for a better deal'. The modified contractual approach, favoured by NTIA, 'allows businesses and consumers to reach agreements concerning the collection, use, and dissemination of TRPI, subject to two fundamental requirements, provider notice and customer consent. Our recommended approach should adequately protect individuals' legitimate privacy interests without excessive government intervention in the marketplace'. Finally to reinforce its view, NTIA offers both the carrot and the stick. It recommends that the modified contractual framework be grounded in the 'principles of fair information practices released by the IITF's Privacy Working Group in June 1995'. NTIA expects the private sector to implement this framework voluntarily but '(i)f such private sector action is not forthcoming, however, that framework can and should form the basis for government-mandated privacy regulations or standards'.

Not surprisingly, the private sector has responded with the formation of something called eTRUST (eTRUST Press Release, 1996):

> The Electronic Frontier Foundation (EFF) and CommerceNet are partnering to implement eTRUST, a global initiative for establishing consumer trust and confidence in electronic transactions. Tapping the combined strength of industry and public interests, eTRUST is designed to address the issues of consumer trust in the Internet marketplace.
>
> eTRUST will build an integrated logo system which consumers will associate with trust and confidence in electronic transactions. Though eTRUST will address privacy and security concerns initially, the eTRUST brand will grow to encompass a variety of other consumer interests. A major component of eTRUST will be an awareness and education program for consumers and businesses.

The current membership is not large, but with such powerful members as Coopers & Lybrand, KPMG Peat Marwick, Firefly, and CommerceNet, it may grow. How this approach will play out in the context of the European Privacy Directive remains to be seen. Will a sophisticated public relations campaign convince the average uninformed consumer that all is well? If large companies launch such campaigns to convince the public that a particular logo guarantees privacy protection, how will the average person be expected to maintain a realistic level of scepticism and concern?

SUMMARY AND CONCLUSIONS

Early in this paper, four possible approaches were suggested: legislation and regulation, voluntary codes and standards, technological solutions, and consumer education. Most of the present effort have been to explore the legislative option and indeed to advocate its adoption as a necessary step in protecting individual privacy. By default, therefore, voluntary codes are seen at best as a temporary precursor to legislation. This perspective is supported in Canada and can be seen as a possible strategy in the US if the private sector is not aggressive in developing, employing, and enforcing adequate privacy codes. The NTIA October 1995 White Paper, although very reluctant to recommend government intervention does threaten it if industry is recalcitrant in vigorously pursuing a comprehensive and effective privacy policy. North America has taken a much more relaxed view than Europe in the development of comprehensive legislation to ensure that, in the OECD terminology, data subjects have adequate safeguards in place with respect to the collection, storage, processing, transmission, and use of personal data by government and companies alike.

To preserve anonymity and protect the privacy of users, the responsibility cannot just be left to the users themselves or to the companies that serve them. In the former case, it is too difficult and, in the latter, too much of a conflict of interest. North American governments can follow the lead of European countries and both the spirit and letter of the current OECD directive, and pass appropriate legislation to protect the privacy of their citizens in a meaningful manner. It is not necessary to threaten public well-being with government intrusiveness as in the Clipper Chip chronicles. The creation, under effective legislation, of arm's length data protection boards or commissions to monitor the establishment and operation of all government agencies and companies that collect, process, and use personal information, is the necessary action to be taken to safeguard the increasing amounts of personal data being gathered.

Enormous profits are on the horizon if the realization of the information highway matches the projections of its supporters. Surely the stakes are high enough and the rewards sufficiently great to take the initiative in drawing up appropriate comprehensive privacy legislation. Surely, we have learned that, unless adequate protections are built in from the start, they are difficult to achieve after the fact. It remains for an informed public to demand that its privacy is preserved given the relentlessness of contemporary attacks. It is the responsibility of consumer and civil liberties groups to focus a spotlight on the privacy practices of government as well as the private sector and to articulate the options currently available to the US

as well as those in place elsewhere. Historically, the public has been uninformed, an untenable situation in the age of the information highway.

NOTES

1. The Netscape Navigator 3.0 permits a setting under the Options menu and the Network Preferences submenu Protocols that shows an alert when a request is made to accept a cookie or send a cookie. If this option is not set, cookies are automatically created and stored. This option is not advertised and thus most users have accepted many cookies without any advance knowledge. What is also of interest is that if acceptance is refused, it is frequently asked for repeatedly until the web site is escaped. Thus many sites will not permit entrance if the cookie is not eventually accepted.

ACKNOWLEDGEMENT

The very helpful comments of the referees are gratefully acknowledged as is the financial support of the Natural Sciences and Engineering Research Council of Canada.

REFERENCES

Bennett, Colin. 1992. *Regulating Privacy: Data Protection and Public Policy in Europe and the United States. Ithaca*, NY: Cornell University Press.

Blackman, Joshua D. November, 1993. A Proposal for Federal Legislation Protecting Informational Privacy Across the Private Sector. *Santa Clara Computer and High Technology Law Journal,* (9:2), pp. 431 - 468.

Building the Information Society: Moving Canada into the 21st Century. 1996, May. Industry Canada. Accessible from the Web site with URL: <http://strategis.ic.gc.ca/cgi-bin/dec/wwwfetch?/sgml/ih01015e_pr702.sgml>.

Connection, Community, Content: The Challenge of the Information Highway. Final Report of the Information Highway Advisory Council. 1995, September. Industry Canada. Accessible from the Web site with URL: <http://strategis.ic.gc.ca/cgi-bin/dec/wwwfetch?/sgml/ih01015e_pr702.sgml>.

Clarke, Roger. 1989. The OECD Data Protection Guidelines: A Template for Evaluating Information Privacy Law and Proposals for Information Privacy Law. Australian National University Unpublished Working Paper of 1989. © Australian National University, 1987, 1988, 1989.

Directive 95/EC. June 1995. Directive of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data And on the Free Movement of Such Data. Accessed from the Web page with URL: <http://www2.echo.lu/legal/en/dataprot/directiv/directiv.ht ml> on May 15, 1996.

eTRUST Press Release: CommerceNet and Electronic Frontier Foundation Partner to Implement eTRUST. October 16, 1996. Accessed from the Web page with URL: <http://www.etrust.org/07press.html> on November 16, 1996.

Flaherty, David. 1989. *Protecting Privacy in Surveillance Societies: The Federal Republic of Germany, Sweden, France, Canada, and the United States.* Chapel Hill, North Carolina: The University of North Carolina Press.

Fogarty, Kevin. Infoseek to track cookies information, *Computerworld,* October 4, 1996. Accessed at the Web page with URL: <http://www.computerworld.com/news/infoseek.html> on October 21, 1996.

Gates, Bill. Billionaire Bytes, *The Vancouver Sun,* September 14, 1995, D 4.

The Global Information Infrastructure: Agenda For Cooperation. 1995, February. Information Infrastructure Task Force. Available on the NII Virtual Library, WWW site with URL: <http://iitf.doc.gov>.

Information Security and Privacy in Network Environments. 1994, September 15. U.S. Congress, Office of Technology Assessment, Washington, DC: U.S. Government Printing Office. Also available on Web page with URL: <http://www.ota.nap.edu/pdf/data/1994/9416.PDF>.

Letter from Senators Bryan, Pressler, and Hollings. October 8, 1996. Accessed from the Web page with URL: <http://www.epic.org/privacy/databases/ftc_databases. html> on October 21, 1996.

Model Code for the Protection of Personal Information. August, 1995. Final Draft. CSA Technical Committee on Privacy, Canadian Standards Association, CAN/CSA-Q830-1995. Available at the Web site with URL: <http://www.csa.ca/>.

Netscape's Cookies Crumble. 1996, April. Australian Personal Computer Online - News. Accessed from the Web page with URL: <http://www.com.au/apc/9604/thenet/onnews.html> on May 13, 1996.

Privacy and the Canadian Information Highway. 1994, October. Communications Development and Planning Branch, Spectrum, Information Technologies and Telecommunications Sector, Industry Canada. Also available at the WWW site with URL: <http://info.ic.gc.ca/info-highway/ih.html>.

Privacy and the NII: Safeguarding Telecommunications-Related Personal Information. October, 1995. NTIA, Office of Policy Analysis and Development, Washington, DC. Also available at Web page with URL: <gopher://www.ntia.doc.gov:70/HO/policy/privwhitepaper.html>

Privacy and the National Information Infrastructure: Principles for Providing and Using Personal Information. January 19, 1995. Information Infrastructure Task Force Working Group on Privacy. Available on IITF Web site with URL: <(http:// iitf.doc.gov>.

Quebec Act respecting the protection of personal information in the private sector. 1993, Bill 68 (1993, chapter 17), National Assembly of Quebec, Second Session, Thirty Fourth Legislature.

Westin, Alan. 1967. *Privacy and Information.* Atheneum: New York.

Yang, John, a research assistant in the geology department at Florida International University as quoted in James Staten, Netscape Tricks Raise Security Concerns, *MacWeek,* March 13, 1996. Accessed from the Web page with URL: <http://www.zdnet.com/macweek/mw_1011/gw_net_tricks.html> on May 13, 1996.

Appendix A

Four Approaches to Privacy Protection in Canada on the Information Highway:

Legislation and Regulation

Protection of the enormous information holdings of governments, including medical, welfare, tax, immigration and police records, exists at the federal level and in the provinces of Quebec, Ontario, Saskatchewan, Alberta and British Columbia. The quality of coverage varies from jurisdiction to jurisdiction and, when information travels, it is not always clear which law applies.

Voluntary Codes and Standards

Voluntary codes have been the preferred approach of Canadian business and industry associations. This approach allows for flexibility in application, so that different industries can tailor their data protection schemes to the needs of their customers, the regulatory environment in which they operate and the demands of the marketplace.

Technological Solutions

Another approach to privacy protection is to use technology to safeguard personal data. Traditionally, technology has been exploited to increase the amount of information gathered, and hence has been feared rather than welcomed by privacy activists. But technology itself is neutral, and can be used to enhance privacy as well as threaten it. Technologies can be designed so that the 'default setting' is on zero information collection.

Consumer Education
There is a fundamental need to educate businesses about the need for more enlightened approaches to the handling of personal data, and to raise the awareness of consumers about how to protect themselves. Consumers need information and education about their rights, about the value of their personal information, about the risks to their privacy that new technologies can bring, and about what they can do to retain privacy.

Appendix B

In the explanatory notes that precede the Quebec Act respecting the protection of personal information, the following relevant information appears:

> The object of this bill is to establish special rules regarding the personal information on others that is collected, held, used or communicated to third persons in the course of operating an enterprise in the private sector and the rights and obligations resulting from the provisions of the Civil Code of Quebec that deal with the protection of personal information.
>
> Under the bill, a person collecting personal information for the purpose of establishing a file on another person or entering information in such a file can collect only information that is necessary to attain the object of the file ...
>
> Persons operating an enterprise are required by the bill to ensure that any personal information on others that they hold or use remains confidential ...
>
> ...
>
> The 'Commission d'accès à l'information', on its own initiative or following a complaint from an interested person, will have the power to inquire into, or entrust another person with inquiring into, any matter relating to the protection of personal information and the methods used by a person operating an enterprise and collects, hold or uses personal information or communicates it to third persons ...
>
> ...
>
> Lastly, the bill prescribes penal sanctions and ensures concordance of its provisions with the legislation currently in force.

Appendix C

Fundamental Principles of Fair Information Practice*:

- There must be no personal-data record-keeping systems whose very existence is secret.
- There must be a way for an individual to find out what information about him is in a record and how it is used.
- There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
- There must be a way for an individual to correct or amend a record of identifiable information about him.
- Any organization creating, maintaining, using, or disseminating records of identifiable personal data must ensure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data.

**Records, Computers, and the Rights of Citizens.* Report of the Secretary's Advisory Committee on Automated Personal Data Systems, US Department of Health, Education and Welfare. Cambridge, MA: The Massachusetts Institute of Technology, 1973, p. 41.