

JAN 15 2008

January 11, 2008

Richard Simpson  
Director General  
Industry Canada, Electronic Commerce Branch  
300 Slater Street  
Ottawa, Ontario  
K1A 0C8

Re: Consultations on the Implementation of the Government Response to the Fourth Report of the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the "Committee"), Statutory Review of the *Personal Information Protection and Electronic Documents Act* (PIPEDA)

Mr. Simpson:

The Privacy Advisory Group (PAG) of the Canadian Institute of Chartered Accountants (CICA) is pleased to submit this letter in response to the Government of Canada's request for consultations regarding the review of PIPEDA. The PAG is made up of leading privacy professionals from several Canadian accounting firms and advises the CICA on the development and promotion of privacy services and resources including *Generally Accepted Privacy Principles*.

The PAG has considered the Government's request and wishes to present views on the following topics: Breach Notification, Work Product and Investigative Bodies.

#### Breach Notification

In the Government's response, it noted that the Government supported a notification requirement in certain cases where "...a high risk of significant harm to individuals or organizations exist..." While the PAG supports that PIPEDA be amended to include a breach notification provision, the group believes that the use of terms such as "high risk" or "significant harm" is subjective and open to inconsistent interpretation. In addition, we believe that all individuals and organizations have a right to be notified should they be exposed to harm, significant or not. Accordingly, we propose that individuals and organizations be notified, along with the Office of the Privacy Commissioner of Canada (OPC), when there is any risk of harm to them from the breach.

The PAG also recommends the following:

- That PIPEDA be amended to include a definition of what constitutes "harm" to the organization or individual, giving consideration to personal harm, financial harm, security of the person and reputation.
- That PIPEDA be amended to include a definition of what constitutes a "privacy breach"
- Notification should be direct to each individual as well as a public notification in a manner similar to toy or food recalls. The timing of such notification should be as



soon as possible after the breach is identified, confirmed and its extent (who may have been impacted) is reasonably understood.

- Organizations that fail to notify specific individuals and organizations, the general public and the privacy commissioner should be subject to fines and penalties.
- Without consent notification of certain third parties (such as credit bureaus) should be made whenever a breach requiring notification occurs. Credit bureaus should be required to make a notation to each record that includes when and where the breach occurred.

### Work Product Information

The PAG supports the Committee's recommendation that work products be excluded from the definition of personal information. In considering an appropriate definition of work product, the group considered the definition from British Columbia's *Personal Information Protection Act* (PIPA) and wishes to propose the following addition to the current PIPA definition:

"information prepared or collected by an individual or group of individuals as a part of the individual's or group's responsibilities or activities related to the individual's or group's employment or business, but does not include personal information about an individual who did not prepare or collect the personal information *unless such personal information is incidental to the information being prepared or collected.*"

In support of their professional obligations as public accountants, Chartered Accountants are required to document their work in files known as "working paper files". Working paper files may include evidence such as quantitative and qualitative analysis, copies of statements and results of sampling tests. At times, obtaining evidence in a particular area may include the collection of personal information from a client's customers. The information collected is usually incidental to the work product being generated. We believe that should the personal information be incidental to the report being created, that such personal information should not prevent the report and its associated working paper files from being considered as work products.

### Investigative Bodies

The PAG supports the Committee's recommendation that the "investigative bodies" designation process be replaced with a definition of "investigation"<sup>1</sup> similar to that found

---

<sup>1</sup> "**investigation**" means an investigation related to

- (a) a breach of an agreement,
- (b) a contravention of an enactment of Canada or a province,
- (c) a circumstance or conduct that may result in a remedy or relief being available under an enactment, under the common law or in equity,
- (d) the prevention of fraud, or
- (e) trading in a security as defined in section 1 of the *Securities Act* if the investigation is conducted by or on behalf of an organization recognized by the British Columbia Securities Commission to be appropriate for carrying



in the Alberta and British Columbia *Personal Information Protection Acts* thereby allowing for the collection, use and disclosure of personal information without consent for that purpose. The definition provides greater clarity and would harmonize practices with provincial privacy legislation.

In adopting the Alberta/BC definition, the PAG proposes that the definition be expanded to include “regulatory activities by a self-regulatory body”. The provincial institutes of Chartered Accountants, as self-regulatory bodies (SROs), are required to develop and enforce high national standards to protect the public interest and maintain the good reputation and integrity of the CA profession. Being able to conduct investigations in support of their regulatory activities is essential in protecting the public interest and in some cases, the collection, use and disclosure of personal information by SROs without consent is necessary in ensuring a complete and thorough investigation. Many of the organizations currently designated as investigative bodies under PIPEDA are SROs. This addition would ensure that SROs can continue their important regulatory activities while providing additional specificity and clarity to the definition.

Thank you for the opportunity to share our views on the specific topics requested. In addition to the above comments, the CICA Privacy Advisory Group has comments and recommendations on other areas within PIPEDA and would be pleased to discuss these with you or others within your office.

Should you have any questions or wish to contact the Privacy Advisory Group, please contact Nicholas F. Cheung, CA, Principal, Assurance Services Development by e-mail at [nicholas.cheung@cica.ca](mailto:nicholas.cheung@cica.ca), by phone at (416) 204-3251 or by mail at CICA, 277 Wellington St W, Toronto, Ontario, M5V 3H2.

On behalf of the Privacy Advisory Group,

Yours very truly,

A handwritten signature in blue ink, appearing to read 'Robert G. Parker', written over a light blue horizontal line.

Robert G. Parker, FCA, CA•CISA, CMC  
Chair

---

out investigations of trading in securities,  
if it is reasonable to believe that the breach, contravention, circumstance, conduct,  
fraud or improper trading practice in question may occur or may have occurred