Information and Privacy
Commissioner of Ontario
Commissaire à l'information
et à la protection de la vie privée de l'Ontario

February 24, 2010

Federal Trade Commission
Office of the Secretary
Room H-135 (Annex P)
600 Pennsylvania Avenue, N.W.
Washington, DC 20580

Re: Privacy Roundtables – Comment, Project No. P095416

As the Information and Privacy Commissioner of Ontario, Canada, please accept my submission to the Federal Trade Commission's (FTC) third privacy roundtable. I applaud the FTC for initiating this series of public roundtable discussions that explore the privacy challenges of twenty-first century technology and business practices involving the collection, use and disclosure of consumer data.

I believe that organizations can best respond to these privacy challenges by taking a *Privacy by Design* approach – a term I coined back in the '90s. Indeed, having the Center for Democracy and Technology (CDT) recommend *Privacy by Design* in their submission to the FTC's second privacy roundtable, *Role of Privacy by Design in Protecting Consumer Privacy*, was very gratifying.

Back in the '90s, when the notion of embedding privacy into the design of technology and business practices was far less prominent, I developed the concept of *Privacy by Design* to address the ever-growing and systemic effects of large-scale networked data systems and the growing use of information and communication technologies (ICTs). I strongly believe that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation. Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution to putting the control over personal data back into the hands of the consumer. Today, however, technological innovation and the digitization of information have created an unimaginable number of new services and benefits for consumers, while at the same time, creating an unprecedented number of privacy risks. Therefore, a more substantial approach is now required – *Privacy by Design* extends to a 'trilogy' of encompassing applications not limited only to IT systems, but extending to accountable business practices and physical design and networked infrastructure.

The need for an organization to have accountable business policies and practices to protect consumer data remains constant. More than ever before, a comprehensive and proactive *Privacy by Design* approach to information management is called for – one which assures an end-to-end chain of custody and responsibility, right from the very start.

.../2

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

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

Tel: 416-326-3333
1-800-387-0073
Fax/Téléc: 416-325-9188
TTY: 416-325-7539
www.ipc.on.ca

An important element of *Privacy by Design*, contained in the 7 Foundational Principles, is the concept of achieving full functionality while at the same time, protecting privacy. For some time now, I have advanced the view that it is not necessary to trade off privacy against equally important goals such as security, transparency or business functionality. I call this taking a positive-sum, not a zero-sum approach, where privacy and information technology or business practices may co-exist in a doubly enabling 'win-win' scenario, not an 'either/or' scenario, involving unnecessary tradeoffs. I believe that this is integral to the FTC's goal of determining how to best protect consumer privacy while supporting the beneficial uses of technological innovation.

Privacy by Design provides organizations with the opportunity to achieve what I envision as the 'Gold Standard' in the handling of consumers' personal information. One of the over-arching goals of *Privacy by Design* is to gain the lasting confidence and trust of consumers.

Below I outline the 7 Foundational Principles of *Privacy by Design*, in greater detail:

1. Proactive not Reactive; Preventative not Remedial

The *Privacy by Design* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. *Privacy by Design* does not wait for privacy risks to materialize, nor does it offer remedies for resolving privacy infractions once they have occurred - it aims to *prevent* them from occurring. In short, *Privacy by Design* comes before-the-fact, not after.

2. Privacy as the Default

Privacy by Design seeks to deliver the maximum degree of privacy by ensuring that personal data are automatically protected in any given IT system or business practice. If an individual does nothing, their privacy still remains intact. No action is required on the part of the individual to protect their privacy - it is built into the system, *by default*.

3. Privacy Embedded into Design

Privacy by Design is embedded into the design and architecture of IT systems and business practices. It is not bolted on as an add-on, after the fact. The result is that privacy becomes an essential component of the core functionality being delivered. Privacy is integral to the system, without diminishing functionality.

4. Full Functionality – Positive-Sum, not Zero-Sum

Privacy by Design seeks to accommodate all legitimate interests and objectives in a positive-sum 'win-win' manner, not through a dated, zero-sum approach, where unnecessary trade-offs are

.../3

made. *Privacy by Design* avoids the pretense of false dichotomies, such as privacy vs. security, demonstrating that it is possible to have both.

5. End-to-End Lifecycle Protection

Privacy by Design, having been embedded into the system prior to the first element of information being collected, extends throughout the entire lifecycle of the data involved, from start to finish. This ensures that at the end of the process, all data are securely destroyed, in a timely fashion. Thus, *Privacy by Design* ensures cradle to grave, lifecycle management of information, end-to-end.

6. Visibility and Transparency

Privacy by Design seeks to assure all stakeholders that whatever the business practice or technology involved, it is in fact, operating according to the stated promises and objectives, subject to independent verification. Its component parts and operations remain visible and transparent, to users and providers alike. Remember, trust but verify.

7. Respect for User Privacy

Above all, *Privacy by Design* requires architects and operators to keep the interests of the individual uppermost by offering such measures as strong privacy defaults, appropriate notice, and empowering user-friendly options. Keep it user-centric.

The FTC is also seeking comments related to personal health information. Our view is that all personal health information is sensitive in nature. We note that the principles of *Privacy by Design* may be applied to all types of personal information. You may also find it interesting to learn that here in Ontario, my Office has jurisdiction over health care privacy legislation through the *Personal Health Information Protection Act of 2004* (*PHIPA*). This *Act* applies to both public and private sector health care providers (known as 'health information custodians' in the *Act*) involved in the delivery of health care services. *PHIPA* is considered to be groundbreaking legislation as a result of the manner in which it was drafted – so as to ensure that privacy would not impede the delivery of health care services, yet at the same time, the protection of patients' personal health information would be paramount.

The popularity of *PHIPA* continues to grow. According to a recent report by the U.S. Institute of Medicine (IOM), *Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research*, the IOM concluded that the existing rules under the *Health Insurance Portability and Accountability Act* (*HIPAA*) did not sufficiently protect privacy. It pointed directly to Ontario's *PHIPA* as the sole model to serve as a framework for revising the Privacy Rule in *HIPAA* and developing a new approach in the United States.

.../4

Building consumer confidence and trust in organizations is greatly facilitated by making privacy the default. This is one of the reasons why I believe it has become more critical now than ever to embrace *Privacy by Design*. If it grows well into the future, then we can be certain of ensuring the future of privacy.

I want to thank the FTC for the opportunity to submit comments to the third privacy roundtable. For more information on *Privacy by Design*, please feel free to visit our website at http://www.privacybydesign.ca, and do not hesitate to contact me if I can be of any assistance.

Sincerely yours,

Ann Cavoukian, Ph.D.
Commissioner

cc: The Honorable Jon Leibowitz, Chairman, Federal Trade Commission
David Vladeck, Director, Federal Trade Commission