SUBMISSION ON AUSTRALIAN PRIVACY PRINCIPLES: EXPOSURE DRAFT

JULY 30, 1010

Dr. Colin J. Bennett
Department of Political Science
University of Victoria
PO Box 3060 STN CSC
Victoria, BC V8W 3R4
Canada
cjb@uvic.ca
http://web.uvic.ca/polisci/people/faculty/bennett.php

Introduction

I have been researching and writing about privacy protection policy for over 25 years, and have written a number of books on the international and national rules for the protection of personal data, including *The Governance of Privacy: Policy Instruments in Global Perspective* (MIT Press, 2006). For the last six months, I have been a Visiting Scholar affiliated with the Cyberspace Law and Policy Center at the University of New South Wales. During this time, I have become quite familiar with Australian privacy protection policy. I hope, therefore, that I can draw upon this experience, as well as my comparative knowledge, to offer some contributions to the debate about the new Australian Privacy Principles (APPS). I am, of course, submitting this in my name only.

I will focus on those aspects of the Exposure Draft which, I think, are in most need of attention. I hope also, that I can offer some potential insights and solutions from my knowledge of the operation of Canadian privacy protection laws, and especially the Protection of Personal Information and Electronic Documents Act (PIPEDA) of 2000.

Before commenting on the Exposure Draft, I wanted first to add my voice to the calls to remove the small business exemption from Australian privacy law, referred to on page 6 of the Companion Guide. I think this is one of the principal differences between Australian privacy protection law for the private sector and comparative provisions in other countries, including Canada. Experience with PIPEDA suggests that there have been many successfully upheld complaints against small business. Some enterprises with few employees can process extraordinarily sensitive forms of data, the misuse of which can prove exceptionally harmful to individuals. I would strongly encourage the committee to recommend the repeal of this exemption.

APP1

There is one important omission from the principle of the "open and transparent management of personal information." Some laws contain a provision that organizations should nominate a "responsible person" or "designated individual" who should be responsible for the implementation of privacy law within the organization. This need not be an exclusive responsibility, but it is essential that one person assumes that responsibility, and develops an expertise on the issue. Schedule One of the Canadian Protection of Personal Information and Electronic Documents Act (PIPEDA) of 2000 contains the following:

4.1 Principle 1 — Accountability

An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.

4.1.1

Accountability for the organization's compliance with the principles rests with the designated individual(s), even though other individuals within the organization may be responsible for the day-to-day collection and processing of personal information. In addition, other individuals within the organization may be delegated to act on behalf of the designated individual(s).

4.1.2

The identity of the individual(s) designated by the organization to oversee the organization's compliance with the principles shall be made known upon request.

This maybe implicit in section 2(4) of APP 1, but I would strongly recommend that it be made explicit. It sends an important signal to organizations that they have to devote continuous resources to the implementation of their privacy policy.

APP2

I think section 2(a) of APP2 means that anonymity or pseudonymity does not apply if individuals are required by law to identify themselves – presumably to obtain a benefit or service. Presumably all government entities are authorised under some law. This should be clarified to stipulate that there must be another legal authorization for identification.

APP3

One of the main problems with "reasonably necessary" tests related to an organization's function is that organizations can specify a very broad set of goals and purposes, without limitation by law. Without a corresponding provision requiring a **justification of purpose**, this provision leaves open huge opportunities to define their functions and activities in such a way that any collection of personal information is "reasonably necessary" or "directly related." Section 5(1)3 of PIPEDA attempts to limit purpose specification as follows:

> *(3) An organization may collect, use or disclose personal information only for purposes that a reasonable person would consider are appropriate in the circumstances.*

Thus there has to be a reasonable purpose or activity, and not just a "reasonable" connection to a pre-defined purpose or activity. This provision is also, of course, open to abuse but it does allow the Privacy Commissioner to find that the purposes stated are not "reasonable"; and there have been one or two occasions in Canada when this has occurred. I note that the Companion Guide states that this section does mean that "from the perspective of a reasonable person the function or activity is legitimate for that type of entity" (p. 16). I do not think that the existing draft makes this clear.

It also seems to me that the information should be "reasonably necessary**and** directly related to."

I am also troubled by the provisions regarding sensitive information contained in 4(2)(ii) where "consent" is not explicitly defined as "express" or "positive" consent. An international standard seems to have emerged, inherent in the EU Directive and elsewhere, that there must be *express* consent for the collection of sensitive information whereas implied consent may be satisfactory for non-sensitive data. Further if there is any doubt, organizations should assume that the information is sensitive. This may be the intention of these sections, but it is not clear from my reading. The provision is open to abuse where, for instance, an organization might assume implied "consent" for the collection of health data and simply provides an "opt-out" or "negative consent" option.

2(a)(ii) should read:

"The individual provides express consent for the collection of the information."

I would also encourage the committee to consider another provision which appears in the Canadian law – the so-called "refusal to deal" clause. Section 4.3.3. of Schedule One reads:

> *An organization shall not, as a condition of the supply of a product or service, require an individual to consent to the collection, use, or disclosure of information beyond that required to fulfil the explicitly specified, and legitimate purposes.*

What this means in practice is that an organization cannot say that an individual has to consent to the use or disclosure of personal information as a condition for supplying a product or service. An example would be if an organization requires an individual to allow the organization to use information for direct marketing purposes at the time of filling out a warranty on a product. This addition would address what has been called the "bundled consent" issue in the Australian debates.

APP 5

I do not understand the logic for inserting the words "if any" into 6(1) of APP5. It organizations collect personal information then I see no reasonable circumstances under which they would not notify the individual of the matters listed in subsection 2.

APP7

It is really erroneous to list "direct marketing" as a "privacy principle." Direct marketing is a practice not a principle, although I am not at all clear what today constitutes "direct" marketing particularly online. There might be an argument for applying special rules to direct marketing, as exist in the 1995 EU Directive for instance. But to elevate this practice (and industry) to the status of a principle is really inconsistent with other "principle" based laws and regimes, and will be viewed as such by overseas privacy regulators and experts. If there is the need to stipulate special provisions for direct marketing, and I am not convinced that there is, then I would strongly advise that these rules be distributed appropriately throughout the other sections. Furthermore, I do not understand why this "principle" is included under Division 4 on "Dealing with Personal Information." Direct marketing rules relate to collection, use and disclosure, another reason for distributing the rules throughout the various sections.

APP8

I do not understand the "reasonably believes" wording in 9(2)(a). Either there is a law, or binding scheme, or there isn't. Most privacy experts could provide a list of countries that have comprehensive privacy or data protection laws of similar breadth to the APPs. It is also not too difficult to ascertain the more precise sectoral laws (on consumer credit reporting, for instance) that might apply in some circumstances. An organization should not be excused of liability for the transfer of personal information because it has not properly done its homework.

The sum total of APP8 is quite confusing, because nowhere does it specify what the "reasonable steps" might be, although the Companion Guide makes it clear that ordinarily there would be a contractual relationship. Again, I think the Canadian law is an improvement – and it is simpler. It makes no distinction between processing by a third party in Canada, or overseas. It is also not qualified by a long list of exemptions as are listed under Section (2) of APP8. The organization is responsible, and liable, for any breach of the principles. Section 4.1.3 of Schedule One of PIPEDA reads:

> *An organization is responsible for personal information in its possession or custody, including information that has been transferred to a third party for processing. The organization shall use contractual or other means to provide a comparable level of protection while the information is being processed by a third party.*

The Companion Guide makes it clear that "if the overseas recipient does an act or practice that would be a breach, then the entity will be liable" (p. 13). If that is the intention, then why not state this more explicitly in APP8?

APP9

See my comments on APP7 above. Again, the provisions here should not be listed as a separate "principle." I applaud the intention behind this provision – to restrict the use of government identifiers by the private sector, something that is not so explicit in Canadian legislation. But, again, I think that the rules concerning identifiers should be spread throughout the other sections.

APP 10

I do not understand why the word "relevant" appears in 11(2) but not in 11(1).

APP 12

I disagree with the exemption to individual access for requests that are "frivolous or vexatious." I can understand why such provisions are justifiable in general access to

information statutes, but not in privacy protection laws. The right to access ones personal information is a human right, regardless of motive. This provision is open to abuse, especially where individuals might be in conflict with a particular organization over a particular matter, and reasonably want to know everything the organization holds on them. At the very least, the provision should state that the organization should be obliged to report and account for the use of this discretion.

I hope these comments prove useful to the Committee in its deliberations:

Dr. Colin J. Bennett
Department of Political Science
University of Victoria, BC. Canada