



Information and Privacy  
Commissioner/Ontario

Commissaire à l'information  
et à la protection de la vie privée/Ontario

January 13, 2011

European Commission  
Directorate-General Justice  
Unit C3 - Data Protection  
B - 1049 Brussels

**Re: Comments on the European Commission's Comprehensive Approach  
on personal Data Protection in the EU – Public Authority**

I am pleased to offer my comments and support regarding the above consultation, through the enclosed document. The European Commission's leadership and outreach efforts are to be applauded, as well as the consideration given to the key challenges in privacy protection facing us in the 21<sup>st</sup> Century.

My comments include ideas for supporting and strengthening the four privacy principles and processes identified in the consultation document.

I am grateful for the opportunity to provide this input and would welcome the opportunity to assist further, if requested.

Sincerely yours,

A handwritten signature in blue ink, appearing to read 'Ann Cavoukian'.

Ann Cavoukian, Ph.D.  
Commissioner

Enclosure



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

2, rue Bloor est  
Bureau 1400  
Toronto (Ontario)  
M4W 1A8

416-326-3333  
1-800-387-0073  
Fax/Télééc: 416-325-9195  
TTY: 416-325-9539  
<http://www.ipc.on.ca>

**Submission from Dr. Ann Cavoukian, Ph.D.,  
Information and Privacy Commissioner of Ontario, Canada**

European Commission  
Directorate-General Justice  
Unit C3 - Data protection  
B - 1049 Brussels

**Re: Consultation on the Commission's Comprehensive Approach on  
personal Data Protection in the European Union - Public Authority**

As the Information and Privacy Commissioner of Ontario, Canada, I welcome the opportunity to comment on the European Commission's consultation on a comprehensive approach on personal data protection in the European Union. Since 1988, my Office has been independent of government and is mandated to uphold and promote open government and the protection of personal privacy in Canada's largest province.

I applaud the Commission's leadership and outreach efforts, and the thoughtful consideration given to the key challenges in privacy protection facing us in the 21<sup>st</sup> Century. I'd like to offer comments and support for strengthening the following privacy principles and processes identified in the consultation document:

- Data Minimization
- Accountability
- Privacy Impact Assessments
- Privacy by Design

***Data Minimization***

I wholeheartedly support strengthening the principle of data minimization as it applies to data controllers. By "data minimization" I refer to limits on collection, use, retention and disclosure of any personal data. Data minimization is essential to effective privacy protection, and can save organizations the risk and expense of managing personal information they may have no need for. Where there is no personal information, there is no consequent duty of care, with all that it implies. Further, data minimization requirements assists organizations to think through what personal information is actually necessary for their purposes, and guards against secondary uses and possible function creep.

***Accountability***

I also support strengthening the principle of accountability. In today's world of ubiquitous data availability, trust is increasingly a function of how well organizations manage personal information in their care transparently and responsibly, and are able to demonstrate their diligence to customers, partners, shareholders, and regulators. Putting into place effective policies and mechanisms to ensure compliance with data protection laws is essential. In this respect I am delighted to see Commission support for greater uses by data controllers of Privacy Enhancing Technologies (PETs) and for applying the "principle" of *Privacy by Design*.

Privacy by Design (PbD) offers excellent prospects for strengthening accountability, security and individual rights. More than a single principle or concept, PbD consists of a set of seven foundational principles that, taken together, represents a privacy solution that is both comprehensive and proactive. PbD principles are universal in nature; they may be applied to technologies such as PETs, and to business information systems and processes, as the consultation paper notes, and also to information eco-systems, meta-structures, even extending to systems of regulation and oversight.

### ***Privacy Impact Assessments (PIAs)***

I applaud Commission proposals supporting greater uses of data protection impact assessments. In Canada, Privacy Impact Assessments (PIAs) have been mandatory for the federal and provincial public sectors for the past decade. Here I would direct you to my office's work on [Privacy Risk Management](#) and [Privacy Risk Optimization](#), and also on [Federated Privacy Impact Assessments](#) (PIA), which are relevant to PIAs that may cut across organizational boundaries. In most instances it is not the technology itself, but, rather, how it is implemented that raises privacy concerns. This is an issue that would have to be considered in scenarios where multiple organizations, operating under different implementation models, are asked to jointly prepare an assessment of a particular technology or system.

In Ontario, a PIA is understood as a process – a living document – to evaluate the privacy implications of information or technology systems. It involves developing an information flow map, applying a set of privacy questions to the information flow, identifying risks and impacts and developing dynamic responses. In general terms, PIAs offer a number of benefits, including supporting informed decision-making and system design, anticipating the public's possible privacy concerns, and generating confidence that privacy objectives are being considered and addressed in the development and implementation of new systems or processes. The real value of a PIA, however, lies in how it is implemented.

The PIA in itself is not a mechanism for protecting consumer privacy; it is simply a tool for working through the application of practical privacy principles to particular contexts.

If the findings of a PIA are not acted upon, and the privacy risks identified are not resolved, then the PIA has little value, serving as a procedural exercise to be completed.

In my view, PIAs function optimally when they are used as a design tool, helping to guide the embedding of privacy, ideally as a default. For several years now, I have been a vocal proponent of [Privacy by Design](#) – the concept of engineering privacy directly into the design of new technologies, business processes, and networked infrastructure as a core functionality. PbD makes it clear that privacy and other core business objectives can – and must – co-exist in a positive-sum (win/win), not zero-sum relationship.

### *Privacy by Design*

In October 2010, at the International Conference of Data Protection and Privacy Commissioners in Jerusalem, I proposed a *Privacy by Design* [resolution](#) to the full assembly of regulators. The resolution was unanimously adopted, and privacy regulators around the world have now recognized *PbD* as an “essential component of fundamental privacy protection.”

For the purposes of this consultation, I believe this to be significant in two ways: first, *Privacy by Design* is rapidly emerging as the gold standard for data protection internationally, and is therefore relevant to the Commission’s objective of engaging other jurisdictions on reducing barriers to trade and commerce across borders.

Second, and perhaps more important, our *Privacy by Design* approach fosters precisely the kind of simultaneous protection *and* innovation the Commission is hoping to enlist by challenging system designers and engineers to think creatively to address privacy issues, as design requirements. For examples of this kind of innovation in action, please see my office’s recent papers on building the [7 Foundational Principles of Privacy by Design](#) into Ontario’s emerging [Smart Grid](#), published with Ontario’s leading utility, Hydro One, and a joint [paper](#) with the Ontario Lottery and Gaming Corporation (OLG), building on a privacy-enabled facial biometric application.