PUBLICLY AVAILABLE PERSONAL INFORMATION AND CANADA'S PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT

Rick Shields

McCarthy Tétrault

Ottawa

October 12, 2000

TABLE OF CONTENTS

INTRODUCTION

This paper has been produced by McCarthy Tétrault for Industry Canada. Our mandate was to explore the concept of "publicly available information" as that phrase is used in sections 7 and 26 of the *Personal Information Protection and Electronic Documents Act* (the "Act"), S.C. 2000, c.5. More particularly, we have been charged with the task of fleshing out that concept by examining various matters of relevance to it in a Canadian setting.

With that task in mind, Part 1 of our paper examines the manner in which technology is changing the private sector's use of publicly available personal information. Part 2 considers the inherent policy tension existing between access to information and privacy initiatives in Canada and abroad, before going on to review the way that Canada's Federal Court has interpreted the meaning of "publicly available" within the context of existing federal privacy and access to information legislation. Part 3 explores the legislative methods employed in certain other jurisdictions to respond to the "privacy versus free access" issues raised by the private sector's new techniques for processing personal information. Part 4 of our paper looks at the views expressed by academics, regulatory officials and others regarding the optimal means of balancing these competing policy impulses, and the ambit of the regulation making power granted by the Act as it pertains to publicly available information.

As we have also been asked to identify, based upon our research, possible limits that might be placed upon the collection, use and disclosure of publicly available personal information by the private sector in Canada, Part 5 of our paper contains a brief discussion of a number of limits that might merit consideration.

PART 1 WHAT IS PUBLICLY AVAILABLE PERSONAL INFORMATION?

1(i) Varying Forms of Publicly Available Personal Information

The phrase "publicly available personal information" in its broadest sense encompasses all personal information that has entered the public realm by any means whatsoever. For the purposes of this paper, however, it is useful as a means of providing a conceptual framework to bear in mind some of the more common forms of that type of information. One of the most familiar can be found in nearly every Canadian household: the white pages telephone directory, which furnishes the names, telephone numbers and addresses of millions of Canadian subscribers. Similarly ubiquitous are the nation's newspapers and periodicals, which, together with the more transitory media, television and radio, deliver large amounts of third party personal information to Canadians every day.

Perhaps the largest potential sources of publicly available information, and the sources which are dealt with most extensively in this paper[1], are the diverse public registries maintained across Canada by all three levels of government. These registries collectively contain a vast amount of personal information about Canadians that ranges across the spectrum of sensitivity from mildly sensitive (e.g. eye colour) to the extremely sensitive (e.g. health histories, criminal histories). The purposes underlying these registries are as disparate as the legislation that created them - some are repositories of information concerning those individuals holding licences issued by government (e.g. hunting licences, taxi licences), while others are designed to provide an administrative framework for commercial activity (e.g. real property registries) or to track differing forms of social behaviour (e.g. marriage and divorce records).

[1] This differentiation was not by design. While the privacy implications of public records data mining have generated debate worldwide, private sector use of personal information gleaned from directories or media sources has proven to be far less controversial. Accordingly, this aspect of the "publicly available information" equation has generated much less commentary.

A considerable variance also exists in the degree of public access that is permitted to records contained in these registries. While, for example, all personal information contained in a real property or corporations registry might be available for public consultation, information contained in an individual's drivers record abstract might be accessible only to a small subset of the public (e.g. insurance providers). Other information (e.g. criminal history) might not be available to anyone other than law enforcement officials except in very limited circumstances (e.g. media accounts of specific court proceedings, sexual predator announcements).

While a truly comprehensive listing of sources of publicly available personal information would be very difficult to produce and is, in any event, beyond the scope of this paper, the following brief listing details some of the more significant sources:

- telephone directory listings
- property tax records
- drivers licence and other licence records
- automobile registrations
- census and electoral data
- birth/marriage/divorce/death records
- news media
- credit histories
- court decision databases and other court records
- corporate and other business-related registries
- some commercial mailing lists
- business and professional directories
- some Internet tracking information
- promotional contests
- subscriptions.

When taken together, it becomes readily apparent how private parties with an interest in systematically compiling information about Canadians might view these sources as a very fertile field, subject to the constraints of access and technological capacity.

1**(ii) Federal Court of Canada Decisions Respecting Access to Information/Privacy**

The term "publicly available" found in paragraphs 7(l)(d), 7(2)(c.l) and 7(3)(h.l) is not defined in the Act. While at first blush its meaning may appear self-evident, the legal parameters of public availability have, in fact, been the subject of considerable legal debate in Canada. The resulting court and administrative decisions, in particular those originating with the Federal Court of Canada, will doubtlessly help to frame the analysis of this aspect of the Act in future court proceedings.

Pursuant to sections 14 through 17 of the Act, the Federal Court - Trial Division is the Canadian court with the primary responsibility for hearing disputes arising under the Act. This entails hearing applications brought by aggrieved individuals or by the Privacy Commissioner concerning (i) any alleged contraventions by organizations[2] of Division 1 of Part 1 of the Act or (ii) the failure of organizations to comply with a recommendation contained in Schedule I of the Act. The Federal Court is also responsible, pursuant to section 18.1 of the *Federal Court Act*[3], for hearing any applications for judicial review that might be brought concerning the actions of the Privacy Commissioner when exercising his or her statutory authority or concerning the exercise by the Governor in Council of the regulation-making authority granted to it under the Act.[4]

---

2 As defined in section 3 of the Act.

3 R.S.C. 1985, F-7.

4 When the Governor in Council acts pursuant to a statute, it is deemed at law to be a "federal board" for the purposes of section 18.1 and is therefore susceptible to having its actions judicially reviewed. See *Re Saskatchewan Wheat Pool et al. and Attorney-General of Canada* (1994), 107 D.L.R. (4th) 190 at 192 (F.C.T.D.).

As the Act is not yet in force, the Federal Court has not been required to consider the meaning of "publicly available" in the context of sections 7 and 26 of the Act. It has, however, examined the legal dimensions of public availability on a number of occasions in the past when hearing disputes involving the federal *Access to Information Act* ("AIA").[5] The AIA establishes the legal means by which a person may obtain access to information under the control of a federal department or a specified federal agency.[6] Such access is not unrestricted; the AIA contains, in sections 13-24, a number of exemption provisions that limit the general right of access.

One such provision is section 19 of the AIA, which stipulates that government institutions[7] shall refuse, subject to the restrictions contained in subsection 19(2), to disclose records containing "personal information" as defined in section 3 of the federal *Privacy Act* ("PI").[8] The PI imposes restrictions on the collection, use or disclosure of personal information by federal departments and specified federal agencies.[9] It also grants individuals the right to obtain access to their own personal information that is under the control of a federal institution.[10] Paragraph 19(2)(b) of the AIA vests heads of government institutions with the discretion to release records containing personal information without the consent of the individual whose personal information is at issue if the information is already publicly available.

Also of relevance to the issue of public availability have been the Federal Court's findings with respect to the meaning of the term "confidential" as it is used in paragraph 20(1)(b) of the AIA. That paragraph creates an exemption from disclosure in some circumstances for third party financial, commercial,

---

5 R.S.C. 1985, c. A-1.

6 *Ibid*., section 4.

7 As defined in section 3 of the AIA.

8 R.S.C. 1985, c. P-21.

9 *Ibid*., sections 4-8.

10 *Ibid*., section 12.

scientific or technical information that is confidential and that has been treated consistently in a confidential manner.

When interpreting the AIA, the Federal Court has established legal parameters for the concept of public availability which it is reasonable to expect will be applied by that court if it is called upon to consider sections 7 and 26 of the Act. The central legal issue, not surprisingly, has involved determining the point at which personal information ceases to be private or confidential and becomes public. The general rule that has emerged is that information, whether personal or otherwise, becomes publicly available, and ceases to be private/confidential, when it has become accessible by the public by any means.[11] The test as to whether information has passed into the public realm is an objective one; a party's perception that information remains confidential and private is not determinative if the evidence reveals that the information became available to the public from another source.[12] Public availability can be established even in circumstances where no member of the public has previously exercised the right of access[13] or where the public right of access is subject to restrictions.[14]

Personal information has also been found to be publicly available in circumstances where the item of information at issue could have been gleaned from a number of distinct public sources. In *Canada*

---

11 *Maislin Industries v. Minister for Industry, Trade and Commerce et al*., [1984] 1 F.C. 939 at 944; *Noel v. Great Lakes Pilotage Authority Ltd*., [1988] 2 F.C. 77 at pp. 83-84; *Air Atonabee v. Canada (Minister of Transport)* (1989), 37 Admin. L.R. 245 at 268.

12 *Canada Packers Inc. v. Canada (Minister of Agriculture)*, [1988] 1 F.C. 483 (T.D.); *Cyanamid Canada Inc. v. Canada (Minister of Health and Welfare)* (1992), 52 F.T.R. 22 (T.D.), (1992), 45 C.P.R. (3d) 390 (F.C.A.); *Timiskaming Indian Band v. Canada (Minister of Indian and Northern Affairs)* (1997), 148 D.L.R. (4th) 356 at 365.

13 *Timiskaming*, supra, p. 364.

14 In *Canada (Information Commissioner) v. Canada (Minister of Public Works and Government Services)*, [1997] 1. F.C. 164 (T.D.), Richard J. ruled, at p. 179, that information available to patrons of the Library of Parliament was publicly available despite the fact that permission is normally required to access the Library's collection.

(Access Commissioner), supra, Richard J. held that a list of Members of Parliament showing the date of their election was publicly available because it could have been compiled from various sources including old newspapers, the *Who's Who of Canada* and Elections Canada publications. He concluded that when different items of publicly available personal information are combined, the resulting information product is also publicly available.

The federal Court has ruled that there may, nonetheless, be circumstances where personal information would not be considered to have become publicly available despite having been disclosed to members of the public. In *Terry v. Canada (Minister of National Defence)*[15], the Federal Court was asked to determine whether documentation relating to military disciplinary proceedings became public upon being inadvertently shown to a member of the media. Rouleau J. decided that the inadvertent nature of the release, and the fact that only a single record was involved, prevented the disclosure from converting the confidential personal information at issue into public information.[16]

Finally, it should also be noted that personal information does not become publicly available merely by virtue of coming into the possession of a public body such as a government department.[17]

---

15 30 Admin. L.R. (2d) 122.

16 *Ibid*., p. 125.

17 *Canada (Information Commissioner), supra*.

PART 2 TECHNOLOGICAL CHANGE AND THE USE OF PUBLICLY AVAILABLE PERSONAL INFORMATION

2(i) The Impact of Technology

During the last quarter of the twentieth century, and particularly during the last decade, technological innovation has fundamentally altered the mode of delivery, accessibility and speed of acquisition of publicly available personal information. Theretofore, the limitations inherent in most forms of recorded information - available in a limited number of locales, at limited times during the course of the business day, suitable only for manual review and with few options for effective cross referencing - meant that the task of gathering detailed personal information about an individual through a comprehensive review of publicly available source materials was a labour, cost and time-intensive exercise.[18]

That approach to information gathering has been fundamentally impacted by the development of modern electronic technology. The introduction of computers to government records offices and the news media meant that a wide variety of official and unofficial records containing personal information began to be available in a digitized format after 1980. As the processing power and speed of computers increased at a seemingly exponential rate thereafter, computing functions that had previously been the exclusive preserve of large, and very expensive, mainframe computers became achievable on smaller "work stations", networked personal computers and, more recently, on "stand alone" personal computers. While these changes were occurring, the cost of processing and data storage was dropping precipitously due to new technology, improved production techniques and a very competitive marketplace. Advances in data compression meant that digitized information became increasingly portable; large data sets could now be readily transported by mail or courier in tape and diskette

---

[18] United States Federal Trade Commission, Bureau of Consumer Protection, "Individual Reference Services: A Federal Trade Commission Report to Congress", December 1997, p.2, online: http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm#Individual Reference Services.

formats. Corresponding improvements in database software meant that large volumes of information could now be sorted and compared, thereby permitting much more sophisticated analyses of, amongst other things, individual behaviour patterns.[19]

Perhaps the most striking development in data dissemination capability occurred during the 1990s with the explosive growth of the Internet. Information which, even if digitized, had formerly needed to be physically transported from one location to another was now capable of being almost instantaneously transmitted between widely separated sites. Corresponding developments in e-mail technology meant that data could be distributed to multiple recipients in a wide variety of places with a single transmission. Today, as personal computer usage and ownership becomes more pervasive, and as telecommunications technology is continually improved, our social and economic lives are increasingly affected by massive flows of electronic information.

With these advances in data collection, processing and retention has become such a widespread concern that such innovations are levying a heavy cost in terms of lost personal privacy. Traditional information gathering methods, although slower, more cost-intensive and with limited processing capacity, are remembered with a degree of fondness in privacy circles because their very technological limitations for generations sustained what has been termed "practical obscurity" - the measure of privacy afforded to individuals by public records that could not be accessed in anything other than a

---

[19] H. Jeff Smith, *Managing Privacy: Information Technology and Corporate America*. University Press, 1994; Suzanne M. Thompson, "The Digital Explosion Comes with a Cost: The Loss of Privacy," in *Journal of Technology Law & Policy*, vol. 4, issue 1, Spring 1999, pp. 1-5; Beth Givens, "Public Records in a Computerized Network Environment: Privacy Implications," a speech given to the Privacy Rights Clearinghouse First Amendment Coalition Conference, Oakland, CA, September 23, 1995, online: http://www.privacyrights.org/AR/speech1.htm, pp. 1-2; Privacy Commissioner of Canada, "Freedom of Information and Privacy," a speech delivered at the Freedom of Information and Privacy '99 conference, Edmonton, Alta., June 7 7 8, 1999, online: http://www.privcom.gc.ca/english/02_05_a_990607_e.htm, pp. 2-3.

piecemeal fashion.[20] In that era, even events that attracted sizeable amounts of public attention were gradually forgotten, due in large part to the transitory nature of major information sources such as newspapers, magazines and television. In such a setting, an individual whose personal information was disclosed to a wide audience, such as a convicted felon, could take comfort that his or her public notoriety would diminish over time - a process sometimes called the restoration of anonymity.

This comfortable state of affairs no longer exists. Information, once captured in any electronic medium, can now be retained indefinitely, can be accessed from literally any point on the globe and can be refined, repackaged and redistributed with a truly frightening degree of technical dexterity.[21] There is a revealing scene in the recent film *Notting Hill* in which the female lead, who plays a famous film star, is discovered by the *paparazzi* in somewhat compromising circumstances at the home of a male friend. Having retreated from a barrage of flash bulbs back into her friend's home, she rebuffs his efforts to comfort her by noting that today's news doesn't disappear, it is merely retained in its original form somewhere in storage, awaiting future use.

There are other information gatherers active in the marketplace today whose utilization of available public information engenders more disquiet amongst privacy advocates than does the excesses of the popular press. Technology has given rise to "data warehouses" - commercial enterprises whose lucrative business is centred upon acquiring vast stores of publicly available information for processing and resale. This business trend has been particularly apparent in the United States, where a technologically advanced marketplace and historically broad rights of access to public records have

---

20 Robert Gellman, "Public Registers and Privacy: Conflicts with other Values and Interests," a paper presented at the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, September 13, 1999, p. 7, online: http://www.pco.org.hk/conproceed.html.

21 B. H. Slane, New Zealand's Privacy Commissioner, "Bulk Release of Public Registers: A New Zealand Perspective," an address to the 20th International Conference of Data Protection Authorities, September 16-18, 1998, p. 2, online: http://www.knowledge-basket.co.nz/privacy/spubregf.html.

encouraged the development of the so-called "individual reference services."[22] One of the more prominent members of this new industry promoted its information processing capabilities in 1997 by revealing that one of its databases contained the *"...names, current and former addresses, Social Security numbers, and telephone numbers of 160 million individuals."*[23]

Individual reference services assemble electronic profiles of individuals or groups of individuals for their clientele. Depending upon the data sets available to them, and their own internal policies, they can create an impressively detailed dossier depicting an individual's basic identifiers (name, address, age, telephone number, etc.) together with a sizeable array of more detailed information (occupational, health, travel and criminal history, purchasing habits, licences held, marital status, etc.). Some services formerly provided have been affected by recent American laws. Limitations, for example, have been imposed on uses of drivers' records and credit reports.

These businesses could not thrive without advanced technology. The computational power necessary to continually sort through the transactional trails of hundreds of millions of data subjects was unavailable until quite recently. Now, however, vast and disparate streams of information can be brought together to produce an end product that is in many respects more than the sum of its parts. Noted privacy commentator Robert Gellman has described this phenomenon in the following terms:

> *Consider, for example, a CD-ROM that reproduces in one place an entire community's public register data. Using a GIS, the map could be produced that would identify each building in the city. Property tax records might provide the value, size, and floor plan of each house. Land*

---

[22] A 1998 news report indicated that there were then over 1,000 data warehouses operating in the United States: R. O'Harrow Jr., "Are Data Firms Getting Too Personal," March 8, 1998, *Washington Post* web site, online: http://washingtonpost.com/wp-srv/frompost/march98/privacy8.htm.

[23] FTC, "Individual Reference Services," *supra*.

> *ownership records would identify the owner and the purchase price. Motor vehicle records could be sorted to identify each driver living in the house, together with driving history and car ownership. Other public register information could easily be added, with vital statistics records likely to identify the names and ages of everyone living in the house, including children. If historical information were available as well, the resulting profile could trace the entry of a family into a community and the interactions of its members with most public institutions. The records might reflect changes in political party registration, new occupations (if they require licenses), school graduations, handgun ownership, and similar activities.*[24]

While such an aggregation of information may be viewed by some as being reasonably benign, there have been a considerable number of cases where the ready availability of personal information has had more serious consequences. Personal data from commercial sources has been used by disgruntled former spouses and celebrity stalkers to terrorize and even kill. Individuals have had their employment prospects seriously impaired by the revelation of past transgressions discovered through court or newspaper databases.

In such a changed environment, with the prospect for further technological breakthroughs seemingly around every corner, it is easy to understand why individuals, advocacy groups and governments around the world are increasingly concerned. As raw personal information is the grist for the new data mills, it is only natural that law makers in many countries have taken, or are currently contemplating, steps to regulate the flow of personal information in the private marketplace.

---

[24] Gellman, Robert. *Public Records: Access, Privacy, and Public Policy*. May 16, 1995. Online: http://www.cdt.org/privacy/pubrecs/pubrec.html.

2(ii) Public Policy Incentives to Permit Public Access to Government Information

As noted in section 1(ii) herein, the public in many western, industrialized nations has, over the course of this century, become accustomed to the availability of an ever increasing amount of detailed personal information about their fellow citizens.[25] This development has certainly been mirrored in Canada, where one of the largest sources of such information continues to be the myriad registries maintained by the federal, provincial and municipal levels of government.

These repositories vary in terms of the volume, nature and sensitivity of the information that they contain and in terms of the amount of access to personal information that is granted to the public. All of them share the common characteristic that such access as is permitted is the result of policy decisions made over the years. While the reasons for disclosing personal information from specific registries are not always explicitly stated in the framing statute or regulations, and while these reasons differ substantially from registry to registry, it is nonetheless possible to discern basic, recurring policy themes.

In the most general sense, the public is permitted access to specific forms of third party personal information held by government in order to advance objectives that are considered to be of importance to society. These objectives run the gamut from the reinforcement of democratic ideals and social equity through to consumer protection and public safety and on to the advancement of economic efficiency. When considered in more detail, as the examples briefly discussed below demonstrate, it becomes apparent that each such objective has merit.

Real Property Registers

---

[25] Beth Givens. *Public Records in a Computerized Network Environment: Privacy Implications*, a speech delivered to the Privacy Rights Clearinghouse First Amendment Coalition Conference, Oakland, CA, September 23, 1995. Online: http://www.privacyrights.org/ar/speech1.htm.

In Canada, one of the largest sources of publicly available third party personal information is contained in the various land title registration and real property tax assessment systems operated by provincial and municipal governments throughout the country. By consulting such registries, one can secure a wide variety of personal information, including: the identity and address of a property owner, the price paid for, and taxes levied against, a particular property, the amount of any mortgage placed upon the property and the identity of the mortgage holder. The provision of such information in a structured, objective and rule-centred manner, in turn, facilitates the operation of the real estate market, a vital sector of our economy.

The public availability of this sort of real property information has deep roots in Canada and elsewhere.[26] As noted by one American commentator:

> *Open ownership laws, bringing with them the citizen's right to review publicly recorded documents relating to the ownership, sale, transfer, and financing of real estate, have been an established part of government policy since the earliest days of our democracy...*[27]

Rationales for this ready access are varied. Traditionally, it has been believed that open realty records act as a defence against cronyism, self-dealing and other corrupt practices that might flourish if the

---

[26] By contrast, there is substantially less personal information contained in real property registers in England. See Davies, J.E. and Oppenheim, C. *Study of the Availability and Use of Personal Information in Public Registers: Final Report to the Office of the Data Protection Registrar.* Loughborough University: Department of Information Science, September 1999. Online: http://wood.ccta.gov.uk/dpr/dpdoc.nsf, paragraph 7.3.4.

[27] Real Estate Information Providers Association, Government Affairs Committee. *Principles of Government Sourced Data, Commercial Dissemination and Responsible Information Handling: An Industry Whitepaper*. January 11, 1997. Online: http://www.reipa.org/association/reports/reipacc1.html, p.2

system was closed to scrutiny.[28] Reasoned arguments can also be made that procedural transparency helps to protect the public from victimization by criminals: the real estate marketplace has long been a favoured milieu for fraud artists drawn by its size, anonymity and cash flows.[29]

In addition, governments have long recognized the economic benefits accruing to society from relatively unrestricted access to realty information. An Australian government official has recently pointed out that:

> *Current, complete and accurate land information can add economic value to the state by enabling dealings or investment decisions to be made earlier or project implementation to start more quickly, thus freeing up resources that are otherwise spent, for example, in paying interest on money borrowed or revenue foregone.*[30]

With the real estate sector of the economy undergoing continual evolutionary change, there are some grounds for concern that inhibiting the availability of reliable, timely and reasonably comprehensive information, including personal information, would exacerbate the illiquidity of the real estate market, hampering established practices while simultaneously threatening the viability of recent innovations, such as real estate securitizations, that are dependent upon full disclosure of relevant information.[31]

---

28 Information and Privacy Commissioner of British Columbia. *Investigation Report P98-011: An Investigation Concerning the Disclosure of Personal Information through Public Property Registries*. March 31, 1995, online: *http://www.oipcbc.org/investigations/reports/*invrpt11.html, p. 14-15; REIPA, *Principles of Government Sourced Data*, *supra*.

29 REIPA, *Principles of Government Sourced Data*, *supra*, p. 4.

30 O'Keefe, Elizabeth. *Electronic Service Delivery of Land Information - New Directions, New Issues*, a paper presented to the Institute of Public Administration Australia's National Conference, November 25-27, 1998. Online: http://www.ipaa.org.au/conference/papers/papers.htm., p.5.

31 REIPA, *Principles of Government Sourced Data*, *supra*, p. 3.

Court Records

The right of public access to court proceedings and records has a long history in English jurisprudence, having been recognized as early as the fourteenth century.[32] This common law entitlement, although subject to a variety of qualifications in Canada[33] and abroad, [34] continues to reflect the generally held policy perspective that public access to the court process is a cornerstone of Western democracy. By encouraging public oversight, it is believed, fairness is enhanced and citizens develop greater confidence in the judiciary.[35] Given the judiciary's vital role as arbiter in criminal and civil proceedings, such enhanced confidence, in turn, buttresses the legitimacy of the state as a whole and serves an important social control function. In speaking of the criminal law process in the United States, Burger C.J. of the United States Supreme Court stated:

> *When a shocking crime occurs, a community reaction of outrage and public protest often follows. . . . Thereafter the open processes of justice serve an important prophylactic purpose, providing an outlet for community concern, hostility, and emotion. Without an awareness that society's responses to criminal conduct are underway, natural human reactions of outrage and protest are*

---

32 *Vickery v. Nova Scotia Supreme Court (Prothonotary)*, [1991] 1 S.C.R. 671 at 681, Cory, J. (dissenting).

33 Ibid., at p. 678, Stevenson J.

34 Office of the Judges Programs of the Administrative Office of the United States Courts. *Privacy and Access to Electronic Case Files in the Federal Courts*. December 15, 1999. Online: http://www.uscourts.gov/privacyn.htm; European Commission, Data Protection Working Party. *Opinion No. 3/99 on Public Sector Information and the Protection of Personal Data*. May 3, 1999. Online: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp20en.htm at p. 5.

35 Gellman, Robert. *Public Records: Access, Privacy, and Public Policy*. May 16, 1995. Online: http://www.cdt.org/privacy/pubrecs/pubrec.html.

frustrated and may manifest themselves in some form of vengeful "self-help," . . .

The crucial prophylactic aspects of the administration of justice cannot function in the dark; no community catharsis can occur if justice is "done in a corner [or] in any covert manner." . . . It is not enough to say that results alone will satiate the natural community desire for "satisfaction." A result considered untoward may undermine public confidence, and where the trial has been concealed from public view an unexpected outcome can cause a reaction that the system at best has failed and at worst has been corrupted. To work effectively, it is important that society's criminal process "satisfy the appearance of justice," . . . .[36]

Access to information about court proceedings involving certain specific categories of private citizens is also widely endorsed on public policy grounds. Many jurisdictions have now enacted sexual predator legislation designed to authorize the dissemination of details about the criminal records of certain released sex offenders and those offenders' whereabouts in an effort to protect members of the community who might be at risk if those individuals were to re-offend.[37] These legislative efforts tend to meet with public approval; surveys have revealed that *"...most are willing to give up some privacy protection if the trade-off results in a benefit to the public, such as increased safety,*

---

36 *Richmond Newspapers, Inc. v. Virginia*, 448 U.S. 555 (1980) at pp. 571-73.

37 Solicitor General of Canada, *Report to Federal, Provincial and Territorial Ministers on Information Systems on Sex Offenders against Children and Other Vulnerable Groups* by the Federal, Provincial and Territorial Working Group on High Risk Offenders. Ottawa: 1998, online: http://www.sgc.gc.ca/epub/corr/e199810d/e199810d.htm; M. Burns, *Do Sexual Predators have the Right to Privacy?: Confidentiality Provisions for Registered Sex Offenders in California and Massachusetts*, 1999, online: http://www.cs.cmu.edu/~burnsm/SOR.html.

crime prevention or the protection of children."[38] Similarly, other commentators have noted the public's willingness to accept the abridgement of the privacy of politicians when criminal history information is involved; here again an impulse towards the enhancement of public safety appears to be stronger than support for personal privacy.[39]

Electoral Records

The public availability of a variety of personal information concerning individuals involved in the electoral process is also a time-honoured practice in many jurisdictions.[40] For example, most democracies make public, to varying degrees, the personal information compiled in the electoral roll.[41] New Zealand's Privacy Commissioner has succinctly noted that the electoral roll *"...is used to ensure that on election day only eligible people vote, that their votes are counted in the correct electorate, and that each elector votes only once each for a candidate and a party."*[42] It is plain that the attainment of the aforementioned objectives is vital to the functioning of the democratic process; the publication of the information thus collected is intended, like the publication of court records, to permit citizens to satisfy themselves that the electoral process is fair.

---

38 T.D. Ellard, "Privacy, Technology and Criminal Justice Information: Public Attitudes towards Uses of Criminal History Information", National Conference on Privacy, Technology and Criminal Justice Information, Washington, D.C., May 31, 2000 [unpublished].

39 E. Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You," Working Paper # 14, The Independent Institute, Oakland, CA, December, 1999, online: http://www.independent.org/tii/WorkingPapers/InfoPrivacy.pdf, at p. 29.

40 European Commission, *Opinion No. 3/99*, *supra*., p. 6

41 Gellman, "Public Records: Access, Privacy, and Public Policy", *supra*., p. 23.

42 Privacy Commissioner of New Zealand, "Report by the Privacy Commissioner to the Minister of Justice on the Electoral Act 1993", April 29, 1997, p. 2, online: http://www.knowledge-basket.co.nz/privacy/top.html.

It is the desire to prevent the tainting of the democratic process that also underlies campaign contributions legislation. As noted by the Western Australia Commission on Government in a 1995 Discussion Paper on campaign contributions law and policy:

> *Supporters of disclosure say that it deters attempts by parties, politicians and other participants in the electoral process to trade preferential treatment for election funds. Donations that are not made public have the potential to corrupt the political process. Full disclosure is one way of reducing this potential and enhancing public confidence in the political process by informing voters about who is financing a political party. Disclosure ensures public knowledge and enables the public, and therefore voters, to determine the propriety of donations which might have the potential, because of their size, to influence a decision of a member of parliament.*[43]

In each of the categories of government information canvassed above, the policy incentives for the release of certain forms of personal information to the public are quite strong. There is, however, an inherent tension between the policy objectives that prompt such releases of information and the potentially incompatible policy goal of safeguarding the privacy of citizens. Confronted with this friction, policy makers must attempt to attain a balance between these objectives that maximizes the public benefit. Given the widely ranging, and often fervently held, viewpoints of members of the public on the proper relationship between access to government information and privacy, this balancing act poses substantial challenges.

---

[43] "Discussion Paper No. 7", online: http://www.wa.gov.au/cog/discussion/dis7.html.

PART 3 INTERNATIONAL RESPONSES TO THE PUBLICLY AVAILABLE PERSONAL INFORMATION DILEMMA

The dilemma of how to deal with the use of publicly available information in a balanced manner that will properly support both access to information principles and the rights of inhabitants to privacy is not unique to Canada. This same debate has taken place in other Western democracies, with varying results.

Europe

The current international flurry of private sector privacy law developments owes much of its vigour to the data protection leadership role taken by the European Union ("EU"). The new or amended privacy/data protection laws in place in EU member states that were promulgated during the last five years, and private sector privacy legislation now in place or under development in Canada, all reflect the influence of a single directive jointly issued by the European Parliament and the Council of the EU. That instrument is the *"Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data"*[44] (the European Directive").

The European Directive outlined the requirements for data protection laws to be put in place by EU member states. In doing so, it did not comprehensively address the treatment to be accorded to publicly available information by state privacy regulators. However, it did stipulate the need for controls governing the processing and international transmission of personal information contained in publicly accessible registers, while simultaneously recognizing the right of member states to apply the

---

[44] *Official Journal* L 281, November 23, 1995, pp. 0031-0050, online: http://europa.eu.int/eur-lex/en/lif/dat/1995/en_395L0046.html.

principle of public access to official documents when framing their resulting data protection laws.[45]

There are two provisions in the European Directive that are particularly relevant to our discussion. The first is found in Article 18, which establishes the need for controllers of personal data to notify the public authority in their respective states that is responsible for the administration of that state's data protection laws before undertaking wholly or partially automated processing of personal data. Subarticle 18.3 contemplates an exemption from the notification being granted by member state legislation with respect to:

> *...processing whose sole purpose is the keeping of a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person demonstrating a legitimate interest.*[46]

The second relevant provision is found in Article 26, which limits the right of member states to transfer personal information to third party countries that lack adequate personal data safeguards. Subarticle 26.1(f) provides that a transfer of personal data can take place to such a state if:

> *...the transfer is made from a register which according to laws or regulations is intended to provide information to the public and which is open to consultation either by the public in general or by any person who can demonstrate legitimate interest, to the extent that the conditions laid down in law for consultation are fulfilled in the particular case.*

---

45 *Ibid*., recital 72.

46 A corresponding exemption from the obligation to provide notice to the public concerning processing found in subarticle 21.3 flows naturally from the exemption from notification of the public authority contained in subarticle 18.3.

In response to concerns that the European Directive did not adequately address concerns pertaining to publicly available information, the European Commission's Data Protection Working Party (the "Working Party") produced and adopted its "Opinion N° 3/99 on Public Sector Information and the Protection of Personal Data"[47] on May 3, 1999. The Working Party took an unambiguous stance on the issue of whether the Directive, and member state legislation made in response to it, addresses personal information:

> *It is perfectly clear from the wording of our data protection legislation that it applies to personal data made publicly available: even after personal data are made public, they are still personal and must therefore be protected.*[48]

Having examined the exemptions discussed above in subarticles 18.3 and 26.1(f), the Working Party went on to note:

> *It is clear...that personal data protection considerations should not be used to prevent citizens from accessing administrative documents under conditions laid down in national legislation. However, the Directive is not intended to remove all protection from publicly-accessible data either.*[49]

Citing the overarching principle that personal data must be collected for specific, explicit and legitimate purposes and must not subsequently be processed in a manner contrary to that principle, the Working Party opined that member states should construe collections, uses and disclosures of public information

---

47 Online: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp20en.htm.

48 *Ibid.*, p. 3.

49 *Ibid.*, p. 4.

on a case by case basis under their national laws to ensure compliance. It also spoke of the need to achieve a balance between public access and privacy protection, and provided examples of how this balance is being achieved under the national legislation of member states. Amongst these innovations:

- In Germany, portions of the personal information required to be provided by electoral candidates for inclusion in the list of candidates is removed before the data is made public.[50]

- In France, birth certificate information is only available to those who can cite the name, date and place of birth of the individual in respect of whom information is being sought.[51] Land registration information is generally available, but may not be used commercially.[52] Searches of electronic telephone directories using the first few letters of a name to compile a list of matching subscribers is no longer permitted.[53] Electoral lists may not be published on the Internet and may not be used commercially.[54] Lists of naturalized persons are not published on the Internet.[55]

- In Belgium, databases of court decisions may not be indexed by name, thereby inhibiting name-based searching.[56] Italy has contemplated going one step

---

50 *Ibid.*, p. 6.

51 *Ibid.*, p. 7.

52 *Ibid.*, p. 6.

53 *Ibid.*, p. 7.

54 *Ibid.*, p. 6.

55 *Ibid.*, p. 5.

56 *Ibid.*

further and is considering giving its citizens the right to "opt out" of having their name appear in a case law database.[57]

- In Greece, prospective land registry users must demonstrate their legitimate interest in acquiring information contained in the registry and cannot search land records by name of landowner.[58]

The Working Party also noted that the European Directive imposes additional constraints if publicly available information is to be used in a commercial manner. Citing Principle 11, the Working Group stated:

> *Directive 95/46/EC recognises the right of data subjects to be informed about the processing of data concerning them and stipulates that at the very least they have the right to object to legitimate processing. Data subjects must therefore be informed about the commercial usage of data concerning them and must be able to object to such usage by simple and effective means.*[59]

United States

Unlike Canada or New Zealand, the United States has so far resisted calls for the implementation of comprehensive privacy legislation aimed at the private sector. Instead, both the federal and state governments have encouraged industry self-regulation while simultaneously developing single issue or sectoral legislation aimed at the most acute areas of privacy-related concern.

---

57 *Ibid.*

58 *Ibid.*, p. 6.

59 *Ibid.*, p. 8.

As the government oversight rationale for access to information law strikes a particularly resonant chord in American political culture, proposals to limit access to public registers in order to enhance privacy have proven controversial. In a similar vein, the notion of limiting the collection, use and disclosure of publicly available personal information has not found favour with those commentators who view it as a thinly disguised attack on cherished First Amendment principles.[60]

Nevertheless, there are instances in which legislation has been implemented in the United States for the express purpose of limiting public access to otherwise publicly available information. One of the best known examples of this sort of legislation is the *Driver's Privacy Protection Act of 1994* (18 U.S.C. 2721-2725) (the "DPPA"). Inspired by the murder of a young actress at the hands of a deranged fan who had obtained her home address from motor vehicle records, this federal law limits the right of state motor vehicle authorities to release personal information contained in their records to third parties. The DPPA contains a sizeable number of exemptions, including two exemptions permitting (a) disclosure of individual records upon request and (b) bulk disclosures for survey, marketing and solicitation purposes if the relevant state authority has put in place methods and procedures to permit individuals to opt to prohibit such disclosures of their personal information.[61]

The DPPA has been criticized in various quarters. Its constitutionality, challenged by a number of states, was ultimately upheld by a recent decision of the United States Supreme Court.[62] Other commentators, including the American Civil Liberties Union, while supporting the DPPA's general

---

60 E. Volokh, "Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People From Speaking About You," Working Paper # 14, The Independent Institute, Oakland, CA, December, 1999, online: http://www.independent.org/tii/WorkingPapers/InfoPrivacy.pdf.

61 Subsections 2721(B)(11) and (12).

62 Linda Greenhouse, "Justices Uphold Ban on States' Sales of Drivers' Licence Information," *The New York Times on the Web*, January 13, 2000, online: http://st7.yahoo.com/lib/retrace/nytimes011300driverbanupheld.htm.

policy objectives have complained about the breadth of the exemptions it affords.[63]

A more broadly based treatment of the privacy considerations affecting publicly available personal information is found in the *Gramm-Leach-Bliley Act* (Pub. L. 106-102) (the "GLB Act"), which was signed into law on November 12, 1999. Subtitle A of title V of the GLB Act restricts the entitlement of certain financial institutions to disclose "nonpublic personal information" of consumers to non-affiliated third parties. The GLB Act, by implication, excludes from its ambit any "publicly available information," except where that information is combined in a "*...list, description or other grouping of consumers...*" with an item or items of nonpublic personal information.[64]

The GLB Act does not define "publicly available information." However, federal regulators were directed by the GLB Act to create a definition of "publicly available information" by regulation.[65] As the GLB Act applies to a group of federal regulatory authorities, the resulting definition is common to a series of regulations and regulatory authorities.[66] Using the Office of the Comptroller of the Currency as an example, new regulatory provisions dealing with privacy have resulted which have been added as Part 40 to Chapter I of title 12 of the *Code of Federal Regulations*.

Pursuant to paragraph 40.3(p)(1), "publicly available information" is defined to mean:

> *...any information that a bank has a reasonable basis to believe is lawfully made*

---

63 Gregory T. Nojeim, Legislative Counsel, American Civil Liberties Union, "Statement on Drivers' Privacy And Amendments to the Driver's Privacy Protection Act Before The Senate Appropriations Committee Subcommittee on Transportation", April 4, 2000, online: http://www.senate.gov/~appropriations/transportation/testimony/nojeim.htm.

64 GLB Act, subsection 509(4).

65 *Ibid.*

66 *Ibid.*, section 504.

available to the general public from:

(i) Federal, State, or local government records;

(ii) Widely distributed media; or

(iii) Disclosures to the general public that are required to be made by Federal, State, or local law.

The regulation states that a bank will have a reasonable basis for believing that information has been lawfully made available to the general public (with the result that the bank could make free use of the personal information) if the bank has taken steps to confirm that (a) the information is of the sort that is available to the general public and (b) to the extent that the individual enjoyed a right to refuse to have the information disclosed to the general public, that the individual has not exercised that right.[67] Using more detailed examples, the regulation provides that a bank would reasonably believe mortgage information to be lawfully made available to the general public if the bank had determined that the information was of a sort placed on the public record in the jurisdiction where the mortgage was registered. Similarly, a bank would reasonably view an individual's telephone number as being publicly available if the phone number is listed in a telephone book or the individual has advised the bank that his or her telephone number is not unlisted.[68]

The regulation defines publicly available information in a way that encompasses government records, including real estate records and security interest filings. It also defines "widely available media" to include "*...information from a telephone book, a television or radio program, a newspaper, or a web site that is available to the general public on an unrestricted basis.*"[69]

---

67 *Code of Federal Regulations*, Chapter I , Title 12, Part 40, paragraph 40(3)(p)(2).

68 Subparagraphs 40(3)(p)(3)(A) and (B).

69 Subparagraphs 40(3)(p)(3)(i) and (ii). The regulation notes that a web site is not restricted merely because access to the site requires a password or the payment of a fee, so long as access is available to the public generally.

It is interesting to note that the regulatory authorities that designed the aforementioned regulations sought input from the public when drafting the definition of "publicly available information." Two alternatives were put forward; one would have deemed information to be publicly available only if the financial institution obtained it directly from a publicly available source, the other alternative expanded the parameters of the first by including information gathered about a consumer by any means if that information was also available from a public source.[70] Comments in favour of each of the alternatives were received, with advocates of the first noting that it enhanced the privacy protection afforded to consumers while advocates of the latter alternative stressed that it would avoid needless administrative complexity without compromising privacy.[71] Ultimately, the drafters opted for a hybrid approach to the definition; financial institutions are required to have a reasonable basis for believing that information is publicly available. To attain this reasonableness standard, however, financial institutions must determine whether the information at issue is the sort that is made available to the public and, if it is, may treat the information as publicly available only if the consumer has not exercised a right to withhold that information from disclosure.

New Zealand

New Zealand has been an innovative force in the realm of legislated privacy protection, having implemented private sector controls on the use of personal information as early as 1993. The *Privacy Act 1993*[72] (the "New Zealand Act") applies to both the public and private sectors.

---

70 Department of the Treasury, et al., "Privacy of Consumer Financial Information; Final Rule," *Federal Register*: June 1, 2000 (vol. 65, no. 106), p. 35170, online: http://mbaa.org/resident/lib2000/65fr35161.html.

71 *Ibid.*

72 Online: http://www.knowledge-basket.co.nz/privacy/recept/rectop.html. Amended by the *Privacy Amendment Act 1993* and the *Privacy Amendment Act 1994*.

The New Zealand Act exempts "publicly available information" from the restrictions otherwise imposed by it on the collection, use or disclosure of personal information. "Publicly available information" is defined in subsection 2(1) to mean *"...personal information that is contained in a publicly available publication."* "Publicly available publication" is defined, in turn, in the same subsection to mean: *"...a magazine, book, newspaper, or other publication that is or will be generally available to members of the public; and includes a public register."* An "Agency" (a term that is defined in subsection 2(1) to include: *"...any person or body of persons, whether corporate or unincorporate, and whether in the public sector or the private sector..."*) is authorized to collect publicly available information in an indirect manner,[73] to use it for one or for many purposes at the agency's discretion[74] and to freely disclose such information to third parties.[75]

While an item of personal information contained in a public register is by definition both a publicly available publication and publicly available information, Part VII of the New Zealand Act establishes qualified rules to control collection, use and disclosure of public register information. Public registers are defined to mean *"...any register, roll, list or other document..."* maintained pursuant to legislative requirements itemized in the Second Schedule to the New Zealand Act.[76] Section 59 establishes four public register privacy principles, which are:

> *<u>PRINCIPLE 1</u> (Search References)*
>
> *Personal information shall be made available from a public register only by*

---

73 Section 6, Principle 2(2)(a).

74 Section 6, Principle 10(a).

75 Section 6, Principle 11(b).

76 Section 58. The listing in the Second Schedule applies to such typically large sources of personal information as the land registry and land assessment systems, electoral and motor vehicle registers, the companies registry and to insolvency, marriage and births/deaths records.

search references that are consistent with the manner in which the register is indexed or organised.

PRINCIPLE 2 (Use of information from public registers)

Personal information obtained from a public register shall not be re-sorted, or combined with personal information obtained from any other public register, for the purpose of making available for valuable consideration personal information assembled in a form in which that personal information could not be obtained directly from the register.

PRINCIPLE 3 (Electronic transmission of personal information from register)

Personal information in a public register shall not be made available by means of electronic transmission, unless the purpose of the transmission is to make the information available to a member of the public who wishes to search the register.

PRINCIPLE 4 (Charging for access to public register)

Personal information shall be made available from a public register for no charge or for no more than a reasonable charge.

The New Zealand Act does not purport to make the statutory duties of those agencies operating public registers subordinate to privacy considerations. Rather, such agencies are required to comply with the information privacy principles and the public register privacy principles established by the New Zealand

Act to the greatest extent possible, subject, however, to their primary legislative mandate.[77] Any person who obtains personal information from a public register, meanwhile, must not, *"...so far as is reasonably practicable..."* re-sort that information, or combine it with personal information obtained from another public register, for the purposes of transferring that information in its re-sorted or combined form to a third party for valuable consideration.[78]

In furtherance of the public register privacy principles, the Privacy Commissioner is given reasonably broad advisory and investigative powers. In response to a complaint registered with his Office or on his own initiative, the Privacy Commissioner can make an inquiry into the privacy impact of any public register provision listed in the Second Schedule to the New Zealand Act.[79] If such an inquiry is carried out, the Commissioner must report his findings and recommendations to the Minister responsible for the register at issue.[80] As well, the Commissioner may undertake an investigation to determine (a) whether any agency responsible for a register is failing to comply with the information privacy principles or the public register privacy principles or (b) any person is failing to comply with Principle 2 of the public register privacy principles.[81] In either case, the Commissioner is obliged to report his findings to the party whose practices were under investigation.[82] It is noteworthy that the Commissioner is obliged to report to the appropriate authority any evidence of misconduct or breach of duty on the part of any agency or any officer or employee or member of an agency discovered during such an

---

77 Section 60. It should be noted that subsection 7(6) of the New Zealand Act states: *"Subject to the provisions of Part VII of this Act, nothing in any of the information privacy principles shall apply in respect of a public register."*

78 Subsection 60(2).

79 Subsection 61(1).

80 Subsections 61(2).

81 Subsections 61(3).

82 Subsection 61(4).

investigation.[83]

In recognition of the varying natures of the public registers established by legislation, the Privacy Commissioner is empowered to customize the impact of the New Zealand Act on specific public registers by issuing codes of practice. Such codes of practice can impose privacy protection requirements that are more or less stringent than the public register privacy principles, even to the extent of exempting a register from compliance with one or more of those principles.[84] Such codes can also establish the manner in which an agency operating a register shall carry out its mandate to comply with the public register privacy principles.[85]

The New Zealand Act also obliges the Privacy Commissioner to monitor compliance with the public register privacy principles and to periodically review the principles, *"...with particular regard to the Council of Europe Recommendations on Communication to Third Parties of Personal Data Held by Public Bodies (Recommendation R (91) 10)..."* [86] To the extent that this review reveals a need for changes, the Commissioner is expected to report his findings to the responsible Minister.

In reviewing the public register provisions in the New Zealand Act, New Zealand's Privacy Commissioner has noted that the provisions represent a compromise between privacy concerns and the public need for access to certain forms of government controlled third party personal information.[87] The Privacy Commissioner has also acknowledged that the regime established by the New Zealand

---

83 Subsection 61(5) and section 80.

84 Subsection 63(2).

85 Paragraph 63(2)(c).

86 Paragraph 13(1)(3).

87 Office of the Privacy Commissioner, "Discussion Paper No. 5 - Public Register Privacy Issues,"online: http://www.knowledge-basket.co.nz/privacy/spubregf.html, pp. 3-4.

Act cannot prevent all privacy abuses involving public register-derived information from occurring.[88] With an eye towards addressing these problems, the Privacy Commissioner has recommended that the New Zealand Act be modified by further limiting third party access for purposes other than those that accord with the purpose for which the register was maintained.[89]

Australia

Federal

The Commonwealth of Australia, like Canada, is a federation in which constitutional powers are divided between (a) the federal, or "Commonwealth", government and (b) the governments of six states and two territories. As in other Western nations, Australian legislative initiatives aimed at regulating the use of personal information by the private sector are a relatively recent phenomenon. On April 12, 2000 the Commonwealth government introduced the *Privacy Amendment (Private Sector) Bill 2000* (the "Amendment Bill")[90] for First Reading in the House of Representatives. The Amendment Bill, if passed, would amend the *Privacy Act, 1988* (the "1988 Act")[91], by extending limitations previously applicable to the collection, use and disclosure of personal information by federal agencies (and to private sector dealings with credit and tax information) to the private sector generally. The Amendment Bill will come into effect on the later of July 1, 2001 or the first anniversary of its passage into law.

---

88 Office of the Privacy Commissioner, "Highlights from the Report of the Privacy Commissioner on the First Periodic Review of the Operation of the Privacy Act 1993", Section 3, "Public Registers, Direct Marketing and Unrelated Uses," December 1998, online:http://www.knowledge-basket.co.nz/privacy/recept/rectop.html.

89 *Ibid.*

90 Online: http://www.aph.gov.au/legis.htm.

91 Online: http://www.privacy.gov.au/act.

The Amendment Bill implements the National Principles for the Fair Handling of Personal Information (the "National Principles")[92] developed by Australia's Privacy Commissioner. These National Principles were intended to provide a framework around which businesses could voluntarily construct effective privacy codes and policies. However, with public concerns mounting about the use of personal information by business, and having received strong signals from the European Union that maintaining the status quo on privacy in Australia would invite the imposition of data flow restrictions, Australia has opted to abandon the self-regulatory model at the federal level in favour of the "co-regulatory" approach.[93] Co-regulation involves the establishment of the National Principles as the baseline for privacy; a business will be bound by the National Principles unless it obtains approval from the Privacy Commissioner for its own code. Such approval will only be available if the individual policy affords privacy protection that is at least equivalent to the protection afforded by the National Principles as presented in the Amendment Bill.

Somewhat surprisingly, the issue of publicly available information is not dealt with directly in the Amendment Bill, the 1988 Act or the National Principles. No attempt is made to regulate private sector use of public registers.[94] Instead, it is noteworthy that the definition of *"record"* in subsection 6(1) of the 1988 Act specifically excludes any *"generally available publication."* *"Generally available publication"*, in turn, is defined to mean *"...a magazine, book, newspaper or other publication that is or will be generally available to member of the public."* The Amendment Bill proposes to amend the definition of "generally available publication" in subsection 6(1) of the 1988 Act by adding the phrase *"...(however published)..."* immediately following the term *"...publication..."*.

---

92 Online: http://www.privacy.gov.au/publications/index.html.

93 Parliament of Australia, House of Representatives, *Privacy Amendment (Private Sector) Bill 2000: Explanatory Memorandum*, 2000, online: (http://www.aph.gov.au/hansard/hansreps.htm).

94 Parliament of Australia, Parliamentary Library, *Bills Digest No. 193 1999-2000*, Online: http://www.aph.gov.au/library/pubs/bd/1999-2000/2000bd193.htm.

Also of note is the proposed wording of subsection 16B(2) of the Amendment Act, which would make it plain that the 1988 Act, as amended, would in large part apply only to personal information contained in a "record".

The 1988 Act, if modified in the manner contemplated by the Amendment Bill, will continue to provide private sector organizations with significant latitude when dealing with publicly available information. One of Australia's (and the world's) foremost privacy experts has noted that certain significant repositories of personal information may fall within the ambit of "generally available publication", including:

> *...the electoral register (which is available for purchase); but possibly also births, deaths, marriages and driver licensing registers in the Territories, which are not purchasable in whole, but are publicly accessible; the telephone books, both those published by Telecom, and extracts from them; and publicly purchasable mailing lists (including those from Telecom).*[95]

The fact that this broad exemption has been maintained, and perhaps even broadened, in the Amendment Bill has prompted warnings from academic commentators about its impact on the privacy rights of Australians.[96]

Australian State and Territories

---

95 Roger Clarke, "The Australian Privacy Act 1988 as an Implementation of the OECD Data Protection Guidelines," June, 1989, online: http://www.anu.edu.au/people/Roger.Clarke/DV/PActOECD.html, p. 7.

96 Graham Greenleaf, Professor of Law, University of New South Wales, "Privacy Amendment (Private Sector) Bill 2000: Working Notes used in preparation of a Submission to the House of Representatives Standing Committee on Legal and Constitutional Affairs," May 14, 2000, online: http://www2.austlii.edu.au/~graham/CyberLRes/2000/5, p. 10.

Currently no Australian state or territory government has implemented privacy legislation directed at the private sector. However, at least two states, New South Wales and Victoria, have sought to moderate the privacy consequences of private sector access to personal information contained in public registers. The *Privacy and Personal Information Protection Act 1998*,[97] (the "NSW Act"), which came into force on July 1, 2000, deals with public registers in Part 6. Section 57 of the NSW Act prohibits the release of personal information by a public sector agency responsible for maintaining a public register[98] unless that agency is satisfied that the transferee will use the personal information in a manner that accords with the purposes of the governing legislation. In order to meet its obligation to screen transferees in this manner, the NSW Act contemplates the public sector agency requiring third party data requesters to execute a statutory declaration specifying their intended uses of the personal information.[99]

The NSW Act also permits individuals whose personal information is slated for inclusion in a public register to request that the information be removed from or not placed on the public register in a publicly available form and to further request that the information not be disclosed to the public.[100] If the public sector agency is satisfied that the safety or well-being of the individual would be affected if the information was not suppressed in the manner requested, the agency is placed under a positive obligation to see that the individual's wishes are respected, except in circumstances where the agency believes that the public interest in maintaining access to the information outweighs the individual's needs.[101] Information that is designated as non-public as the result of a request can nonetheless remain

---

97 Online: http://www.lawlink.nsw.gov.au/pc.nsf/pages/generalinfo.

98 Public register is defined in section 3 of the NSW Act to mean: *"...a register of personal information that is required by law to be, or is made, publicly available or open to public inspection (whether or not on payment of a fee)."*

99 Subsection 57(2).

100 Subsection 58(1).

101 Subsection 58(2).

on the register for other purposes.[102]

To ensure that the privacy rights thus afforded by Part 6 of the NSW Act are upheld, section 59 specifies that the provisions of Part 6 shall prevail over any inconsistent provisions in the legislation under which the public register was established.

It is noteworthy that the safeguards afforded to personal information by the NSW Act do not extend to published personal information. The definition of "personal information" in section 4 specifically excludes *"...information about an individual that is contained in a publicly available publication."*[103]

The public register provisions in Part 6 of the NSW Act are not applicable to land registry and property assessment records by virtue of section 5 of the *Privacy and Personal Information Protection Regulation 2000*.[104] In addition, a Privacy Code of Practice has been approved under Part 3 Division 1 of the NSW Act in respect of local government personal information holdings that has the effect of easing the privacy constraints in Part 6 in order to facilitate oversight of local government activities by members of the public.[105]

Quite recently, the state of Victoria has also initiated public sector privacy legislation. *The Information Privacy Act 2000*[106] (the "Victoria Act") was introduced in the Victoria Assembly on May 24, 2000.

---

102 Subsection 58(3).

103 Paragraph 4(3)(b). Publicly available publication is defined negatively in section 3 to exclude *"...any publication or document declared by the regulations not to be a publicly available document for the purposes of this Act.*

104 Online: http://www.austlii.edu.au/au/legis/nsw/consol_reg/papipr2000555.

105 Online: http://www.lawlink.nsw.gov.au/pc.nsf/pages/locgovtcode.

106 Online: http://www.dms.dpc.vic.gov.au/pdocs/bills/B00596/B00596I.html.

Like the NSW Act, the Victoria Act contains language limiting third party access to personal information contained in public registers. Subsection 16(4) obliges public sector agencies or Councils to treat such information, as much as possible, as though it was entitled to the safeguards afforded by the Information Privacy Principles appended as Schedule 1 to the Victoria Act. Unlike the NSW Act, the Victoria Act does not accord the subsection 16(4) requirement any special status; rather, the provisions of the Victoria Act are expressly subordinate to the provisions of any other Act.[107] The ambit of the Victoria Act is further limited by section 11, which specifies that a record containing personal information is not affected by that legislation if, amongst other things, it is a generally available publication[108] or if it is: *"...a public record under the control of the Keeper of Public Records that is available for public inspection in accordance with the Public Records Act 1973."*[109]

---

107 Subsection 6(1).

108 Paragraph 11(1)(a). "Generally available publication is defined in section 3 to mean "...a publication (whether in paper or electronic form) that is generally available to members of the public and includes information held on a public register."

109 Paragraph 11(1)(c).

PART 4 COMMENTARIES AND POLICY RESPONSES

Legislative changes, as described in Part 3, have been prompted in part by research conducted by, and advice received from, a core group of academics, administrative officials and privacy consultants located throughout the world. While this group does not share a common perspective on all matters relating to privacy matters, they have, as a collectivity, produced many valuable recommendations concerning the public information issue.

In some cases these insights have been delivered as part of administrative proceedings. During the course of an investigation into the manner in which property assessment information was being disclosed to the public by the City of Victoria, the Information and Privacy Commissioner of British Columbia (the "B.C. Commissioner") had occasion to consider the policy implications of permitting otherwise publicly available registry information to be conveyed to a potentially vast audience via the Internet.[110] In carrying out his analysis, he was confronted with a very startling statistic: on its first day of operation the assessment information web site was visited more than 15,000 times, a massive utilization when contrasted to the average of twenty-five to thirty information calls that Victoria's land assessment office had received theretofore.[111]

In his resulting report, the B.C. Commissioner acknowledged that the scheme enhanced operational efficiency and service delivery while simultaneously advancing the democratic ideal of administrative transparency - rate payers could now satisfy themselves that they were being taxed in an equitable manner relative to their neighbours without imposing an administrative burden on limited municipal resources. However, he also observed that the virtues of the new mode of information delivery were

---

110 Information and Privacy Commissioner of British Columbia. *Investigation Report P98-011: An Investigation Concerning the Disclosure of Personal Information through Public Property Registries*. March 31, 1995, online: http://www.oipcbc.org/investigations/reports/invrpt11.html.

111 *Ibid*., p. 1.

counterbalanced by some disturbing privacy implications. He noted:

> *There is a widely-held assumption that information in such "public" registers need not be protected at all, or that only very limited protections are needed. It is this Office's position that public records pose a challenge to the privacy rights of citizens and, once in digital format, pose an even greater challenge to those privacy rights. Digital technology fundamentally changes the nature of public records as the paper record decomposes and becomes discrete pieces of information that can be searched, manipulated and reconfigured in ways that may improve efficiencies but were never intended by the legislature.*
>
> *In short, from a privacy perspective, information which is "public" information is vulnerable to misuse, particularly when the information is provided in an electronic format. One of the goals of the Freedom of Information and Protection of Privacy Act is to limit the collection, use and disclosure of personal information by public bodies. The Act presumes that personal information, for example, your name and address, will be collected and used by public bodies for a specific purpose, and disclosed only in limited circumstances, as permitted by law, for the original purpose, or for a purpose consistent with the purpose for which it was obtained.*[112]

This concern about public information, particularly government records, being used in a manner at odds with both the interests of affected data subjects and the original purposes for which the information was

---

[112] *Ibid.*, p. 2.

compiled - what Australian privacy expert Roger Clarke has termed "function creep"[113] - echoes misgivings expressed by other privacy regulators and commentators around the world. The European Commission's Green Paper on public sector information warns: "*The emergence of the Information society could pose new risks for the privacy of the individual if public registers become accessible in electronic format (in particular on-line and on the Internet) and in large quantities.*"[114] The President of France's National Data Processing and Liberties Commission shares this sentiment.[115] New Zealand's Privacy Commissioner, meanwhile, has opined: "*The bulk release of public register information has little to do with effective participation, accountability or good government.*"[116]

While a broad consensus thus exists concerning the general diminution of privacy arising from electronically enhanced access to public information, the specific harms identified by commentators around the world as being associated with that phenomenon are as varied as the information sources themselves. Some of the more noteworthy include:

- disclosure of information that may result in a third party harming the data subject, such as the

---

113 Roger Clarke, "Privacy and 'Public Registers'," Text of an Address to the IIR Conference on Data Protection and Privacy, Sydney, Australia, May 12-13, 1997, p. 5, online: http://www.anu.edu.au/people/Roger.Clarke/DV/PublicRegisters.html.

114 European Commission, "Green Paper on Public Sector Information in the Information Society," 1999, chap. III.7, online: http://158.169.50.95:10080/info2000/en/publicsector/gp-index.html.

115 M. Gentot, "Access to Information and Protection of Personal Data," a paper delivered to the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, September 14, 1999, p. 5, online: http://www.pco.org.hk/conproceed.html.

116 B.H. Slane, "Bulk Release of Public Registers - A New Zealand Perspective,"an Address by the Privacy Commissioner to the 20th International Conference of Data Protection Authorities, September 16-18, 1998, online: http://www.knowledge-basket.co.nz/privacy/spubregf.html.

release of driver's licence information containing addresses[117] or the release of information about naturalized citizens[118];

- Broad dissemination of inaccurate information that can cause harm to either the data subject or the data recipient, such as might happen to a professional who was inadvertently left off the rolls of a professional association with the result that he or she lost referral business[119];

- The use of public record information to market unsolicited products to potential consumers against those consumers' wishes;[120]

- The increased use of compiled (albeit accurate) public information in a manner that causes embarrassment to the data subject,[121] or results in the data subject being denied services or

---

117 Robert Gellman, "Public Records: Access, Privacy, and Public Policy," May 16, 1995, p. 28, online: http://www.cdt.org/privacy/pubrecs/pubrec.html; Information and Privacy Commissioner of British Columbia, Investigation P95-005 "Cars, People and Privacy: Access to Personal Information through the Motor Vehicle Data Base," March 31, 1995, p. 4, online: http://www.oipcbc.org/investigations/reports/MVB.html.

118 M. Gentot, "Access to Information and Protection of Personal Data," *supra*, p. 6.

119 Federal Trade Commission, Bureau of Consumer Protection, "Individual Reference Services: A Federal Trade Commission Report to Congress", December 1997, online: http://www.ftc.gov/bcp/privacy/wkshp97/irsdoc1.htm#Individual Reference Services at p.2.

120 Information and Privacy Commissioner of British Columbia, "P98-011," *supra*, p. 15; Robert Gellman, "Public Records, Public Policy, and Privacy," in *Human Rights Magazine*, Winter 1999, p. 2, online: http://www.abanet.org/irr/hr/winter99toc.html.

121 European Commission, Data Protection Working Party, "Opinion NE 3/99 on Public Sector Information and the Protection of Personal Data," May 3, 1999, p. 5, http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp20en.htm.

products;[122] and

- Social withdrawal based on fears about loss of privacy.[123]

Possible solutions for the privacy risks associated with unrestricted access to, and use of, publicly available information have been the topic of considerable discussion and debate during the past several years. Most commentators have recognized that the central factor impinging upon the design of effective policy responses to this problem is the need to achieve a proper balance between public access to information and the privacy rights of individuals. As the B.C. Commissioner has noted:

> *The debate concerning public records centers on striking the balance between providing personal information that is necessary and useful to realize a public policy goal, while at the same time protecting the privacy of the data subjects as much as possible. The challenge, from our perspective, is to develop information guidelines which promote the policy goal while at the same time give individuals some control over the use of their personal information contained in a particular database.*[124]

While the B.C.Commissioner's comments were specific to public records and thus did not encompass other forms of publicly available information, the balancing principle he referred to can reasonably be

---

122 R. O'Harrow Jr., "Are Data Firms Getting Too Personal," March 8, 1998, *Washington Post* web site, online: http://washingtonpost.com/wp-srv/frompost/march98/privacy8.htm.

123 Beth Givens, "Public Records in a Computerized Network Environment: Privacy Implications," a speech given to the Privacy Rights Clearinghouse First Amendment Coalition Conference, Oakland, CA, September 23, 1995, online: http://www.privacyrights.org/AR/speech1.htm, p. 5.

124 Information and Privacy Commissioner of British Columbia, "P98-011," *supra*, p. 2.

viewed as being one of general applicability.

One specific means that has been proposed by a number of commentators to achieve this balance are controls that will authorize only those uses of public register information that accord with the purpose for which the information was compiled. So, for example, a lawyer accessing real property information in a Land Titles office in order to carry out a mortgage deal would be operating within the law, given that the register exists in part to permit the orderly conduct of real property transactions. On the other hand, a private investigator retained by a client to find the client's former spouse presumably would not be acting in accordance with the law if he sought address information through a search of real property records.

Such purpose-oriented constraints can be either of a positive or negative nature. Positive controls define a range of acceptable uses of information. Conversely, negative controls describe what may not be done with certain forms of information.[125] Controls of this sort are featured in the draft legislation from the Australian states of New South Wales and Victoria, in the American *Driver's Privacy Protection Act* of 1994 and in New Zealand's *Privacy Act 1993*. In providing recommendations based upon his review of the City of Victoria's practice of disclosing real estate assessment data via the Internet, the B.C. Commissioner advised:

> *Registry users should be clearly informed of the legitimate purposes for which property registries may be inspected, including prohibitions and limitations on unrelated uses, such as the compilation of mailing lists.*[126]

---

125 Robert Gellman, "Public Registers and Privacy: Conflicts with Other Values and Interests,"a paper delivered to the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, September 14, 1999, p. 9, online: http://www.pco.org.hk/conproceed.html.

126 British Columbia Information and Privacy Commissioner, Investigation P98-011, *supra*, p. 18.

The purposive approach is not uniformly endorsed, however. Robert Gellman has pointed out the interpretational difficulties inherent in trying to apply such purpose-oriented constraints:

> *If election registers can only be used for electoral purposes, can they be used to solicit support for candidates, parties, initiatives, fundraising, and causes? How closely does each purpose have to be tied to an ongoing electoral activity? What must new candidates, parties, and interest groups do to "qualify" to receive the information? Suppose that some electoral functions are conducted by commercial enterprises (e.g., collecting signatures on electoral petitions). Would an overlapping commercial purpose undermine the case for access? Can a commercial industry seeking to support a ballot initiative that would benefit the industry still use the registers? Does a grassroots advertising campaign with multiple purposes still qualify (Drink Milk, and Support Laws that Reduce the Price)? What about an organization interested in investigating voter fraud after an election? Even a seemingly clear purpose test can present enormously difficult application issues.*[127]

Another concern pertaining to the purpose-based approach centres upon the fact that some pieces of legislation which establish public registers lack any commentary setting forth the law's objects and explaining why information is collected, used and disclosed. Without such guidance from the relevant legislature, it can be very difficult for organizations or individuals subject to the law to decipher what limitations are being imposed on their conduct. Happily, this potential problem has been ameliorated to a certain extent in some Canadian jurisdictions by requirements in public sector access to information and privacy legislation for the regular publication of official statements by government departments and agencies detailing the reasons for collection, use and disclosure of information, including personal

---

[127] Gellman, "Public Registers and Privacy, *supra*, p. 6.

information.[128]

Other commentators have advocated that drafters of access to information and privacy legislation abandon their tendency to create blanket exemptions for publicly available information. Blair Stewart, New Zealand's Assistant Privacy Commissioner, has recommended that a more nuanced approach be adopted when fashioning future constraints on the use of information from public registers:

> *Public registers can be maintained consistently with certain normal data protection rules or principles. For example, when information is collected it ought to be possible to make individuals aware of the reason for requiring particular personal details, rights to rectification, and the consequences of the information being made publicly available. However, in my opinion, it would be impracticable to apply all data protection principles in completely unmodified form to public register information and assume that this would solve privacy problems. That approach might instead create new difficulties and render particular registers ineffective.*[129]

As for publicly available information available from media and other published sources, Mr. Stewart does not believe in the efficacy of trying to limit their use, noting: *"...it would be fairly unusual to try*

---

128 See, for example, Government of Canada, *Info Source: Sources of Federal Government Information 1999-2000* and *Info Source: Sources of Federal Employee Information 1999-2000*, online: http://dsp-psd.pwgsc.gc.ca/InfoSource/index-e.html.

129 Blair Stewart, "Five Strategies for Addressing Public Sector Register Privacy Problems", a paper delivered to the 21st International Conference on Privacy and Personal Data Protection, Hong Kong, September 14, 1999, p. 3, online: http://www.pco.org.hk/conproceed.html.

to constrain the use to which information obtained from publicly available publications could be put."[130]

With a view towards eliminating the commercial exploitation of publicly available information in inappropriate ways, some commentators and legislatures have settled upon the device of restricting the physical manner in which information is accessed/disclosed. British Columbia's Information and Privacy Commissioner, for example, has recommended that search engines provided for online review of assessment records be structured in such a fashion as to prevent name-based searching.[131] This accords with the approach taken to court decision databases in Italy, Belgium and France,[132] and to land records in Greece.[133] Other privacy regulators or governments have raised the prospect of, or implemented, process-oriented restrictions on:

(a) the amount of public information that can be accessed in a single transaction;[134]

(b) the search references (e.g. age, marital status) that can be employed when making a search;[135]

---

130 *Ibid*., p. 7.

131 British Columbia Information and Privacy Commissioner, Investigation P98-011, *supra*, p. 18.

132 European Commission, Data Protection Working Party, *Opinion No. 3/99 on Public Sector Information and the Protection of Personal Data*. May 3, 1999. Online: http://europa.eu.int/comm/internal_market/en/media/dataprot/wpdocs/wp20en.htm at p. 5.

133 *Ibid*., p. 6.

134 Blair Stewart, "Five Strategies for Addressing Public Sector Register Privacy Problems", supra, p. 5; New Zealand, *Privacy Act 1993*, Appendix, Principle 4; European Commission, Data Protection Working Party, *Opinion No. 3/99*, supra, p. 7.

135 Blair Stewart, New Zealand's Assistant Privacy Commissioner, "Drafting Suggestions for Departments Preparing Public Register Provisions,"

(c) the amount and type of personal information contained in a public register that is made available;[136] and

(d) the basic availability of data from public registers in an electronic format.[137]

A more fundamental restriction on the use of publicly available information contained in public records involves establishing laws prohibiting commercial usage entirely with respect to certain categories of personal information. This approach, advocated by the President of France's National Data Processing and Liberties Commission,[138] has been implemented in several European countries[139] and is reported to be a feature of American electoral laws[140] and Australian corporate legislation.[141] Partial restrictions are sometimes imposed through the rules prohibiting the re-sorting of public register personal information or its combination with personal information taken from another public register.[142]

As an alternative to a complete prohibition of the commercial use of personal information derived from

---

December, 1999, p. 1, online: http://www.knowledge-basket.co.nz/privacy/spubregf.html.

136 *Ibid.*; British Columbia Information and Privacy Commissioner, Investigation P98-011, *supra*, p. 10.

137 New Zealand, *Privacy Act 1993*, Appendix, Principle 3.

138 M. Gentot, "Access to Information and Protection of Personal Data," *supra*, p. 7.

139 European Commission, Data Protection Working Party, *Opinion No. 3/99*, *supra*, p. 8.

140 Robert Gellman, "Public Records: Access, Privacy, and Public Policy," *supra*, p. 22.

141 Blair Stewart, "Drafting Suggestions," supra, p. 7.

142 New Zealand, *Privacy Act 1993*, Appendix, Principle 2.

publicly available records, a number of regulators and commentators have advocated the use of "opt out" mechanisms.[143] This approach involves giving data subjects an opportunity to reject the disclosure of their personal information from a data repository, and can be seen in operation both in rules governing unlisted telephone numbers and in the American *Driver's Privacy Protection Act*. However, the right to opt out will not always accord with public policy objectives; in some cases the social value ascribed to public access is such that individuals should not be permitted to opt out of disclosure of certain of their particulars.[144] A manifestation of this policy perspective is found in the limiting language contained in the definition of "personal information" in Canada's public sector *Privacy Act*, particularly that paragraph that denies the protection of that Act to:

> *information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit.*[145]

Here personal privacy has been subordinated to the need for public oversight of governmental financial dealings. In other cases, the right to opt out has been made conditional upon the data subject being able to demonstrate, to the satisfaction of the administrator of the relevant data repository, a probability that the data subject will suffer harm if the personal information at issue is disclosed and/or that the individual's need for privacy in particular circumstances exceeds the assessed public need for the information to be disclosed.[146]

---

143 See, for example, European Commission, Data Protection Working Party, *Opinion No. 3/99*, supra, p. 8.

144 Robert Gellman, "Public Registers and Privacy: Conflicts with Other Values and Interests," supra, p. 6.

145 R.S.C. 1985, chap. P-21.

146 See, for example, subsection 58(2) of New South Wales' *Privacy and Personal Information Protection Act 1998*.

With all of the options for legislative intervention canvassed above, success would be dependent in large part upon creating rules that the public would view as a workable compromise between competing interests. This need for public validation of legislative constraints arising from privacy concerns has been acknowledged by some commentators. Robert Gellman, the noted American privacy expert, views the public records issue as an invitation for public dialogue:

> *Decisions about public availability of government records should be made with open eyes and after public debate. When the government discloses records about individuals, we know that the records will be exploited by marketers, placed on the Internet, and used in other ways that invade the privacy of citizens. The states do not have to allow these invasions to continue unchecked. Citizens can make choices about what records should be public in light of the institutions and technologies that are capable of using the records. They just have to let their legislators know that they care.*[147]

---

147 Robert Gellman, "Public Records, Public Policy, and Privacy," in *Human Rights Magazine*, Winter 1999, online: http://www.abanet.org/irr/hr/winter99toc.html.

PART 5 ANALYSIS OF POSSIBLE POLICY APPROACHES

5(i) The Ambit of Regulation Making Power in the Act

The power to make regulations pertaining to Part 1 of the Act is vested in the Governor in Council[148] by subsection 26(1) of the Act. Paragraph 26(1)(a.1) authorizes the Governor in Council to make regulations specifying information or classes of information for the purposes of paragraphs 7(1)(d), (2)(c.1) or (3)(h.1). Those three paragraphs provide for the collection, use or disclosure, respectively, of personal information without the knowledge or consent of the affected individual where the information being collected, used or disclosed is publicly available and is specified by the regulations.

In this Section, we will briefly consider certain general principles that affect the making and subsequent interpretation of regulations. We will then consider the scope of the regulation making power vested in the Governor and Council by paragraph 26(1)(a.1) in an effort to explain the nature and extent of the regulations that may hereafter be made pursuant to that provision.

General Principles

Regulations are a form of delegated legislation made by an administrative authority, using powers granted by a legislature, that impose legal standards of behaviour on the community at large. Once made, a regulation has the force of law. Parties that fail to comply with a regulation risk the imposition of any penalties that may be provided for in the enabling legislation or in the regulation itself.

The authority of administrative authorities to create and impose regulations is by no means absolute.

---

[148] The exercise of the powers granted to the Governor in Council in federal legislation is an executive function performed by the Special Committee of the federal Cabinet.

Rather, their exercise of regulation making power is subject to review by the courts. To be legally effective, a regulation must be made in accordance with a regulation-making authority contained in the governing statute.[149] If a regulation exceeds the underlying grant of authority, it is *ultra vires* and is susceptible to being struck down by the courts.[150] The degree of strictness with which Canadian courts review regulations tends to bear a direct relationship to the impact of the regulation on individual rights.[151]

In general terms, the judicial approach to the interpretation of statutes in Canada has been reasonably liberal. Canadian courts have repeatedly expressed the view that a "broad and purposive" interpretive approach should be taken wherever possible[152], and have repeatedly rejected a narrow and technical construction of enabling legislation.[153] At the federal level, this moderate approach is, in fact, a statutory requirement imposed by Parliament through section 11 of the *Interpretation Act*.[154]

When called upon to examine a regulation, a Canadian court will typically consider whether it is

---

149 G. Pépin and Y. Ouellette, *Principe de contentieux administratif*, 2nd Ed., Cowansville, Les Éditions Yvon Blais, 1982 at p. 321; R. Dussault and L. Borgeat, *Administrative Law - A Treatise*, 2nd Ed., Vol. 1, Canada, Carswell, 1985 at p. 317; Brown, D. and Evans, J. *Judicial Review of Administrative Action in Canada*. Toronto, Canvasback Publishing, 14:3310.

150 See, for example, *Eurig Estate (Re)*, [1998] 2 S.C.R. 565 (S.C.C.).

151 Brown & Evans, *supra*.

152 *Haig v. Canada* [1993] 2 S.C.R. 995 at 1019.

153 *Maple Lodge Farms Ltd. v. R.* [1982] 2 S.C.R. 2 at 7. *See Also: Canadian Association of Regulated Importers v. Canada (A.G.)* [1994] 2 F.C. 247 (C.A.) at 257.

154 R.S., c. I-23. That section states:

Every enactment is deemed remedial, and shall be given such fair, large and liberal construction and interpretation as best insures the attainment of its objects.

consistent with the "purposes and scope" of the enabling legislation.[155] This will often involve a review of the "objects" or "purposes" clause that is found near the beginning of most statutes in an effort to comprehend the Parliament's reasons for making the legislation.[156] Particular attention will be paid to any limitations, express or implied, on the exercise of the regulation-making power.[157]

Regulations made Pursuant to Paragraph 26(1)(a.1) of the Act

In a Canadian federal context, regulations are frequently made by the Governor in Council (the formal name given to the Special Committee of Cabinet) on the recommendation of a Minister of the Crown based upon authority contained in a statute passed by Parliament. Canadian courts have tended to exercise considerable deference when reviewing the exercise of regulation-making power by Cabinet.[158] Only in the most obvious cases will the courts intervene to invalidate such a regulation.[159] If, for example, the Governor in Council were to proceed to make a regulation without first performing some preliminary step imposed by Parliament in the enabling legislation, the resulting regulation would be susceptible to being overturned by a court if formally challenged.[160]

Based upon previous court decisions, any regulations made by the Governor in Council pursuant to section 26 of the Act would presumably operate within similar parameters, receiving a substantial degree of judicial deference if the statutory prerequisites are met. Viewed in this light, it is reasonably

---

155 *Jafari v. Canada (Minister of Employment and Immigration)* [1995] 2 F.C. 595 (F.C.A.) at 602.

156 Section 3 in the Act.

157 *Jafari, supra*.

158 *Thorne's Hardware Ltd. v. R.*, [1983] 1 S.C.R. 106 (S.C.C.)

159 Brown & Evans, *supra*, 14:3352.

160 *Inuit Tapirisat of Canada v. Canada (Attorney General)*, [1980] 2. S.C.R. 735 (S.C.C.).

straightforward to appreciate the expansive mandate given by Parliament to the Governor in Council in paragraph 26(1)(a.1): any personal information that can properly be described as being publicly available (as that term is understood at law) can be specified in a regulation, either by name or by class, whereupon that information or class of information may be collected, used or disclosed without the consent or knowledge of the affected individual.

In determining whether a type of personal information or a class of personal information meets the threshold test of being publicly available, the drafters of any future regulation made pursuant to that paragraph will need to consider the limits placed on the concept of "publicly available" by previous court decisions, as discussed in Part 1(ii) of this paper. Regulations under this paragraph cannot properly be made with respect to information that is not of a publicly available sort.

If government authorities opt to exercise their delegated authority to regulate in respect of classes of personal information, they may properly combine within any such class items of personal information that share "common characteristics or attributes."[161] Given the broad discretion that the Cabinet enjoys when fashioning regulations pursuant to a specific grant of power[162] such as paragraph 26(1)(a.1), it appears that the Governor in Council will be largely free to determine the extent and characteristics of any such classes as it sees fit, subject to the caveat that any class created must pertain to information that is publicly available at law.

---

161 Garner, B.A., ed. *Black's Law Dictionary*, 7th ed., Minneapolis, West Group, 1999 at p. 242.

162 *Gill v. Canada (Minister of Citizenship and Immigration)* [1999] F.C.J. No. 1250 (F.C.T.D.).

5(ii) Possible Regulatory Responses

Based upon a review of (i) policy initiatives undertaken in other countries to address the issue of the appropriate use of publicly available personal information, (ii) the recommendations of privacy experts from various lands and (iii) the legal framework created by the Act and relevant jurisprudence, it appears that there are a number of basic policy mechanisms that might reasonably be employed to delimit the forms of publicly available information that organizations subject to the Act will be permitted to collect, use or disclose without the consent of the affected individual.

As a preliminary matter, we note that the broadly worded delegation of power granted to the Governor in Council by the Act appears to justify the crafting of regulations providing for the unregulated use of both specific items and general categories of publicly available personal information. Any regulations of the latter sort should, of course, not be so general as to unduly impede their comprehension and application by those Canadians made subject to the Act. The Act's requirement that every form of publicly available personal information which is to benefit from the exemption afforded by the regulations must be specified therein creates a strong incentive to reference categories of information, for otherwise the task would be to individually list each possible form of such information, which would prove very onerous indeed.

As for the substantive element of any regulations that might be produced, there appears to be strong international and domestic support for the use of purpose-oriented language to restrain the inappropriate collection, use and disclosure of publicly available personal information contained in public registries/records. A defensible argument can also be made in support of applying this same limitation to personal information that is made available to the public through the news media or other publications. As the regulation provisions are framed in a way that requires the creation of positive controls, any purpose-oriented language that was employed would presumably purport to exempt those collections, uses or disclosures that were in keeping with the purpose for which the register or

publication was created.

The use of "opt out" provisions has also proven attractive to legislators in other jurisdictions. While policy considerations may render this alternative unattractive in the context of public registers, it may be nonetheless useful in controlling the collection, use or disclosure of personal information derived from common commercial relationships, such as that personal information found in the telephone white pages.

Arguments in favour of outright bans on the collection, use or disclosure of certain forms of publicly available personal information are less persuasive. While it is possible, for example, that regulatory language could be produced that would authorize only non-commercial activity, this approach seems at odds with the presumed objective of attaining a balance between access and privacy. If, instead, an appropriate use of both "opt out" and purpose-oriented provisions is made, it should be possible to isolate those commercial uses that are problematic from those which are generally regarded as being beneficial.

Reliance on purpose driven provisions may give rise to some initial uncertainty as affected organizations attempt to distinguish permitted from proscribed conduct. However, interpretational disputes are a normal part of the legislative process. With most categories of public information, a common sense approach should permit most organizations to discern their entitlements in this regard.

CONCLUSION

We note that the research that we have carried out in the course of preparing this paper has only served to fortify our belief that technological advances have fundamentally altered the parameters of "private" life; both government and business now possess the means to compile and analyze vast amounts of data derived from our individual public interactions. Left unregulated, this ever developing technological proficiency could run roughshod over our conventional concepts of privacy. The challenge, therefore, will be to develop reasonable rules to frame the private sector's dealings with third party personal information. In doing so, federal authorities will need to avoid unduly impeding both the public's ability to oversee government operations and the business sector's ability to carry on business in an efficient manner. If they can master this delicate balancing act, the result should benefit all Canadians.