

**BEFORE THE  
DEPARTMENT OF COMMERCE**

**NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY**

Request for Comments

Docket # 120214135-2135-01

**Multistakeholder Process to Develop Consumer Privacy Codes of Conduct**

---

**COMMENTS OF THE INFORMATION AND PRIVACY  
COMMISSIONER, ONTARIO, CANADA**

---

Ann Cavoukian, Ph.D.  
Commissioner

Office of the Information and  
Privacy Commissioner  
Ontario, Canada  
2 Bloor Street East, Suite 1400  
Toronto, Ontario  
Canada  
M4W 1A8  
Toll Free: 1-800-387-0073

April 2, 2012

## COMMENTS OF THE INFORMATION AND PRIVACY COMMISSIONER, ONTARIO, CANADA ON THE MULTISTAKEHOLDER PROCESS TO DEVELOP CONSUMER DATA PRIVACY CODES OF CONDUCT

### I. INTRODUCTION

In accordance with the National Telecommunications and Information Administration, U.S. Department of Commerce (NTIA), the Information and Privacy Commissioner of Ontario, Canada (the IPC) hereby submits the following comments on NTIA's request for public comments on the multistakeholder process to develop consumer data privacy codes of conduct. The IPC supports NTIA's effort to facilitate the development of enforceable codes of conduct that implement the full *Consumer Privacy Bill of Rights*. In my earlier comments on the Privacy and Innovation Green Paper (which you have referenced in your request for comments<sup>1</sup>) I remarked on distinct consumer privacy issues that relate to mobile devices. Insights such as these have been derived from an approach to privacy protection termed *Privacy by Design (PbD)*.

### II. COMMENTS

#### A. The IPC

As the Information and Privacy Commissioner of Ontario I oversee the freedom of information and privacy laws in Canada's most populous province – a capacity in which I am now serving my third term. Over the past several years my Office has been actively engaged in raising awareness of how to build privacy into many of the issues raised by NTIA concerning consumer data privacy. It is my firm conviction that the process of facilitating enforceable codes of conduct that implement the full *Consumer Bill of Privacy Rights*, and consumer data protection generally, would be well served by applying the principles of *PbD*.

The IPC has authored several papers on *PbD*, including: *Privacy by Design: The 7 Foundational Principles Implementation and Mapping of Fair Information Practices* which relates the principles of *PbD* to the widely-accepted concepts concerning fair information practices in an electronic marketplace; *Mobile Near Field Communications 'Tap 'n Go' Keep it Secure and Private* which discusses short range wireless technology that allows mobile devices to actively interact with passive objects and other active mobile devices; and *Wi-Fi Positioning Systems: Beware of Unintended Consequences Issues Involving the Unforeseen Uses of Pre-existing Architecture* which explores the identity and privacy issues that could arise from the unintended uses of the MAC address of mobile devices. As the successful implementation of any consumer oriented innovation relies on consumer confidence and trust, addressing privacy concerns at the design stage creates an opportunity to establish privacy as a default setting.<sup>2</sup>

---

<sup>1</sup> At footnote 11.

<sup>2</sup> These and more discussion papers can be found at the IPC website: [www.ipc.on.ca](http://www.ipc.on.ca).

## B. Privacy by Design

*PbD* is an approach to protecting privacy that seeks to embed privacy into the design specifications of technologies, business practices, and physical infrastructures from the outset. *PbD* is predicated on the idea that technology is inherently neutral and can be used to chip away at privacy or protect it. The same is true of business processes and physical infrastructure. Based on 7 Foundational Principles, I first developed *PbD* in the 1990s. (For a full overview of *PbD* principles, please read *Privacy by Design: The 7 Foundational Principles*.<sup>3</sup>) NTIA's role in providing a forum for discussion and consensus-building among stakeholders could be further supported and enhanced with the concept of *PbD*. The principles of *PbD* can foster the rules and dialogue aimed at operationalizing the *Consumer Bill of Rights* ensuring that these are carried through to information technologies, business practices and networked infrastructure.

*PbD* maps to the well-established Fair Information Practices (FIPs) and modernizes them. *PbD* principles innovate FIPs by ensuring that the protection of privacy is proactive, not reactive; preventative, not remedial. Being proactive about privacy leads to demonstrating methods that recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct the negative impacts proactively are established. *PbD* principles innovate FIPs by accommodating all legitimate interests and objectives in a positive-sum "win-win" manner, not through a dated, zero-sum approach, where unnecessary trade-offs are made. *PbD* avoids the pretense of false dichotomies, such as privacy versus security, demonstrating that it is possible, and far more desirable, to have both.

*PbD* has been applied to a wide range of dynamic technology contexts. Most notably in the mobile sector my office has collaborated with researchers at Arizona State University to develop a practical tool for developers, service providers, and users.<sup>4</sup> It should also be noted that the GSM Association (GSMA), an association of mobile operators and related companies devoted to supporting the standardizing, deployment and promotion of the GSM mobile telephone system worldwide has explicitly adopted *PbD* as part of its *Mobile Privacy Principles*.<sup>5</sup>

The IPC submits that *PbD* is also consistent with emerging national privacy and security policies, as well as international standards. The recent Federal Trade Commission (FTC) report *Protecting Consumer Privacy in an Era of Rapid Change* refers to *PbD* as a means to build privacy into every stage of product development. The NIST adopted *PbD* as a recommended methodology in *NISTIR 7628 Smart Grid Cyber Security Strategy and Requirements, Vol. 2, Privacy and the Smart Grid*. The FTC adopted *PbD* as a recommended approach in its report *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business*

---

<sup>3</sup> The 7 Foundational Principles of *Privacy by Design* are: 1. Proactive not Reactive; Preventative not Remedial; 2. Privacy as the Default Setting; 3. Privacy Embedded Directly into Design; 4. Full Functionality – Positive-Sum, not Zero-Sum; 5. End-to-End Security – Full Lifecycle Protection; 6. Visibility and Transparency – Keep it Open; 7. Respect for User Privacy – Keep it User-Centric.

<http://www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf>

<sup>4</sup> A. Cavoukian and M. Prosch, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*, (December 2010) available online at

<http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1040>

<sup>5</sup> See GSMA, *Mobile Privacy Principles*, (January 2011) available online at <http://gsmworld-dev.webgen.gsm.org/documents/mobile-privacy-principles/20005/>

*and Policymakers*. A *PbD* requirement is also included in the draft Kerry-McCain *Commercial Privacy Bill of Rights Act of 2011* (§103). The European Commission's Working Party on the Protection of Individuals with Regard to the Processing of Personal Data (Article 29 Working Party) issued *Opinion 12/2011 on smart metering* on April 4, 2011 in which *PbD* is recommended for smart meter deployment in Europe. In October 2010, *PbD* was recognized as the global privacy standard in a landmark resolution by the International Conference of Data Protection and Privacy Commissioners in Jerusalem. Commissioners at this conference are a worldwide assembly of privacy regulators.

## CONCLUSION

The IPC suggests that *PbD* as a methodology for the protection of privacy can support and enhance NTIA's work in developing consumer data privacy codes of conduct. *PbD* is consistent with emerging national privacy and security policies, as well as international standards. I would be pleased to provide any additional information that might assist you in your work.

Respectfully submitted,



---

Ann Cavoukian, Ph.D.

Ann Cavoukian, Ph.D.  
Commissioner  
Office of the Information and Privacy Commissioner  
Ontario, Canada  
2 Bloor Street East, Suite 1400  
Toronto, Ontario  
Canada  
M4W 1A8

Telephone: (416) 326-3948  
Fascimile 416-325-9187  
TTY: 416-325-7539  
Toll Free: 1-800-387-0073  
E-mail: [commissioner@ipc.on.ca](mailto:commissioner@ipc.on.ca)  
Website: [www.ipc.on.ca](http://www.ipc.on.ca)