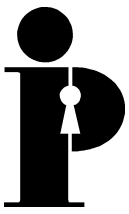
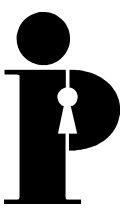
Information
and Privacy
Commissioner/
Ontario

A Report to the 22nd International Conference of Data Protection Commissioners (Venice, Italy)

Should the *OECD Guidelines* Apply to Personal Data Online?



Ann Cavoukian, Ph.D.
Commissioner
September 2000



Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

This publication is also available on the IPC website.

Table of Contents

Question: Is working to amend the OECD Guidelines the best way for Data Protection Commissioners to address online privacy concerns?

Answer: No.

Question: So, now what?

Introduction

The Honourable Justice Michael Kirby opened last year's International Conference on Privacy and Personal Data Protection in Hong Kong by suggesting the 1980 Organisation for Economic Co-operation and Development's *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD Guidelines) were showing signs of their age. Justice Kirby noted that the world, particularly in the area of technology, had changed beyond recognition from the world into which the Guidelines were introduced 20 years ago. He concluded that it would be "timely to consider the changes and some of their implications."[1]

We are here now, a year later, to continue this debate. At the outset, it is important to recognize the context of our discussion about the OECD Guidelines. The intervening year has brought significant developments, both good and bad, to the online world. The incredible rate and scope of change of the Internet needs to inform our debate. Also, we must acknowledge a number of fundamental truths:

The Internet is growing rapidly:

- It is estimated that the World Wide Web (the Web) more than doubles in size every year. Some estimates have it doubling every six months.[2]
- As of April 6, 2000, there were 15,719,462 domains registered worldwide, with 9,482,427 being ".com" domains.[3]
- In the 24 hours before this sentence was written, the Web added an estimated: 3,940,000 new pages, 73,900,000,000 new bytes of text, 887,000 new images, and 14,800,000,000 new bytes of image data.[4]

Companies and individuals are using the Internet:

- In 1999, Forrester Research forecast that world-wide business over the Internet would reach $3.2 trillion (U.S.) by the year 2003.[5]

- One "educated guess" as to how many are online worldwide is: 304.36 million world total; 136.86 million Canada and United States; 83.35 million Europe; and 68.9 million Asia/Pacific (as of March 2000).[6]
- According to the ACNielsen NetWatch, the United States may be first in sheer number of users, but Canada far exceeds any other country in terms of Internet penetration. Four out of every 10 Canadians use the Internet.[7]
- An Angus Reid poll indicated that 40% of the total number of people online had made online purchases.[8]

The Internet and e-commerce function globally:

- Microsoft Corporation operates Canada's most popular Web sites. In April 2000, more than 6.2 million Canadians visited a Microsoft Internet property from their home computers, including Hotmail, MSN.ca, Microsoft.com, and MSN Instant Messenger. Sites operated by America Online Inc. were the second most popular among Canadians. While properties owned by Yahoo! Inc. (e.g., Yahoo.com, Yahoo.ca and Geocities) ranked third.[9]
- In March 2000, the five most visited Internet properties in France were Wanadoo, Yahoo, AOL, MSN and Multimania. The United Kingdom top five comprised MSN, AOL, Yahoo, Microsoft and Freeserve. The German top five list was: T Online, AOL, Yahoo, Lycos and MSN.[10]
- According to a survey from Nielsen NetRatings, MSN and Yahoo properties are the most popular destinations for Web surfers around the world. MSN is the most popular site in the United Kingdom, New Zealand and Australia, and is the second-most popular after Yahoo in Singapore and Ireland. In the United States, AOL is the most popular, followed by Yahoo and MSN.[11]

Individuals are confused about the Internet and concerned about online privacy:

- An April 2000 study by Cyber Dialogue found that 69% of Internet users had unknowingly signed up for e-mail distribution lists and more than 40% did not know or understand what cookies were or how they worked. Twenty-one percent (21%) of users were not sure what their browsers were set to when it came to cookies.[12]
- An IBM-Harris Multinational Consumer Privacy Survey indicated that 94% of American, 79% of British, and 72% of German respondents were concerned about the possible misuse of their personal information online. Sixty-one percent (61%) of American users, 39% of U.K., and 49% of German Internet users had refused to purchase goods because of privacy concerns.[13]
- In 1999, four of five Canadians were concerned about the release of their personal information to other organizations when they shopped online. The survey found a higher level of privacy concern about the Internet than with other buying methods such as telephone or mail.[14]

- A March 2000 survey showed that the majority of respondents (80%) were concerned about privacy on the Internet. Top concerns were:
    - Having one's identity stolen through the use of publicly available personal information (78%);
    - Knowing that an individual or organization may develop a comprehensive file of one's personal information (74%);
    - Not having control over the sale or brokering of one's personal information (72%); and
    - Believing that online ad networks can track personal movement across the Web (65%).[15]

Commercial, not-for-profit and industry organizations are responding to the public's concerns about online privacy:

- In January 2000, TRUSTe announced it had awarded its 1000th Privacy Seal.[16]
- This year, Germany joined England, France, Scotland, Ireland and Wales in the European Union in offering the WebTrust Seal. WebTrust is also available in Australia, Canada and Puerto Rico, in addition to the United States.[17]
- In May 2000, BBBOnLine and the Japan Information Processing Development Center announced their agreement to enter into a joint venture to develop reciprocal online privacy seals recognizable to consumers and businesses in both countries.[18]
- The Good Housekeeping Institute established its criteria for Web site integrity, credibility, security and customer service. In order to receive the Good Housekeeping Web Site Certification, a site must have a clearly defined privacy policy and full disclosure of the use of cookies and how they can be disabled/deleted.[19]
- The Council for Internet Commerce released its *Standard for Internet Commerce*, which specifies merchant practices and policies that lead to high levels of customer satisfaction, service, security and privacy.[20]
- The Global Dialogue for Electronic Commerce, a consortium of companies formed to "strengthen international coordination of e-commerce rules," finalized its policy on the protection of personal data."[21]
- At the beginning of June 2000, the Electronic Commerce and Consumer Protection Group, made up of America Online, AT&T, Dell, IBM, Microsoft, Network Solutions and Time Warner, proposed *Guidelines for Merchant-to-Consumer Transactions* and a companion *Statement on Global Jurisdiction Framework for Electronic Commerce*. The Guidelines include a section on privacy protection.[22]
- enonymous.com runs a Web site (http://www.privacyratings.org) where anyone can check the privacy policy and enonymous.com's rating of 30,000 of the most popular Web sites.

- In May 2000, Privacy Council, Inc. launched its Web site (http://www.privacycouncil.com) designed to help businesses implement and consumers recognize "smart privacy and data practices." Among the current resources on the site are information and links regarding opt-out, privacy organizations, legislative and legal resources, privacy policy generators, seal programs, cookies, encryption, infomediaries, and related surveys.[23]

- In June 2000, a group of more than 20 corporate CEOs and trade association executives announced the formation of the Privacy Leadership Initiative (PLI). Members of this alliance include Procter & Gamble, IBM, Ford, Intel, Sony, E*TRADE, and AT&T. Among other initiatives, the PLI plans to:

    - Perform an analysis of currently available privacy technologies, identify capability gaps and offer ways to make these technologies broadly available to individuals;

    - Conduct consumer research to understand the specifics of consumer privacy concerns and to provide a baseline for measuring progress;

    - Design a set of online privacy templates that enable companies to efficiently implement appropriate privacy practices and conduct an outreach campaign to assure broad distribution within industry;

    - Conduct a consumer education campaign to address consumers' concerns and inform consumers of technology efforts that allow them to control their own privacy; and

    - Form a private sector-led forum, independent of the initiative, that will conduct ongoing and informed assessments of privacy policy issues, and inform stakeholders of its recommendations.[24]

- Companies such as Anonymizer.com, Zero Knowledge Systems, Lumeria Network with its PrivacyPlace Web site, Novell's digitalme, Privaseek's Persona, e-DENTIFICATION, @YourCommand, nCognito, and Lucent Personal Web Assistant, to name just a few, continued to make technology headlines throughout the year.

This is the context in which we must examine the merits of re-visiting the OECD Guidelines. As we consider these first principles, the online world is moving ahead at warp speed, without us. The Data Protection Commissioners are not the ones setting and enforcing online privacy standards. In order to keep pace, we must act quickly.

The purpose of this paper is to review the OECD Guidelines and the work that the OECD itself has done to consider the application of its fair information principles to the Internet. More importantly, we wish to emphasize that our time and limited resources might be better spent by agreeing to basic online privacy protection standards that can cut across jurisdictional boundaries and legislative differences.

OECD Guidelines

In September 1980, the OECD adopted the *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. These Guidelines include the eight Basic Principles of National Application known to us all (Exhibit A). Commonly known as "fair information practices," these principles, which are overlapping and cumulative in nature, outline responsible information-handling practices designed to protect privacy. Adherence to all of the practices is necessary to achieve full informational privacy.

Since their introduction, OECD Member countries have adopted the Guidelines, with Canada doing so in 1984. The Guidelines form the basis of data protection legislation around the world, with varying degrees of consistency and completeness, including Canada's new *Personal Information Protection and Electronic Documents Act*, professional and industry privacy codes, online privacy seals, and individual companies' privacy policies.

There is a tendency to consider fair information practices in isolation. However, the explanatory memorandum of the OECD Guidelines reminds us of a number of important points, including the following:

- The OECD Guidelines are not legally binding.[25]
- The Guidelines identify an international concern regarding the need for a "consensus on the fundamental principles on which protection of the individual must be based."[26] One of the objectives is to achieve acceptance by members of "certain minimum standards of protection of privacy and individual liberties with regard to personal data."[27]
- The "principles for the protection of privacy and individual liberties expressed in the Guidelines are valid for the processing of data in general, irrespective of the particular technology employed."[28] The Guidelines emphasize they are "neutral with regard to the particular technology used."[29]
- The Guidelines do not prescribe or presuppose "uniform implementation by Member countries with respect to details. For instance, different traditions and different attitudes by the general public have to be taken into account."[30] It is recognized that:

  > On the whole the Guidelines constitute a general framework for concerted action by Member countries: objectives put forward by the Guidelines may be pursued in different ways, depending on the legal instruments and strategies preferred by Member countries for their implementation.[31]

- The OECD Guidelines indicate "there is a need for a continuing review of the Guidelines, both by Member countries and the OECD. As and when experience is gained, it may prove desirable to develop and adjust the Guidelines accordingly."[32]

OECD Review

Over the last few years, the OECD and its Members have undertaken a number of reviews of the Guidelines. Below is a summary of the conclusions and findings of these various initiatives.

Implementing the OECD 'Privacy Guidelines' in the Electronic Environment: Focus on the Internet

In October 1997, the OECD's Group of Experts on Information Security and Privacy reviewed this report. It looked at various government and private sector initiatives, including TRUSTe and the World Wide Web Consortium's (W3C) Platform for Privacy Preferences (P3P).

The main points of that report suggested the following action by the OECD and Member countries:

- reaffirm the privacy guidelines as applicable "with regard to any technology used for collecting and processing data;"
- encourage businesses to adopt policies and technical solutions that will guarantee the protection of privacy on information and communications networks, particularly the Internet; and
- foster "public education on issues related to protection of privacy and the use of technology."[33]

The report indicated that "the basic values agreed upon in the OECD Guidelines … are still accepted worldwide … [and] they represent the primary components for the protection of privacy and personal data, comprising a commonly understood reference point."[34]

In particular, the Group of Experts concluded:

> … changes in technology do not diminish the relevance of the consensus achieved in 1980: despite technological advances and the evolution of an electronic environment based on world-wide information and communications networks, the Guidelines are still applicable today…
>
> the Group of Experts on Information Security and Privacy have deemed it not necessary to revise the Guidelines at this time. The Guidelines are, in fact, technologically neutral and apply to all types of personal data, whether traffic data … or content data…[35]

International Workshop on Privacy Protection in a Global Networked Society

In February 1998, the OECD sponsored this workshop in Paris. Representatives from a number of the European Data Protection Commissioners' offices participated. The workshop's objective was:

> … to bring together representatives from the 29 OECD Member countries to engage in a dialogue among governments, the private sector, the user and consumer communities, and data protection authorities to focus on how the *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* may be implemented in the context of global networks.[36]

Participants concluded that "the growth of electronic commerce requires increased consumer confidence in privacy protection, and that the OECD Guidelines continue to provide a common set of fundamental principles for guiding efforts in this area."[37]

A Borderless World: Realising the Potential of Global Electronic Commerce

In October 1998, the OECD held this Ministerial Conference in Ottawa. Several documents were produced for review at the conference, including an *Inventory of Privacy Instruments and Mechanisms for Implementing and Enforcing the OECD Privacy Guidelines on Global Networks*.[38] This report was later revised and updated.[39]

The inventory reviewed "guidance instruments" such as treaties, constitutions, laws, regulations, and self-regulatory codes, as well as mechanisms such as technology, contracts, practices, and civil/criminal procedures, for implementing and enforcing privacy principles. It included reports on initiatives at the international, national, and regional levels, from both the public and private sectors. The report also examined issues around the collection and use of clickstream data, anonymity, P3P, and online privacy seals.

Another document, the *Consumer Protection in the Electronic Marketplace*, was submitted for discussion and approval at the Ottawa conference. With regard to privacy protection, the paper stated:

> As consumers become increasingly aware and concerned about the potential online threats to personal privacy, they need assurances about the fair collection and use of their personal data.
>
> … technology alone will not provide consumers with sufficient online privacy protection… Governments, the private sector and consumer representatives should work to ensure that commercial activities conducted over global networks are at least consistent with the effective implementation of the 1980 OECD Privacy Guidelines.[40]

Three critical declarations came out of the Ottawa OECD Ministerial Conference:

- a Declaration on Authentication for Electronic Commerce;[41]
- a Declaration on Consumer Protection in the Context of Electronic Commerce;[42] and
- a Declaration on Protection of Privacy on Global Networks.[43]

Declaration on Protection of Privacy on Global Networks

With the Privacy Declaration, the OECD Members reaffirmed their belief in the continued utility of the OECD Guidelines by committing to:

- "… work to build bridges between the different approaches adopted by Member countries to ensure privacy protection on global networks based on the OECD Guidelines…;"

- "… ensure that the OECD Privacy Guidelines are effectively implemented in relation to global networks…;" and
- "Examine specific issues raised by the implementation of the OECD Privacy Guidelines in relation to global networks and, after collection and distribution of examples of experiences on implementation of the Guidelines, provide practical guidance to Member countries on the implementation of the Guidelines in online environments, taking into account the different approaches to privacy protection adopted by Member countries and drawing on the experiences of Member countries and the private sector."[44]

The Declaration also included an agreement "to review progress made in furtherance of the objectives of the Declaration within a period of two years" (i.e., 2000), and "to assess the need for further action to ensure the protection of personal data on global networks in pursuit of these objectives."[45]

Action Plan for Electronic Commerce

This plan, that came out of the Ottawa conference, highlighted areas for consideration by the OECD Council and various working groups, including the protection of privacy and personal data. Referencing the Privacy Declaration, the Action Plan noted:

> … it recognises that the principles outlined in the 1980 OECD Guidelines continue to provide an international foundation for the protection of privacy on any medium, and that countries should work together, and with the private sector, to ensure their effective implementation in an open and global network environment.[46]

Practices to Implement the OECD Privacy Guidelines on Global Networks

In 1999, the results of an OECD survey of 50 Web sites were published in this report. The purpose of the survey was to determine the extent to which, and how, the OECD Guidelines were put into practice on the Web. The study looked at the collection of personal information by commercial sites, the processing of personal information, the transparency of policies, the use of security and privacy enhancing technologies (PETs), and issues of responsibility, liability and redress. Specific findings included:

- A majority of sites attempted to set cookies.[47]
- Three-quarters of the sample Web sites had a policy for the protection of privacy. However, the ease with which visitors could access the privacy statements was mixed, with just over half being considered "easy."[48]
- At least one third of the sites surveyed were not "very explicit" about the data collected, and over half did not address the question of clickstream data and the processing to which they were subject. Another third of the sites did not provide opt-out possibilities or a right of access. Almost one-quarter of the sites surveyed did not give any physical address permitting visitors to know something about who they were dealing with in order to seek redress through traditional forms of communication, if necessary.[49]

- Only a quarter of the sites providing individuals with a right of access enabled that right to be exercised online.[50]
- Only one-tenth of the sites in the sample offered their visitors possibilities for recourse in the case of disagreement.[51]
- Only 7 of the 50 sites explicitly held themselves responsible for the application of their privacy policy statements.[52]

The "most striking" conclusion drawn from the study was the existence of:

> … a marked discrepancy between the world of the various institutions and organizations that develop ideas and instruments for data protection on the one hand, and the world of Web sites on the other. The latter, or the great majority of them, whatever their sincerity or their good intentions with regard to their visitors, actually give the impression … that they pay too little attention to the issues involved in the protection of privacy and transborder data flows, and, most importantly, that they lack precise and consistent direction for privacy protection applicable to online networks.[53]

After reviewing the survey results, the OECD's Group of Experts on Information Security and Privacy concluded:

> It therefore seemed useful to draw up a set of generally applicable suggestions corresponding to some of the "best practices" that were highlighted by the survey or which, on the contrary, can be derived from the shortcomings or gaps that can be seen in the Web sites analysed.
>
> Without claiming to be exhaustive, and without implying any kind of ranking in their classification other than that stemming from the chronology of this report, we can thus formulate, in the spirit of both the proper application of the OECD principles and the promotion of a climate of confidence for electronic commerce, … ten series of suggestions …[54]

The OECD's 10 best practices for "privacy-friendly" Web site design, included suggestions about cookies, e-mail, opt-out, education, transparency, security, individual rights, PETs and site responsibility.[55]

Privacy Policy Statement Generator

Also in 1999, the OECD began to beta test its Privacy Policy Statement Generator as a way of implementing the OECD Guidelines. The introduction of the OECD Privacy Policy Statement Generator states:

> The OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 1980 (OECD Privacy Guidelines) represent an international consensus on how best to balance effective privacy protection and the free flow of information…

> It is the aim of the project to encourage the development among public and private organisations in the online environment of privacy policies and statements, and thus contribute to the online implementation of the Openness Principle in the OECD Privacy Guidelines.
>
> It is hoped that the widespread display on Web sites of privacy policy statements based on an international instrument such as the OECD Privacy Guidelines, will foster education among Web site owners. It is also hoped that the Generator will increase awareness among visitors about the privacy practices of Web sites which they browse…
>
> When an organisation posts its privacy statement on a Web site, the statement will be available to, and relied on by visitors globally. The OECD Generator is therefore valuable since its use as a global educational tool is endorsed by all 29 OECD Member countries.[56]

Guidelines for Consumer Protection in the Context of Electronic Commerce

At the end of 1999, the OECD issued its consumer protection guidelines. The Privacy section of that report stated:

> Business-to-consumer electronic commerce should be conducted in accordance with the recognised privacy principles set out in the OECD Guidelines Governing the Protection of Privacy and Transborder Flow of Personal Data (1980) and taking into account the OECD Ministerial Declaration of the Protection of Privacy on Global Networks (1998) to provide appropriate and effective protection for consumers.[57]

Current Work

The OECD is preparing a report on the use of contractual solutions for transborder data flows. The report will examine, in the context of business-to-business as well as consumer-to-business contracts, issues such as content of contracts, certification and labelling and rights of data subjects. The report also will examine dispute resolution mechanisms and enforcement, such as mediation, arbitration, litigation, and remedies.[58]

As of the time of writing this paper, the OECD had not yet published its final report on contracts, or the review committed to in the OECD Ministerial Declaration of the Protection of Privacy on Global Networks in 1998.

Criticism of the OECD Guidelines

The above history is included here to highlight the repeated commitment that the OECD and its Member countries have made to the Guidelines, and their ongoing belief in the relevance and applicability of the existing principles to the online world. Others have taken a different, and more critical, view of the Guidelines.

At last year's conference, Justice Kirby, a major architect of the OECD Guidelines, characterized them and the OECD's review as follows: "This unexpected child, conceived in a union of economics and human rights, born in 1980, is now 20 years old. Its parents have acknowledged and praised it."[59] Elsewhere, he has stated:

> There is an urgent need, in the light of technological change and the enhanced capacity of the Internet, for a review to be conducted of the information privacy principles developed by the OECD twenty years ago. There are now serious gaps in those principles. Informed writers are already suggesting that new privacy principles are needed, such as:
>
> - A right not to be indexed.
> - A right to encrypt personal information communications effectively.
> - A right to fair treatment in public key infrastructures, so that no person is unfairly excluded in a way that would prejudice that person's ability to protect their privacy.
> - A right to human checking of adverse automated decisions and a right to understand such decisions.
> - A right, going beyond the aspirations of the OECD openness principle, of disclosure of the collections to which others will have access and which affect the protection of the profile of the individual concerned.[60]

Professor Colin Bennett has correctly pointed out that the OECD Guidelines are not strictly a privacy instrument.[61] Significant qualifiers and restrictions to privacy protection exist within the Guidelines themselves, such as:

Member countries should avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties, which would create obstacles to transborder flows of personal data that would exceed requirements for such protection.[62]

The Guidelines attempt to balance what could be reasonably characterized as competing interests. The need or desire to protect privacy is always qualified by the need "to avoid undue interference with flows of personal data between Member countries."[63]

Graham Greenleaf has been critical of the OECD Guidelines because, in his view, privacy can be compromised, and surveillance permitted, under these fair information practices. He maintains that such practices even may be used to sanitize surveillance. In particular, he has noted that they do not set limits on the breadth or intrusiveness of the defined purpose(s).[64]

Calling the OECD Guidelines "first generation" privacy principles, Greenleaf argues that cyberspace brings forward privacy issues not directly anticipated when the Guidelines were first formulated. He indicates that one of the most difficult privacy problems of the Internet is the power of search engines and indexing facilities.[65] He also points out that defining what constitutes personal information online is "problematic," and questions how notice would be provided for the collection and aggregation of usage information identified by machine address.[66]

Roger Clarke has been one of the most vocal critics of the OECD Guidelines:

> The fair information practices approach has been demonstrably inadequate as a means of protecting personal privacy. It has had the effect of legitimizing existing privacy-invasive practices, it has failed to prevent unreasonable invasive new schemes and new features of existing schemes, and it has failed dismally to adapt to the rapid advances in information technology.[67]

Clarke argues the information privacy principles (IPP) approach, as embodied by the OECD Guidelines, has substantial inadequacies:

> The OECD Guidelines are showing their advanced age. Enhancements are overdue, to cope with the ravages of technological advance, and the increasing expectations of consumers and citizens…
>
> Even more fundamentally, however, the weaknesses of the IPPs reflect their origins in an overriding commitment to administrative efficiency rather than to privacy interests. The so-called 'Fair Information Practices' movement within which these IPPs were derived adopted the approach that the efficiency and administrative convenience of business and government should not be hindered: there should merely be some conditions applied to business processes. Aided by this business-friendly approach, practices have become increasingly information-intensive and the personal data collected has become increasingly fine-grained.[68]

Specific weaknesses highlighted by Clarke include the IPP's failure to:

- require public justification for privacy-invasive schemes or features;
- control the purposes of personal data systems;
- control the legal authorization of use and disclosure;
- control exemptions and exceptions;

- sustain anonymity (i.e., require anonymous transactions as the norm, identified transactions only where justified, and pseudonymous transactions as the compromise mechanism);
- "negate the monolithic state" or prevent information-sharing among government agencies;
- protect dimensions of privacy other than data privacy;
- preclude inequitable access to services;
- stop multiple use of identification schemes; and
- prevent the dominance of administrative efficiency over privacy interests.[69]

Clarke has stated: "In short, the fair information practices paradigm is in urgent need of replacement or at least substantial augmentation."[70] He also has criticized the OECD's own action, calling it "a disappointingly static approach to the relationship between its 1980 Guidelines and the Internet."[71]

Other critics have pointed to the obvious limitation of the OECD Guidelines with regard to enforcement:

> The OECD guidelines … provide for no procedural means to ensure that the guidelines actually result in effective protection for individuals… This leads to the conclusion that, although international instruments such as the OECD Guidelines have shown their importance in world-wide protection of personal data, they are not sufficient as such to safeguard a comprehensive and appropriate personal data protection in the context of the digital economy.[72]

This issue was discussed by Robert Gellman in his review of privacy regulation. Gellman argued broad agreement on general principles, such as those reflected in the OECD Guidelines, is not enough to establish the common processes and procedures needed to implement and enforce common international privacy rules. He pointed to the experience in the United States, regarding implementation of the OECD Guidelines, to illustrate the practical shortcomings of general standards. While many companies agreed to the standards, few changed their practices or policies.

Gellman argued there should be substantive and procedural details that go beyond general principles. In particular, there should be an enforcement mechanism that offers some oversight of the activities of record keepers as well as a practical remedy for individuals.[73]

So where do we go from here?

The reality of today's world is that global e-commerce is exploding. One of the significant conclusions of the Australian Freehill, Hollingdale and Page *Internet Privacy Survey Report 2000* was that the strength of Internet privacy concerns should not be underestimated. Contrary to some earlier industry expectations, greater usage of, and familiarity with, the Internet has not alleviated users' concerns. Well publicized privacy breaches by online companies have reinforced Internet users' scepticism about adequate privacy protection.[74]

The public's expectation of privacy on the Internet is at odds with the reality of online business practices. While the high-level of publicity associated with the DoubleClick controversy may have recently changed this, generally people have an expectation of anonymity when they surf the Web. They believe that:

> … if they have not affirmatively disclosed information about themselves, then no one knows who they are or what they are doing. But, contrary to this belief, the Internet generates an elaborate trail of data detailing every stop a person makes. … This transactional or click stream data can provide a "profile" of an individual's online life.[75]

As Jerry Berman has noted, the Internet accelerates the trend toward increased information collection already evident in our offline world. The trail of transactional data left behind as we use the Internet is a rich source of information about our habits of association, speech, and commerce. When aggregated, these data can reveal an enormous amount about our lives. This increasingly detailed information is bought and sold as a commodity by a growing assortment of players, and often sought by government.

Berman also pointed out a number of unique challenges to implementing and enforcing data protection policies and practices on the Internet. The most obvious is that information and communications flows unimpeded across national borders. Also, the fact that the Internet was designed without gatekeepers means that there is no single entity that controls the flow of information or enforces practices.[76]

Andrew Grove, Chairman, Intel Corporation, recently stated that personal data is "the currency of the Internet. People trade it, people covet it – it is as valuable a good as the money in my pocket."[77]

Need for international agreement

Given the global nature of the Web and the local jurisdiction of the Data Protection Commissioners, the need for an international consensus regarding online privacy protection does not seem to be in dispute. The question seems to be what data protection standard should form the foundation upon which effective action can be built – the OECD Guidelines (as currently worded or amended), or some other standard entirely?

The OECD and others argue that the Guidelines represent an unprecedented international agreement on data protection and, accordingly, form the necessary basis for efforts designed to protect privacy in the online world. Indeed, some maintain the OECD Guidelines "may provide the best, most well informed consideration to date of how best to protect this fundamental human right in light of technological change."[78]

On the other side, critics maintain that the Guidelines need to be revised in light of technological change. These developments, they argue, invalidate the assumptions that underlie the principles. Critics also point out that the OECD Guidelines only specify standards for fair information handling, and are silent on the nature of remedies and enforcement mechanisms.[79]

Should the Data Protection Commissioners take the call to revise the OECD Guidelines literally, and want this to be something more than an academic exercise, we need to answer two fundamental questions: how and what?

Ontario does not have an answer to these questions, but we believe that Commissioners must not minimize the work done by the OECD itself, or the support the governments of the Member countries have given to it. To change their minds regarding the applicability of the OECD Guidelines, as currently drafted, to the online world, would be a formidable and time-consuming task.

Given the process of ongoing review by the OECD, shouldn't we, as Data Protection Commissioners, raise our concerns within the parameters of that process? Why would we discuss this matter in a parallel and, for the most part, unrelated manner? How would actual, meaningful change be possible if we continue to stand apart? The need for the Commissioners to take advantage of existing venues, initiatives, and organizations to advance our objectives is a theme that will be re-visited later in this paper.

The question of what changes we would propose to the OECD and its members is even more difficult to answer. If we propose to disassemble the international consensus developed around the Guidelines, what would we offer in its place? The majority of current data protection legislation and agreements are informed by, or actually based upon, the OECD Guidelines. What would happen to these instruments if we changed the first principles?

Realistically, how would we arrive at an international agreement on an issue, for example, as controversial as online anonymity? The courts in various jurisdictions have made specific and conflicting rulings– on this issue, while a few jurisdictions have specific and conflicting legislative requirements. In their study of data protection law and online services, Joel Reidenberg and Paul Schwartz note the explicit rules for anonymous and pseudonymous interactions in Germany's *Information and Communications Services Act*. But, they also note the different approaches taken in the United Kingdom, France and Belgium.[80]

Also, as Justice Kirby correctly pointed out, countries outside of the "developed" world should be involved in the formulation of applicable guidelines so their concerns and values also may be reflected.[81] Some of these countries have entirely opposing views on anonymity and other issues.

Regarding the creation of new international privacy instruments, Nigel Waters remarked at last year's conference:

> … the problems of interpretation, and of application in practice, that arise with the OECD based principles are equally likely to arise with any new formulation. Reaching agreement on implementing the already agreed principles is proving difficult enough, without opening up the possibilities of disagreement on a revision of the principles.[82]

Given the very real logistical and interpretative problems associated with amending the OECD Guidelines, we believe the more important question for Data Protection Commissioners to answer is: why change it? Is it really necessary to amend the OECD Guidelines?

Today, individuals and companies offering services or products to a global market through the Web generally are not aware of, or concerned with, the OECD Guidelines. Voluntary fair information practices are not utmost in the minds of start-up e-commerce ventures. If any awareness of the need to protect privacy online exists at all, the immediate concern is compliance with mandatory legislation, existing agreements, and industry standards. The European Union's *Directive on Data Protection*, the *Safe Harbor Agreement*, and legislation such as Canada's *Personal Information Protection and Electronic Documents Act*, have overtaken the OECD Guidelines in relevance to online business.

Here a standard, there a standard

At the beginning of this paper it was noted that various types of organizations are responding to the public's concerns about online privacy. Daily there are media releases about some product, seal or standard designed to enhance online privacy. However, as repeated studies have shown, these ad hoc measures tend to be woefully inadequate.

While acknowledging the existence of a privacy policy does not equate to effective privacy-protective practices, it is a rough indicator of the degree of privacy awareness online. Recent surveys reveal that while most popular Web sites seem to have some type of privacy policy, the practice is not wide-spread, and the quality of those policies is questionable.

- In the United States, the Federal Trade Commission's most recent report to Congress indicated that while 92% of the Web sites randomly surveyed collected personal information from consumers, and 88% of those sites had at least one privacy "disclosure" or notice, only 20% implemented, at least in part, the four fair information practices of notice, choice, access and security.[83]
- The 1999 version of the Electronic Privacy Information Center's (EPIC) Surfer Beware Survey, *Privacy Policies Without Privacy Protection*, showed that none of the 100 most popular online shopping sites met all the basic criteria for privacy protection. All but 18 of the sites displayed a privacy policy, thereby illustrating the discrepancy between policies and protection. EPIC found that the privacy policies available at many Web sites were typically confusing, incomplete, and inconsistent. As Marc Rotenberg noted: "Companies are posting privacy policies, but these policies are not the same thing as fair information practices."[84]

- An enonymous.com survey showed that of the 30,000 busiest top-level domains, only 25% of the ".com" Web sites and 14% of ".org" sites had a written privacy policy.[85]
- A Jupiter Communications survey found that 68% of European Web businesses collected information on their customers, but only 10% displayed their policy on privacy.[86]
- A June 2000 survey conducted by the Ryerson Polytechnic University revealed one in three on-line retailers failed to provide e-shoppers with adequate security and privacy protection. The study looked at 200 sites in Canada, the United States and Europe and found that, in the area of security and privacy, 36% of the sites were poor, 32% were "satisfactory to good" and only 32% delivered a high performance.[87]

Online consumers are both distrustful and confused by online privacy policies. One study indicated that 64% of respondents were unlikely to trust a Web site regardless of whether or not it posted a privacy policy.[88] A survey in April 2000 by Odyssey indicated that 92% of online households either agreed or agreed strongly with the statement: "I don't trust companies to keep personal information about me confidential, no matter what they promise."[89]

An analysis of online privacy policies conducted for *USA Today* found that, "without exception, policies are ponderous, full of jargon or written so as to leave many surfers scratching their heads." This analysis included sites certified by seal programs such as TRUSTe. The Yahoo! policy, as an example, had 3405 words and 167 sentences. In DoubleClick's policy, a user had to read through over 2000 words, on three different pages, before they came to the opt-out provisions.[90]

Online privacy seals

In our discussion of online policies and practices, a special mention needs to be made of the privacy seal programs. Much has been made of seals in terms of their role in enhancing online privacy. Nielsen/NetRatings rated TRUSTe the most visible symbol on the Internet. Reportedly, as of April 2000, the TRUSTe seal was displayed on all of the Internet's portal sites, 15 of the top 20 sites, and approximately half of the top 100 sites.[91] However, it is important to note that:

> While industry has been quick to point out that many of the most heavily trafficked web sites have posted privacy policies, and belong to seal programs, such sites represent an infinitesimally small proportion of the universe of roughly seven million ".com" web sites. As a result, consumers are likely to be in the dark about the privacy practices of 99.99 percent of commercial web sites.[92]

One of the potential shortcomings is that seal programs only monitor and enforce privacy policies on the Web site, and not other areas of the Internet or offline practices. This limitation was brought into sharp focus with Jason Catlett's complaint to the United States Federal Trade Commission about TRUSTe's investigation of Microsoft Corporation. TRUSTe concluded its investigation of Microsoft's online registration process that generated a secret hardware identification number, by noting that the number had nothing to do with the Web site, so it did not revoke Microsoft's seal.[93]

As Forrester Research noted: "… because independent privacy groups like TRUSTe and BBBOnLine earn their money from e-commerce organizations, they become more of a privacy advocate for the industry – rather than for consumers."[94] Also, the revocation of a seal does nothing to redress privacy violations for the affected individual.

Another, and more troubling problem, relates to the actual privacy standards set by the seal programs. Different seals mean different things. Some are not seals of assurance at all, and do not require adherence to a specified privacy policy.

This office and Australia's federal Data Protection Commissioner conducted a joint study comparing the privacy criteria of the three most popular seals – TRUSTe, BBBOnLine and WebTrust – against the OECD Guidelines. In our opinion, none of these seal programs, at the time of our review, fully met the standards of the OECD Guidelines. The common deficits were no requirement to: 1) limit collection; 2) ensure that data was relevant to the purposes; 3) provide information to the data subject in a reasonable time and manner, without excessive charge, and in an intelligible manner; and 4) provide reasons for any denial of access.

Today, there are many significant policy and technical initiatives shaping online privacy practices. For example, the Council for Internet Commerce developed its *Standard for Internet Commerce*, the International Chamber of Commerce developed its *Guidelines on Advertising and Marketing on the Internet*, and the Internet Engineering Task Force worked on its new standard for assigning Internet protocol numbers. All have merit, but all are different. Exactly who is to follow what standards, in what circumstances, is confusing for all involved. Additionally, as the review of the seal programs illustrates, not all standards address privacy protection in a manner that may be acceptable to Data Protection Commissioners.

If not the OECD Guidelines, then what?

Before we can influence others, we must first agree to what is the appropriate minimum online privacy standard. In their discussion paper on data protection standards in the digital economy, Jos Dumortier and Caroline Goemans noted:

> … electronic business on a global scene is in the long run unthinkable without an international consensus on how individuals should be protected with regard to the processing of their personal data.
>
> The question is how to proceed towards such a consensus? Is it possible to reach a globally accepted behaviour in this domain? Are the cultural, social or political differences not an insurmountable obstacle for an international consensus about personal data protection in online e-business? Fortunately it seems not.
>
> Former experiences such as the OECD guidelines have already demonstrated that it is possible to define a commonly accepted code of "fair information principles" in this area. These principles are certainly too vague to serve as the basis for the behaviour of e-business in this respect. However they may constitute the platform for starting the discussion.[95]

When dealing with international organizations or businesses, Ontario has found the OECD Guidelines to be an excellent platform for starting discussions about online privacy protection. As specified in the OECD Guidelines themselves:

> These Guidelines should be regarded as minimum standards which are capable of being supplemented by additional measures for the protection of privacy and individual liberties.[96]

We believe that the OECD Guidelines are good enough to serve this purpose. They are designed to be a voluntary minimum standard, and as such, they function quite adequately.

As the OECD's Group of Experts on Information Security and Privacy noted in October 1997:

> The relevant question today is not … whether it is necessary to define new principles for the protection of privacy in an expanding global electronic environment, but rather what are the appropriate means of putting these established principles into practice, particularly on the information and communications networks.[97]

We agree, and have taken action in a number of areas in an effort to have some practical impact on online privacy. As examples, we have worked with W3C on its P3P, critiqued the OECD Privacy Policy Statement Generator, and evaluated online privacy seals.

Ontario's online privacy best practices

More relevant to this discussion, Ontario has tried to put the minimum standards set by the OECD Guidelines into operation by developing our own set of online privacy "best practices" (Exhibit B). We developed these in an effort to make the fair information practices set by the OECD Guidelines and Canadian Standards Association's *Model Code for the Protection of Personal Information*[98] more accessible to Ontario businesses and consumers. These practices continue to evolve as the online world, and our understanding of it, changes.

Our best practices are not meant to supersede or compete with existing or future legislation, international agreements, membership requirements for industry associations, or any other mandatory provisions to which Ontario's online companies must comply. They represent an "ideal" to which we would like online businesses to strive. Their purpose is to help elevate online business practices by suggesting privacy-protective alternatives. We see them as a necessary first step in our ongoing efforts to move toward more practical, realistic solutions to online privacy problems.

We use these best practices as an educative tool to encourage companies to examine their online business practices, and to more fully integrate privacy protection into their policies and practices by adopting our suggestions. We have also found them useful in educating Web users on what they should look for and expect in terms of online privacy protection.

A Call for Action

It is our view that to continue to discuss the OECD Guidelines at the annual Data Protection Commissioners' conference is no longer a productive use of our limited time and resources. We strongly believe that Data Protection Commissioners need to focus on how to actually apply these generally accepted fair information principles to the online world, rather than on continuing to debate the principles themselves.

Our recommendation is that the Commissioners accept the OECD Guidelines as the minimum standard for online privacy protection. We believe this is the essential foundation for any harmonized initiatives. It is just the starting point for the action we need to take if we wish to effectively influence online practices.

We also recommend that we start to develop a collective strategy for influencing the public and the online business community regarding effective online privacy protection. To achieve this objective, we need to focus our efforts on the development of a co-ordinated educative and advocacy role for Data Protection Commissioners in the area of online privacy.

Commissioners as educators

Education is a fundamental and indispensable component of any strategy designed to empower the public to make informed choices:

> … consumers generally know little about the ways in which personal information can be used online. They do not understand the potential risks of divulging personal information online, and they need guidance on how to protect that information from unauthorized use. This is true for both new and seasoned users of the Internet. Consumers also need to understand the trade-offs in order to make an informed decision to divulge personal information online.[99]

Recognizing our limited resources, we need to develop educational tools and programs that may be shared across jurisdictions. In particular, we should be creative and take full advantage of the interactive nature of the online world.[100] We need to utilize our respective Web sites and other online resources to greater effect – by developing better links, common information, interactive programs, moderated chat lines, and other types of initiatives. Each of us already has done significant work in this area – we just need to co-ordinate our efforts and products more effectively.

The "Virtual Privacy Office" initiative is an excellent example of the potential to use the Internet to enhance the co-operation between Data Protection Commissioners. The project, initiated by the Privacy Commissioner of Schleswig-Holstein, is open to all privacy protection authorities. The rationale for the Virtual Privacy Office is:

> … a joint venture of privacy protection authorities … can increase their efficiency by intensifying the exchange of information and knowledge as well as sharing work and responsibilities. It makes sense to view such co-operations in a global context and to

orientate them internationally. Thus, all available information concerning privacy protection may be provided in an easily accessible format. Additionally, a privacy protection contact in the Internet will provide assistance for users with actual concerns. Forums for discussions with experts and others interested in privacy protection are intended to enable developments in the field to keep pace with technical progress. The Virtual Privacy Office will realize the technical support of these aspects on the basis of Internet technology.[101]

As of the time of writing, the Federal Commissioner for Data Protection in Germany, the Data Protection Commission in the Netherlands, and the Privacy Commissioners in Switzerland, as well as a number of regional European offices for privacy protection had expressed their intention to co-operate in the project.[102] The Ontario Privacy Commissioner also joined the project. We strongly urge other Commissioners to support this project so that it may develop into a truly international undertaking.

There is great potential to develop co-ordinated initiatives in order to have a simultaneous impact across the world. As an example, we could decide to have our own "surf days" or "sweep weeks," where each Commissioner reported on sites within his/her own country. This would certainly raise our collective profile, particularly with online companies identified as bad privacy offenders in multiple jurisdictions. More importantly, it would capture the public's and the media's attention regarding what we consider to be appropriate online privacy practices. Alternatively, we could sponsor "Awareness" days, akin to the European Commission, or any number of other activities designed to increase public understanding of online privacy issues.

In addition, business must be educated about the importance of online privacy protection. In particular, we need to focus on smaller businesses to demonstrate the benefits of protecting privacy to their enterprises.[103] A Web site operated by one person can collect as much personal information as a site operated by a multinational corporation. Here the Commissioners can play a significant role in protecting the public's interest.

Commissioners as advocates

But education alone is not enough. It should only form part of our relationship with online business. An active advisory and advocacy role also needs to be defined.

As Roger Clarke noted: "User empowerment is not by itself sufficient, because there is an enormous power imbalance between corporations and individuals."[104] Last year, Nigel Waters, citing Ester Dyson, reminded us that consumers are "too busy consuming, or working, or just living regular lives" to be good at protecting their own interests.[105]

Waters enjoined the Commissioners not to be "satisfied with the generally low level of public awareness and understanding of their existence and role." He suggested that a significant role for the Commissioners would be to work "largely behind the scenes to orchestrate the 'mainstreaming' of privacy issues into people's everyday life experiences."[106]

We also believe that Commissioners should not be satisfied with the collective level of influence we have played, to date, in the development and enforcement of online privacy standards. Together, we can have greater influence in terms of encouraging businesses to improve their performance, and lobbying for existing, and developing, online privacy projects to reflect what we consider to be an acceptable minimum standard.

Given our limited resources and disparate geographic locations, should not one of our prime objectives be to become advisors to significant international business initiatives, so that we can use those fora and their membership to advance our agenda? As a group, should we actively become involved with such groups as the Global Business Dialogue on Electronic Commerce, the Council for Internet Commerce, the International Chamber of Commerce, the Electronic Commerce and Consumer Protection Group, the Privacy Leadership Initiative, the Privacy Partnership 2000, and the Internet Policy Institute – all of which are working on online privacy initiatives? At a minimum, should we ensure that we are consulted and have the opportunity to comment on these projects?

Additionally, we could work directly with technology companies to influence how their "default" settings and other controls impacting online privacy are used. We could collectively critique the forthcoming OECD work on dispute resolution to ensure that it meets our objectives. Or we could work with various initiatives to facilitate co-operative and co-ordinated enforcement mechanisms.

If Commissioners think that the groups mentioned above are inappropriate, then perhaps the first order of business should be to develop criteria for the selection and formation of strategic partnerships with organizations deemed appropriate to work with the global community of Data Protection Commissioners.

Personal data protection has become a profitable industry. There are numerous "privacy friendly" tools and methods on the market, and more of them are released daily.[107] As the review of the seal programs illustrates, Commissioners should be concerned about what privacy standards seals and other online privacy initiatives are putting forward. Commissioners have a significant and, we believe, under-utilized role to play in working with organizations developing online standards (both policy and technical) to help them improve their privacy standards.

A united voice

As Fred Cate notes: "… information is inherently global; it respects neither geographic nor legal boundaries."[108] Unfortunately, this is not the case for privacy protection regulation. If we define ourselves by our separate jurisdictions and legislative instruments, we will fail to significantly change online practices. To be effective, our efforts must cut across borders despite the limitations of our individual authority.

Ontario residents do not only surf Ontario Web sites. Accordingly, we believe improving online privacy in all jurisdictions directly impacts the privacy of Ontarians. Illustrating the need for global standards, Graham Greenleaf noted:

> Irrespective of what Australian laws say, a large proportion of internet transactions from Australia will be with ISPs who are out of the effective reach of Australian law … A high percentage of internet privacy breaches against Australians are likely to be untouchable by our laws.[109]

Greenleaf concluded that: "International, accepted and enforceable privacy principles that make sense in cyberspace are … our best defence."[110] We agree entirely.

Online business functions globally and, therefore, so must we. Successfully protecting privacy online requires a greater profile for the Commissioners themselves. We need to move to the centre of the online privacy debate. We need to market and effectively use our expertise and resources.

But we cannot afford to duplicate or ignore the efforts of others. Instead of working against the flow, or in isolation, we need to work with existing online privacy initiatives to steer, guide and encourage. We need to work in partnership with each other, as well as with selected and appropriate international organizations.

Individual Data Protection Commissioners have participated in various online privacy initiatives, but collectively, our voice has been silent. We need to be heard: we can only accomplish that goal if we are united in our focus and objective.

The role that Data Protection Commissioners can play, if we acted in unison about online privacy, cannot be under-estimated. Disapproval by one Commissioner will not likely have an impact on a massive multinational corporation or international standard body. But public disapproval or concern by several, if not all, Commissioners will get noticed – by the media, by the public, and thus by business. The examples of DoubleClick and ToySmart graphically demonstrates the economically detrimental effect that wide-spread media and public concerns can have on a company. We have significant persuasive powers, and we can influence and enforce through the court of public opinion.

To illustrate this point, one of the critical questions that came up in our discussions with the online privacy seal companies was: "How many Commissioners do you represent?" As two – Ontario and Australia – we may not have been considered a significant concern to the seal programs, but as Hong Kong, Brandenburg and Berlin became interested, our analysis took on greater weight. Imagine the impact if we had been speaking on behalf of all the Commissioners!

Conclusion

In the year since we last met, think of the number of new online users and Web sites, of the independent privacy standards developed, of the ineffective company privacy policies posted, and on and on, all without our input or guidance.

At the most fundamental level, our objective is to improve the level of online privacy. We believe the starting point for any action in this area is an agreed-upon privacy protection standard. It is our recommendation that Data Protection Commissioners accept the OECD Guidelines for what they are – as an internationally acceptable minimum standard.

The current situation of having many different and jurisdictionally-based online privacy standards is confusing to both businesses and the public. Having one standard advocated by the world's Data Protection Commissioners could have many benefits. As Colin Bennett and Charles Raab have pointed out, an internationally acknowledged standard can result in greater consistency of policy and practice, and facilitate a higher level of consumer awareness of privacy rights. Ultimately, we believe it would enhance the level of responsibility for the processing of personal data.[111]

Our intent in suggesting that we agree upon a basic online privacy standard – the OECD Guidelines – is to encourage a move from reflection to action. Do the Guidelines have weaknesses? Yes. Should they be updated? Perhaps. If individual Commissioners wish to address any specific limitations of the Guidelines, then we believe the OECD itself would provide the appropriate forum to do so.

But, should the international community of Data Protection Commissioners make revisions to the OECD Guidelines their focus? No. It is our view that time and resources are too limited for such an undertaking. We need to directly focus on influencing the users, Web sites, and those currently setting the online privacy agenda and standards.

We believe that our goal should be on making fair information practices understandable and workable, and bringing existing standards and practices up to the level of the OECD Guidelines, rather than on raising the bar even further. To illustrate how we can build on the existing OECD Guidelines, we included Ontario's Online Privacy Best Practices as an example.

As noted earlier, online privacy is a global problem, and thus we must work toward a global solution. It is our view that only through collective and co-ordinated action will we be truly successful. We can have a unified educative and advocacy voice. We can influence online companies and standards associations. We can influence technical standards and architecture, seal programs and organizational practices. We can focus on developing effective dispute resolution and enforcement mechanisms. Our diversity and sheer geographic scope can make us extremely pervasive and effective in all of our efforts. We must recognize that, in whatever we do to influence online privacy, we will be more effective as a collective voice than as solo Commissioners.

We represent the public's interest in privacy protection, and the public has spoken clearly, again and again, that it has significant online privacy concerns. We have the knowledge, experience, and passion to significantly influence the online world and the protection of privacy globally. But we must act, and act now.

Notes

1. The Hon. Justice Michael Donald Kirby, *Privacy Protection - A New Beginning*, 21st International Conference on Privacy and Personal Data Protection, Hong Kong, September 13-15, 1999, p. 4.

2. Censorware Project, "Size of the web: A dynamic essay for a dynamic medium," http://censorware.org/web_size/, 05/10/00.

3. http://www.DomainStats.com/, 04/27/00.

4. Censorware Project, "Size of the web: A dynamic essay for a dynamic medium," http://censorware.org/web_size/, 05/10/00.

5. "CPA to Play Leadership Role in E-Commerce," Canadian Payments Association Forum, Vol.15, No. 2, June 1999, p. 1.

6. Nua Internet Survey, "How Many Online?" http://www.nua.ie/surveys/how_many_online/index.html, 05/29/00.

7. http://acnielsen.com/products/reports/netwatch/pg2.htm, 05/10/00.

8. "Angus Reid Group: Shopping All Over the World," April 12, 2000, http://www.nua.ie/surveys/?f=VS&art_id=905355712&rel=true, 05/10/00.

9. David Akin, "Microsoft has Canada's pet Web sites: Media Metrix Survey," *Financial Post*, May 25, 2000, p. C9.

10. "NetValue: Europe's Consumers Warm to Ecommerce," May 10, 2000, http://www.nua.ie/surveys/?f=VS&art_id=905355769&rel=true, 05/11/00.

11. "NielsenNetRatings: MSN, Yahoo Top Global Traffic Ratings," May 08 2000, http://www.nua.ie/surveys/?f=VS&art_id=905355764&rel=true, 06/06/00.

12. Cyber Dialogue, Press Release, "Online Privacy Issues Divide Internet Users," April 20, 2000, http://biz.yahoo.com/prnews/000420/ny_cyber_d_1.html, 05/18/00.

13. IBM-Harris Multinational Consumer Privacy Survey, as cited in: Jeff Dodd, "Us vs. Them, How U.S. Privacy Concerns Compare with Rest of World," *Smart Computing, Guide to PC Privacy*, Vol. 8, Issue 4, 2000, p. 11.

14. "Poll identifies on-line concerns," *The Globe and Mail*, December 15, 1999, p. B-4.

15. InsightExpress, Press Release, "What's Your Identity Worth? E-tailers and Web Sites, Pay Up," March 23, 2000, http://biz.yahoo.com/bw/000323/ct_insight_1.html, 05/24/00.

16. TRUSTe, Press Release, "TRUSTe Approves 1000th Web Site: Internet Industry Rallies Around TRUSTe Privacy Seal As Prominent Symbol of Trust Online," January 12, 2000, http://biz.yahoo.com/prnews/000112/ca_truste__1.html, 05/10/00.

17. WebTrust, Press Release, "AICPA'S WebTrust Seal of Assurance Expands Into France, Joining Other EU, Asia-Pacific and North American Countries to Protect Online Privacy and Shopping, January 19, 2000, http://biz.yahoo.com/bw/000119/ny_aicpa_1.html, 05/18/00.

18. Business Wire, "New Online Privacy Protection Tool to Transcent Border," May 18, 2000, http://www.businesswire.com/webbox/bw.051800/201391381.htm, 05/18/00.

19. The Good Housekeeping Web Site Certification, http://www.gh-atyourservice.com/certificate/prog_info.html, 05/19/00.

20. "Council approves final standards for e-commerce," December 14, 1999, http://biz.yahoo.com/rf/991214/bf0.htm, 12/16/99, http://thestandard.com/article/display/0,1151,7229,00.html, http://www.gii.com/standard/about.html, and http://www.gii.com/standard/faq/aboutsic.html#whatis, 05/10/00.

21. PricewaterhouseCoopers, "Global Business Dialogue Finalizes Policy on Protection of Personal Data," June 1999, http://www.pwcglobal.com/8525669400473143/0/A7EC2C3203CEED26852567B60071F0D0?Open&Highlight=2,GBD, 05/08/00.

22. Electronic Commerce and Consumer Protection Group, Press Release, "Internet and E-Commerce Group Proposes Guidelines for Consumer Protection Online," June 6, 2000, http://www.ecommercegroup.org/press.htm, 06/07/00.

23. Privacy Council, Inc., Press Release, "Leading Privacy Company Launches Most Comprehensive Interactive Web Site On Internet," May 4, 2000, http://www.prnewswire.com, 05/05/00, and http://www.privacycouncil.com/, 06/06/00.

24. Privacy Leadership Initiative, Press Release, "Industry Leadership Group to Tackle Privacy Concerns; Privacy Leadership Initiative Focuses on Consumers' Concerns About Privacy and Offers Rapid Work Plan, June 19, 2000, http://biz.yahoo.com/prnews/000619/dc_privacy.html, 06/22/00.

25. Organisation for Economic Co-operation and Development, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, "Explanatory Memorandum," Paragraph 20, http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM, 01/25/00.

26. Ibid., Paragraph 8.

27. Ibid., Paragraph 25.

28. Ibid., Paragraph 37.

29. Ibid., Paragraph 38.

30. Ibid., Paragraph 45.

31. Ibid., Paragraph 27.

32. Ibid.

33. Organisation for Economic Co-operation and Development, Group of Experts on Information Security and Privacy, *Implementing the OECD 'Privacy Guidelines' in the Electronic Environment: Focus on the Internet*, September 1998, DSTI/ICCP/REG(97)6/FINAL, p. 4.

34. Ibid., p. 5.

35. Ibid., p. 6.

36. Organisation for Economic Co-operation and Development, Group of Experts on Information Security and Privacy, *Privacy Protection in a Global Networked Society: An OECD International Workshop with the Support of the Business and Industry Advisory Committee (BIAC)*, Paris, February 16-17 1998, DSTI/ICCP/REG(98)5/FINAL, p. 9.

37. Ibid., p. 6.

38. Organisation for Economic Co-operation and Development, Group of Experts on Information Security and Privacy, *Draft Inventory of Privacy Instruments and Mechanisms for Implementing and Enforcing the OECD Privacy Guidelines on Global Networks*, DSTI/ICCP/REG(98)12.

39. Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, *Inventory of Instruments and Mechanisms Contributing to the Implementation and Enforcement of the OECD Privacy Guidelines on Global Networks*, DSTI/ICCP/REG(98)12/FINAL.

40. Organisation for Economic Co-operation and Development, Committee on Consumer Policy, *Consumer Protection in the Electronic Marketplace*, Ottawa, Canada, October 7–9 1998, DSTI/CP(98)13/REV2, p. 5.

41. Organisation for Economic Co-operation and Development, *OECD Ministerial Conference: 'A Borderless World: Realising the Potential of Global Electronic Commerce,' Conference Conclusions*, Ottawa, October 7-9 1998, SG/EC(98)14/FINAL, Annex 3, p. 18.

42. Ibid., Annex 2, p. 16.

43. Ibid., Annex 1, p. 13.

44. Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, *Ministerial Declaration on the Protection of Privacy on Global Networks*, Ottawa, October 7–9 1998, DSTI/ICCP/REG(98)10/FINAL, pp. 4–5.

45. Ibid., p. 4.

46. Organisation for Economic Co-operation and Development, *OECD Action Plan for Electronic Commerce, OECD Ministerial Conference: 'A Borderless World: Realising the Potential of Global Electronic Commerce*, Ottawa, October 7-9 1998, SG/EC(98)9/FINAL, p. 4.

47. Organisation for Economic Co-operation and Development, Group of Experts on Information Security and Privacy, *Practices to Implement the OECD Privacy Guidelines on Global Networks*, DSTI/ICCP/REG(98)6/FINAL, p. 6.

48. Ibid., p. 15.

49. Ibid., p. 16.

50. Ibid., p. 19.

51. Ibid., p. 20.

52. Ibid.

53. Ibid., p. 22.

54. Ibid.

55. Ibid., Annex 1, "Suggestions for a Privacy-Friendly Web Site Design," pp. 23–26.

56. The OECD Privacy Policy Statement Generator, http://www.oecd.org/scripts/PW/PWHome.asp, 05/21/00.

57. Organisation for Economic Co-operation and Development, *Recommendations of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce*, December 1999, http://www.oecd.org//dsti/sti/it/consumer/prod/CPGuidelines_final.pdf, p. 8.

58. Anne Carblanc, *Data Protection on Global Networks in the Context of Electronic Commerce - recent Activities of the OECD*, Datenschutz - Brücke zwischen Privatheit und Weltmarkt Symposium, August 30, 1999, http://www.datenschutz-berlin.de/informat/heft27/carblanc.html, 12/23/00. See also: Organisation for Economic Co-operation and Development, Working Party on Information Security and Privacy, Report on Transborder Data Flow Contracts in the Wider Framework of Mechanisms for Privacy Protection in Global Networks, DSTI/ICCP/REG(99)15.

59. Kirby, *Privacy Protection - A New Beginning*, p. 4.

60. The Hon. Justice Michael Donald Kirby, *Protection of Privacy and Human Rights in the Digital Age*, International Dimensions of Cyberspace Law, June 30, 1998, http://www.fl.asn.au/resources/kirby/papers/19980630_unespriv.html, 12/23/99.

61. Colin J. Bennett, *Prospects for an International Standard for the Protection of Personal Information: A Report to the Standards Council of Canada*, August 1997, http://www.cous.uvic.ca/poli/bennett/research/ISO.html, 05/15/00.

62. Organisation for Economic Co-operation and Development, *Guidelines*, Explanatory Memorandum, Paragraph 18.

63. Ibid., Paragraph 25.

64. Graham Greenleaf, "Stopping Surveillance: Beyond 'efficiency' and the OECD," *Privacy Law & Policy Reporter*, 3 PLPR 148, December 1996, http://www2.austlii.edu.au/itlaw/articles/efficiency.html, 05/01/00.

65. Graham Greenleaf, "Privacy and Cyberspace: An Ambiguous Relationship," *Privacy Law & Policy Reporter*, 3 PLPR 88, August 1996, http://www2.austlii.edu.au/itlaw/articles/GG_priv_cyber1.html, 05/01/00.

66. Graham Greenleaf, "Privacy Principles - Irrelevant to Cyberspace?," *Privacy Law & Policy Reporter*, 3 PLPR 114, September 1996, http://www2.austlii.edu.au/itlaw/articles/IPPs.html, 05/01/00.

67. Roger Clarke, *Platform for Privacy Preference: A Critique*, July 2 1998, http://www.anu.edu.au/people/Roger.Clarke?DV/P3PCrit.html, 01/19/00.

68. Roger Clarke, *The Legal Context of Privacy-Enhancing and Privacy-Sympathetic Technologies*, April 1999, http://www.anu.edu.au/people/Roger.Clarke/DV/Florham.html, 05/21/00.

69. For details see: Clarke, *Platform for Privacy Preferences: A Critique*; Roger Clarke, *Beyond 'Fair Information Practices': A New Paradigm for 21st-Century Privacy Protection*, February 1998, http://www.anu.edu.au/people/Roger.Clarke/DV/BeyondFIP.html, 05/21/00; Roger Clarke, *The Legal Context of Privacy-Enhancing and Privacy-Sympathetic Technologies*, April 1999, http://www.anu.edu.au/people/Roger.Clarke/DV/Florham.html, 05/21/00; and Roger Clarke, *Serious Flaws in the National Privacy Principles*, April 1998, http://www.anu.edu.au/people/Roger.Clarke/DV/NPPFlaws.html, 12/23/99.

70. Clarke, *Platform for Privacy Preferences: A Critique*.

71. Roger Clarke, *Supplementary Submission: Senate Legal and Constitutional References Committee, Inquiry into Privacy and the Private Sector*, August 5, 1998, http://www.anu.edu/people/Roger.Clarke/DV/SLCCPteSupp.html, 01/19/00.

72. Jos Dumortier and Caroline Goemans, *Personal Data Protection in the Digital Economy: the Role of Standardisation*, Discussion Paper prepared for the EC Workshop in Seville on October 25-26 1999, p.9.

73. Robert Gellman, Conflict and Overlap in Privacy Regulation: National, International and Private, http://ksgwww.harvard.edu/iip/gellman.html, 04/07/97.

74. Freehill, Hollingdale and Page, *Internet Privacy Survey Report 2000*, p. 6.

75. Testimony of Jerry Berman, Executive Director, Center for Democracy and Technology, Before the Judiciary Committee, Subcommittee on Courts and Intellectual Property, May 27, 1999, http://www.cdt.org/testimony/Berman.test.House.5.27.99.shtml, 04/26/00.

76. Ibid.

77. John Schwartz, "Intel Exec Calls for E-Commerce Tax," *The Washington Post*, June 6, 2000, http://www.washingtonpost.com/wp-dyn/articles/A7358-2000Jun6.html, 06/07/00.

78. Marc Rotenberg, *Preserving Privacy in the Information Society*, http://www.unesco.org/webworld/infoethic_2/emg/papers/paper_10.html, 12/23/99.

79. Nigel Waters, *Re-Thinking Information Privacy - A Third Way in Data Protection?*, 21st International Conference on Privacy and Personal Data Protection, Hong Kong, September 13–15, 1999, p. 51.

80. Joel R. Reidenberg and Paul M. Schwartz, *Data Protection Law and On-Line Services: Regulatory Responses*, n.d., p. 122.

81. Kirby, *Protection of Privacy and Human Rights in the Digital Age*.

82. Waters, *Re-Thinking Information Privacy*, p. 52.

83. Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress*, May 2000, pp i & ii.

84. John Schwartz, "Internet Privacy Eroding, Study Says," *The Washington Post*, December 17, 1999, http://www.washingtonpost.com/wp-srv/WPlate/1999-12/17/085l-121799-idx.html; and EPIC, *Surfer Beware III: Privacy Policies without Privacy Protection*, December 1999, http://www.epic.org/reports/surfer-beware3.html, 12/20/99.

85. PrivacyRatings.org, *Enonymous.com Publishes Comprehensive Study of Privacy Policies: Report of 30,000 Web Sites Shows Major Changes in Internet Treatment of Privacy*, http://www.privacyratings.org/research.htm, 05/19/00.

86. Justin Pearse, "News Burst: Web businesses ignore privacy concerns," *ZDNet*, http://www.zdnet.co.uk/cgi-bin/printnews.cgi, 05/16/00.

87. Marina Strauss, "E-tailers failing to protect shoppers Study warns security, privacy not adequate," *The Globe and Mail*, June 21, 2000, http://www.globeandmail.com/, 06/22/00.

88. Christopher D. Hunter, *Recoding the Architecture of Cyberspace Privacy: Why Self-Regulation and Technology are not Enough*, December 1999, http://www.asc.upenn.edu/usr/chunter/net_privacy_architecture.html, 01/13/00.

89. Steve Lohr, "Survey Shows Few Trust Promises on Online Privacy," *The New York Times*, April 17, 2000, http://www.nytimes.com/library/tech/00/04/biztech/articles/17/data/html, 04/17/00.

90. Will Roger, "Privacy isn't public knowledge, Online policies spread confusion with legal jargon," *USA Today*, http://www.usatoday.com/life/cyber/tech/cth818.htm, 05/02/00.

91. TRUSTe, Press Release, "Bell Atlantic Teams with TRUSTe Privacy Program To Create Safe Online Environment," April 5, 2000, http://www.truste.org/about/about_bellatlantic.html, 05/29/00.

92. Hunter, *Recoding the Architecture of Cyberspace Privacy*.

93. Jeremy Quittner, "Should You Pay for a Privacy Seal of Approval?," *Business Week Online*, http://www.businessweek.com/cgi-bin/ebiz/ebiz_frame.pl?url=/ebiz/0005/ec0502.htm, 05/05/00.

94. Jason Catlett, President, Junkbusters Corporation, as cited in Hunter, *Recoding the Architecture of Cyberspace Privacy*.

95. Ibid., p.18.

96. Organisation for Economic Co-operation and Development, *Guidelines*, Part One, Paragraph 6.

97. Organisation for Economic Co-operation and Development, *Implementing the OECD 'Privacy Guidelines' in the Electronic Environment*, p. 6.

98. Canadian Standards Association, *Model Code for the Protection of Personal Information*, CAN/CSA-Q830-95, CSA International, http://www.csa.ca/english/home/index.htm, 06/03/00.

99. Staff Report, *Public Workshop on Consumer Privacy on the Global Information Infrastructure*, December 1996, p. 25.

100. Ibid.

101. Privacy Commissioner Schleswig-Holstein, *The Virtual Privacy Office and Its Modules*, March 8, 2000, http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/projekte/virdsb/module_e.htm#1, 06/22/00. See also, Bruno Baeriswyl, Helmut Bäumler, John J. Borking, and Marit Köhntopp, *The Virtual Privacy Office – A New Approach to Privacy Protection*, Submission to ISSE 2000, http://www.koehntopp.de/marit/publikationen/privacyoffice/BBBK_Submission_to_ISSE_2000.pdf, 06/22/00.

102. Privacy Commissioner Schleswig-Holstein, *The Virtual Privacy Office - An Introduction*, March 8, 2000, http://www.rewi.hu-berlin.de/Datenschutz/DSB/SH/projekte/virdsb/allgem_e.htm#8, 06/22/00.

103. Ibid.

104. Clarke, *Platform for Privacy Preference: A Critique*.

105. Waters, *Re-Thinking Information Privacy*, p. 57.

106. Ibid., p. 53.

107. Dumortier and Goemans, *Personal Data Protection in the Digital Economy*, p.6

108. Fred H. Cate, "Global Information Policymaking and Domestic Law," *Global Legal Studies Journal*, http://www.law.indiana.edu/glsj/vol1/cate.html, 08/11/98.

109. Greenleaf, *Privacy Principles - Irrelevant to Cyberspace?*

110. Ibid.

111. Colin J. Bennett and Charles D. Raab, "The Adequacy of Privacy: The European Union Data Protection Directive and the North American Response," *The Information Society*, 13:245–263, 1997 p. 257.

Exhibit A

OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data

Part Two. Basic Principles of National Application

Collection Limitation Principle

7. There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

Data Quality Principle

8. Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

Purpose Specification Principle

9. The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.

Use Limitation Principle

10. Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except:

    a) with the consent of the data subject; or

    b) by the authority of law.

Security Safeguards Principle

11. Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.

Openness Principle

12. There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

Individual Participation Principle

13. An individual should have the right:

    a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;

    b) to have communicated to him, data relating to him

        1. within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him;

    c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and

    d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

Accountability Principle

14. A data controller should be accountable for complying with measures which give effect to the principles stated above.

Latest update 05 January 1999
http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM, 05/18/00

Exhibit B

Office of the Information and Privacy Commissioner/Ontario Best Practices for Online Privacy Protection

Respect for Privacy

- Do business in the least privacy-intrusive manner possible. Do not deliberately violate an individual's privacy.
- Understand and comply with applicable privacy legislation, agreements, and standards.
- Recognize individuals as the owners of their own personal information.
- Recognize that individuals have the right to exercise reasonable control over their own personal information. Therefore, consult with individuals on matters relating to your management of their personal information.
- Understand that personal information includes all information about, or linked to, an identifiable individual. This includes such information as name, address, income, and purchase preferences, as well as e-mail, site registration, and transaction information. Data collected from third parties or from automatic technological methods may also constitute personal information.
- Understand and acknowledge your responsibility, as temporary custodian, to protect individuals' personal information.
- Help individuals exercise their rights to the maximum extent possible.
- Assess the impact on privacy of any proposed new practice, service, product, or technology, prior to implementation. If the activity potentially will adversely impact privacy, do not do it, or find a less privacy-invasive way. Alternatively, fully advise individuals of the impact on privacy and obtain their explicit consent prior to proceeding.
- Educate individuals about the potential privacy risks of using the Internet and doing business online (e.g., that any message sent to request information from a site indirectly may reveal the sender's e-mail address; that data on their local hard drive in their cache files may be disclosed; or that if they disclose their personal information in newsgroups or public forums operated by you, other parties may collect, use, and disclose that information). Also inform individuals of the privacy and security options available to them to minimize those risks.
- Build privacy protection measures into your contracts with business partners or third parties who will have access to personal information collected or controlled by your organization. This is particularly important if you will be sending personal information to jurisdictions without comparable privacy protection regulation. Take all reasonable steps to ensure the contracted party follows the privacy protection measures stipulated in your contracts (e.g., site visits).
- Understand that special care must be taken when dealing with children. If there is the potential of collecting, using, or disclosing personal information about children, follow related legislative requirements and develop appropriate privacy practices.

Openness

- Develop privacy protection policies and practices that require personal information to be handled in an open and accountable manner.
- Be open and informative about your organization's policies and practices involving personal information.
- Ensure your stated policies and practices are factual, accurate, and complete. Do not misrepresent your identity or your information practices.
- Inform individuals of any records your organization maintains that contain their personal information. Do not keep information management practices or record-keeping systems containing personal information secret from the individual to whom the data relates.
- Communicate your privacy protection policies and practices to individuals in a manner that enables them to understand and exercise their rights.
- Prepare and post a privacy policy on your Web site. That policy should clearly explain all your responsibilities and practices as outlined in these best practices. Specifically, it should be designed so it is:
    - easy to find, easy to read, and easy to understand (e.g., use illustrative examples to explain and demonstrate your policy and practices);
    - written in the same language as the Web site to which it is attached;
    - accessible from every Web page, not just the homepage;
    - easy to print;
    - necessary for the individual to click through and acknowledge it prior to commencing a transaction or the collection of any personal information.
- Do not make your privacy policy a legal disclaimer or reserve the right to modify it and your practices without adequate justification and notification. Do not change your stated privacy policies and practices without notifying individuals in a manner that gives them sufficient time and information to make an informed decision and take appropriate action.
- Inform individuals of all applicable privacy legislation and agreements, and provide links to the authorities responsible for the administration and enforcement of these instruments.
- Inform individuals of all professional codes of practices, seals, or other programs that you must be in compliance with, and provide links to the full text of these agreements, and to the organizations responsible for the proper implementation and enforcement.
- Notify individuals if access to any or all of your Web site is conditional upon them agreeing to disclose personal information to you or third parties (e.g., banner ad networks), or to the automatic collection of clickstream data.

- Explain your use of any type of automatic tracking software and clickstream data.
- Explain your own solicitation practices (e-mail and other means), as well as what personal information you rent, sell, or exchange to third parties for marketing purposes.
- Explain all data mining or other modelling practices, including what happens to the individual's personal information after it is de-identified, if applicable.

Accountability

- Acknowledge publicly your commitment to comply with your stated privacy policies and practices.
- Ensure privacy protection is a priority for all levels of your organization. Top level commitment to privacy policies and practices is critical for success.
- Train your staff and make them accountable for adherence to your privacy policies and practices.
- Designate a specific individual or area as responsible for protecting privacy and complying with your privacy policies (i.e., the data controller). For larger organizations it may be necessary to engage a team to share the responsibility. Give them sufficient resources and authority to discharge this responsibility in an effective and timely manner.
- Publicize the identity of the data controller on your Web site, along with information about how the individual can communicate with them on- and offline, and your days and hours of operation, if applicable.
- Establish procedures to review your privacy policies and practices to ensure they remain accurate and complete. This should be done annually, at a minimum.
- Develop effective mechanisms to verify your compliance with your stated privacy policies and practices, and to be able to publicly demonstrate that compliance. At a minimum, this should be a practice of self assessment or periodic internal audits. If possible, have your privacy policies and practices reviewed by an appropriately qualified independent professional service or authority.
- Review the effectiveness of your internal compliance programs at least annually, and revise them, where appropriate.
- Provide individuals with the opportunity and information necessary for them to be able to exercise and enforce their rights quickly, effectively, and without prohibitive cost.
- Inform individuals of the consequences to your organization for non-compliance with your own privacy policies, and with all other relevant programs and legislation (e.g., audit, penalties or sanctions, revocation of seal, loss of professional membership, complaint forwarded to an oversight body for investigation, or publication of non-compliance).
- Inform individuals of their recourse if you are non-compliant with your own policies and practices, or with any other relevant program or legislative requirement.

- Define your obligation to undertake all necessary action, at no cost to the individual, to correct any problems that arise out of your non-compliance with your own policies and practices, or with any other program or legislative requirement.

Purpose Specification

- Define the purposes or reasons why you think you need each piece or type of personal information (e.g., name, address, IP address, clickstream data, age, gender, income, etc.) in order to complete a specific, legitimate business transaction. When identifying potential purposes, consider the following:
  - how the personal information needs to be collected (e.g., directly from the individual through a subscription, automatic collection of clickstream data, or from a third party) and why.
  - who will need to use the information (within and outside the organization), and why.
  - to whom it will need to be disclosed, and why.
- Identify any additional reasons to collect, use, or disclose personal information not strictly related to a specific business transaction (e.g., incentive programs, target e-mail marketing services, data mining or other modelling tools, and the like).
- Determine if the identified reasons for collecting, using, and disclosing individuals' personal information could invade their privacy. Consider if the purposes are still valid or appropriate, given the potential impact to individuals' privacy, and if there are less privacy-invasive ways of achieving your business objective.

Individual Knowledge and Consent

- Obtain consent prior to collecting, using, or disclosing an individual's personal information, whenever possible. Consent is particularly important when collecting, using, or disclosing sensitive personal information, such as medical or financial data.
- Define narrowly the exceptional circumstances where consent is not required or is inappropriate (e.g., urgent medical or security reasons). If consent is not possible or appropriate, ensure the individual has full knowledge of the proposed activity prior to its undertaking, along with an explanation of why consent is not possible/appropriate.
- Provide individuals with clear and adequate information for them to make an informed decision about giving their consent, including the consequences of refusing consent, if any.
- Take reasonable steps to verify the identity of the individual who is providing the consent to ensure it is the individual to whom the personal information relates or an authorized representative.
- Do not deceive or coerce individuals in order to obtain their consent.

- Do not infer consent because individuals complete a form on your Web site or otherwise submit information. Independently confirm consent.
- Obtain consent if you want to use or disclose an individual's personal information for any purpose not identified at the time of collection. Express consent (e.g., opt-in) to such secondary uses is preferred to implied consent or the use of a negative option (e.g., opt-out).
- Provide individuals with a simple and clear online mechanism to indicate their consent or choice regarding the collection, use, and disclosure of their personal information. Do not require individuals to call or write in to make their wishes known. Maintain a record of consent and make it accessible to individuals for their review.
- Carry out individuals' choices/wishes in a timely manner.
- Provide individuals with the opportunity to challenge your organization's decision regarding the feasibility or appropriateness of obtaining their consent, prior to your collecting, using, or disclosing their information.
- Do not revoke opt-in/opt-out options or change time limitations without prior and adequate notice to the individual.
- Inform individuals of exactly what is and is not covered by your consent provisions (e.g., collection and use by your Web site only, clickstream analysis, data mining, or disclosure to third party) and if it is time-limited.
- Ensure individuals are able to withdraw their consent to the collection, use, or disclosure of their personal information at any time, subject to legal or contractual restrictions and reasonable notice. Inform individuals of the implications of withdrawing consent and how to do so.
- Obtain explicit consent before storing, altering, or copying any information on an individual's computer.
- Provide individuals with a simple and clear online mechanism for them to opt-out of the use of any type of automatic tracking software, by you or third party, as well as the automatic disclosure of clickstream data to third parties.
- Obtain consent prior to renting, selling, trading, sharing, or otherwise disclosing an individual's personal information to a third party for marketing purposes.
- Provide individuals with a simple and clear online mechanism to indicate their wishes regarding receipt of any kind of on- and offline marketing communications from you or third parties. At the time of that selection, ask individuals if you can follow-up with them, and how they want to be contacted, if at all.
- Obtain explicit and verifiable consent by the child's parent or authorized guardian prior to the collection, use, or disclosure of any personal information related to a child.

Collection Limitation

- Understand that if you collect personal information, you accept the responsibility to handle that data in accordance with your stated privacy policies and practices, and to make that information available to the individual to whom it relates. If you cannot do that, do not collect the personal information.
- Collect no personal information, whenever possible (e.g., permit the individual to visit your Web site without capturing clickstream data, or let the individual deal with you anonymously or pseudonymously).
- Collect only the amount and type of personal information necessary and relevant for the identified purpose(s), or as required by law.
- Collect personal information by lawful and fair means and from reliable sources.
- Do not collect personal information in a covert, clandestine, or coercive manner, or through misleading or deceptive practices.
- Collect personal information directly from the individual to whom it relates, except in limited circumstances.
- Inform individuals of all types and sources of personal information indirectly collected by automated means or from third parties prior to collection. Also indicate why direct collection is not possible.
- Notify individuals, at or before the time of collection, of all of the purposes for which their personal information will be collected, used, and disclosed. Distinguish between the information required for fulfilment of the identified purposes and any optional information.
- Inform individuals of the consequences of providing and withholding all or part of their personal information.
- Notify individuals, at or before the time of collection, if the personal information to be collected is required by law and, if so, fully explain the specific requirement.
- Inform individuals of their options to restrict the collection of their personal information, if any, and provide them with sufficient means and information for them to be able to effectively exercise their options.
- Explain if individuals' personal information will be de-identified and used for data mining or other modelling processes prior to collection.
- Avoid collecting unique identifiers (e.g., SIN or driver's licence numbers) unless their use is required by law, or explicit consent is obtained from the individual. If required to collect unique identifiers (e.g., for tax requirements), explain reasons to the data subject prior to collection.
- Comply with legislative restrictions on the collection of personal information (e.g., human rights legislation may limit what may be collected on employment applications).

- Inform individuals if data you collect online is handled differently offline and why. If it is, specify how and instruct them how they can interact with your organization through other means (e.g., mail, in person, fax, or telephone).

Use and Disclosure Limitations

- Do not use personal information except in the manner, and for the purpose(s), identified to the individual at the time of collection, unless the individual to whom the personal information relates consents, or by authority of law.
- Do not disclose, distribute, or make available in any way personal information, except for the purpose(s), and to the sources (internal and external), identified to the individual at the time of collection, unless the individual to whom the personal information relates consents, or by authority of law. Maintain a record of disclosure.
- Take all reasonable steps to ensure that personal information you use and disclose is relevant and necessary to fulfil the identified purpose(s) or the requirements of law.
- Provide individuals with a simple and clear online mechanism to express their consent or refusal for uses and disclosures of their personal information not identified at the time of collection.
- Do not withdraw access to services or products to individuals if they refuse to permit the use or disclosure of their personal information for purposes not identified at the time of collection.
- Do not use clickstream data or any type of tracking technology or software without the explicit consent of the individual.
- Use both policy and technical restrictions to control unauthorized and unrelated uses and disclosures.
- Limit your employee access to personal information to only those with legitimate business reasons. This should include access by your information technology staff.
- Do not use or disclose personal information for promotional or marketing purposes, unless the individual has consented.
- Inform the individual of any legal requirements you have to disclose personal information and to whom.
- Identify the circumstances when disclosure may take place without the individual's prior knowledge or consent (e.g., serious and imminent threat to public health or safety).
- Do not knowingly disclose or transfer personal information to third parties without adequate privacy safeguards.

Accuracy

- Do not knowingly collect, use, or disclose inaccurate personal information.
- Take all reasonable measures to ensure personal information is accurate, complete, and up-to-date, having regard for the nature of the data and the purpose(s) for which it is collected, used, and disclosed.
- Do not base decisions affecting individuals solely on unverified information, particularly if the data was collected from a third party.
- Establish a process to correct or delete inaccurate information in a timely manner. The process should be simple, easy to use, accessible online, and provide assurance to the individual that inaccuracies have been corrected and, to the extent reasonably possible, third parties who accessed the relevant data within the last year have been informed of the correction.
- Establish reasonable controls, schedules, and practices for information and records retention. Ensure retention schedules and practices are fully documented.
- Retain personal information in identifiable form only as long as it is relevant and necessary to fulfil the purpose(s) for which it was collected or as required by law.
- Establish procedures to ensure that personal information is not disposed of too soon.
- Destroy, erase, or permanently de-identify any personal information no longer needed for its identified purpose(s) or legal requirements.

Security

- Protect all personal information in your control from loss or theft, and from unauthorized access (from within and outside your organization), use, alteration, copying, disclosure, and destruction.
- Establish security safeguards appropriate and proportional to the sensitivity of the personal information and the nature of the possible risks.
- Implement effective physical, technical, and procedural measures to secure personal information.
- Inform individuals at the time of collection of the security measures you will undertake to protect their personal information.
- Inform individuals of the steps they can take to conduct online transactions safely and securely. At a minimum, provide individuals with the opportunity to encrypt their personal information during the course of communication or transactions with your organization.
- Ensure individuals using your Web site cannot access other people's personal information.

- Verify the identity of individuals or third parties prior to permitting use or disclosing personal information to ensure they are authorized to access such data.
- Establish secure disposal procedures to ensure personal information cannot be recreated or reconstructed after destruction or the individual cannot be identified or linked to that data in any way.
- Create a record of destruction documenting how, when, and who authorized the disposal of personal information.
- Do not store confidential or sensitive personal information online. Move such data to secure non-networked computers.
- Take all reasonable measures to ensure your Web site and computer system are protected from unauthorized outside access.
- Establish appropriate audit trails and record integrity controls to track access and to ensure personal information has not been tampered with or altered in an unauthorized way.
- Notify individuals of any security or privacy violations involving their personal information as soon as technically possible, and instruct them on what action they may take to remedy the problem or minimize the risks.
- Take all reasonable steps to ensure third parties involved in a transaction (e.g., those renting or leasing the data, as well as any party contracted to your organization to conduct such activities as data processing or data mining) have adequate security.
- Take all reasonable steps to ensure that communications or transactions with your Web site do not result in unauthorized access to individuals' computers or information, or unauthorized modification or destruction of their data.
- Use privacy-enhancing technology, whenever possible.

Right of Access and Correction

- Design your Web site and supporting systems and practices to facilitate individuals' right to access their own personal information, and to challenge the accuracy and completeness of their personal information in your control.
- Inform individuals of their right to access and correct their own personal information and how that right may be exercised.
- Establish a simple, accessible, and easy-to-use online process for individuals to find out:
    - the existence and nature of all their personal information in your control (i.e., both on- and offline);
    - the purposes for the collection, use, and disclosure of the data;

- to whom it has been disclosed;
- the full cost of access (costs should be reasonable and demonstrable);
- the sources of the personal information (whenever possible); and
- the name and location of the person/area in charge of the information.

- Establish clear and limited criteria for why individuals' requests for access to, or correction of, their personal information may be denied. Include these reasons in your privacy policies.
- Give individuals a secure online mechanism to access to their personal information in an understandable format, and without undue delay or expense (e.g., at no or minimal cost), upon request, and whenever reasonably possible.
- Provide individuals with a simple, accessible, and easy-to-use online process to review and correct their personal information.
- Verify the identity of the individual before granting access to, or correction of, any personal information.
- Provide individuals with the following if you deny their request to access or correct their personal information:
  - the reasons for that decision in a timely and understandable manner;
  - an opportunity to prepare a "statement of disagreement" and have it, along with your reasons for denial, attached or linked to the data in question, if their challenge remains unresolved; and
  - a fair opportunity to challenge the decision.
- Provide individuals with the opportunity to propose or negotiate alternatives by redefining the request, suggesting a different methods of access, cost sharing, etc.
- Establish a fair and equitable dispute resolution mechanism that is accessible to the individual online. Do not charge the individual for the opportunity to exercise their right to challenge your denial of access decision.
- Correct or destroy personal information found to be inaccurate, incomplete, irrelevant, or inappropriate, as quickly as reasonably possible.
- Take all reasonable measures to inform third parties who have used or accessed the incorrect personal information within the last year of the corrected information or unresolved challenges.
- Ensure all subsequent access is to the corrected personal information or to the statement of disagreement.

Complaints/Dispute Resolution

- Develop procedures to receive, investigate, and respond to complaints and questions. Permit as much online interaction as possible.
- Respond to complaints and take corrective action, as appropriate, in a timely manner.
- Establish a simple, easy-to-use, online mechanism for individuals to challenge your business practices and compliance with all aspects of your posted privacy policies and practices.
- Ensure your process for receiving and responding to inquiries and complaints, along with the individual's recourse, is fully described and easily found on your Web site.
- Ensure your complaint or dispute resolution process is effective, fair, impartial, confidential, understandable, easy-to-use, and timely. It also should be cost effective for all parties involved to the extent reasonably possible.
- Inform individuals of any third party investigative and dispute resolution procedures available to them.
- Direct individuals to relevant authorities (e.g., a Data Protection Commissioner or seal program) if you cannot resolve the complaint to the individual's satisfaction. Alternatively, make available a third party dispute resolution mechanism on an optional basis. Such processes should be accessible, affordable, and impartial for all parties.

Information and Privacy Commissioner/Ontario

2 Bloor Street East
Suite 1400
Toronto, Ontario
M4W 1A8

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca