



Information and Privacy
Commissioner of Ontario

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

**Submission of
the Information and Privacy Commissioner,
Ontario, Canada**

**Response to the Department of Commerce
Internet Policy Task Force**

***Commercial Data Privacy and Innovation in the
Internet Economy:
A Dynamic Policy Framework***

January 27, 2011



**Information and Privacy
Commissioner of Ontario**

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

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca

Table of Contents

Fair Information Practice Principles (FIPPs).....	1
<i>Privacy by Design</i>	2
Enhancing Transparency	5
Privacy Impact Assessments (PIAs).....	6
Privacy Policy Office (PPO)	7
Conclusion.....	7
Appendix A - Extract from Response to the FTC <i>Framework for Protecting Consumer Privacy in an Era of Rapid Change</i>	8

Response to the Department of Commerce Internet Policy Task Force

Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework

Thank you for the opportunity to comment on the proposed framework for *Commercial Data Privacy and Innovation in the Internet Economy*. I applaud your leadership in this area, and the thoughtful consideration you have given to some of the key challenges in privacy protection in the online world.

Fair Information Practice Principles (FIPPs)

I fully support FIPPs as a key foundational element of any privacy protection scheme. FIPPs are, in one form or another, the cornerstone of privacy laws and policies in many jurisdictions, including my own, Ontario, Canada.

I wholeheartedly agree with your attention to the principle of data minimization, which is essential to effective privacy protection, and can save organizations considerable resources by avoiding the expense of protecting personal information they may not need. Where no personal information has been collected, there is no consequential duty of care, with all that it implies. Further, data minimization helps businesses think through what personal information is actually necessary to their business purposes, and guards against potential function creep.

Indeed, data minimization is so fundamental to meaningful privacy protection that I would urge you to include it among your other “high priority” FIPPs: enhancing transparency, encouraging greater detail in purpose specifications and use limitations, and verifiable evaluation and accountability.

In terms of how best to articulate FIPPs, you are, of course, aware of the many different approaches. I would like to call your attention to the [Global Privacy Standard](#), which was developed by a Working Group of International Data Protection Commissioners and accepted in 2006 at the 28th annual International Data Protection Commissioners Conference in the United Kingdom. As such, it provides a good basis for engaging internationally on privacy requirements and for the first time, specifically includes the concept of data minimization in the Collection Limitation principle. That principle states:



The collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.

Data Minimization – The collection of personal information should be kept to a strict minimum. The design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability, and linkability of personal information should be minimized.

The Global Privacy Standard also includes the concepts of limiting disclosure and retention, which I believe are essential components of fundamental privacy principles. Too often, organizations focus exclusively on collection, neglecting to take proper care of the secure destruction of records at the end of their life cycle. We work closely with NAID – the National Association for Information Destruction – since we have seen a great many breaches take place as a result of careless records disposal.

While FIPPs have informed the foundation of data protection efforts around the world, increasingly there is a growing momentum behind the principles of *Privacy by Design*, which build upon, but go beyond FIPPs. *Privacy by Design* is rapidly emerging as the new gold standard for privacy and data protection. I call your attention to its prominence in the Federal Trade Commission’s proposed *Framework for Protecting Consumer Privacy*, and urge you to consider aligning foundational elements of your proposed approaches in order to create clarity for businesses and consumers.

My office has done extensive work on *Privacy by Design* (www.privacybydesign.ca), including a **mapping** of its principles against FIPPs that may be of particular interest to you. We are also currently doing some ground-breaking work in the area of building the principles of *Privacy by Design* into regulatory frameworks. That paper will be posted on our *PbD* web site when it is completed in the coming months.

Privacy by Design

For several years now, I have been an active proponent of *Privacy by Design* (*PbD*) – the concept of engineering privacy directly into the design of new technologies, business processes, and networked infrastructure, as a core functionality. *PbD* is proactive in nature, and *embeds* privacy into the design and architecture of systems and processes as a way of ensuring its protection. It also makes it clear that privacy and other core business objectives can – and must – coexist in a positive-sum (win-win), not zero-sum relationship. Recently, Don Tapscott and Anthony D. Williams, authors of *Macrowikinomics: Rebooting Business and the World*, wrote an **article** urging companies to adopt the principles of *Privacy by Design*.

The 7 Foundational Principles of *Privacy by Design* are as follows:

1. *Proactive* not Reactive; *Preventative* not Remedial

The *Privacy by Design (PbD)* approach is characterized by proactive rather than reactive measures. It anticipates and prevents privacy invasive events *before* they happen. *PbD* 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 Setting*

We can all be certain of one thing – the default rules! *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 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 Security – *Full Lifecycle Protection*

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



6. *Visibility* and *Transparency* – Keep it *Open*

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 – Keep it *User-Centric*

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.

At the International Conference of Data Protection and Privacy Commissioners in Jerusalem, I proposed a *Privacy by Design (PbD) Resolution* to the full assembly of regulators. The Resolution was unanimously passed and adopted. Privacy regulators around the world have now recognized *Privacy by Design* as “an essential component of fundamental privacy protection,” forming a new international privacy standard.

For your purposes, I believe this to be significant in two ways: first, *Privacy by Design* is rapidly emerging as the gold standard for data protection, internationally. Incorporating its principles into your own Framework would certainly be relevant to your objective of engaging other jurisdictions on reducing barriers to trade and commerce across borders, as many will be moving to implement this higher standard.

Second, and perhaps more important, the *Privacy by Design* approach fosters precisely the kind of innovation you are hoping to enable by challenging system designers and engineers to think creatively to address privacy issues as design requirements. I have spoken extensively to engineers, systems designers, academics and research labs on proactively engineering privacy directly into the systems being designed. The creativity and innovation that they bring to this area is unparalleled, and often proportionate to the magnitude of the challenge they are facing. For examples of this type 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, GE, and IBM, and a joint *paper* with the Ontario Lottery and Gaming Corporation (OLG) building on a privacy-enabled facial biometric application.

I urge you, therefore, to consider going beyond FIPPs by adding the principles of *PbD* to the foundation of your proposed Framework.

You may also be interested to note that my office has announced, in its response to the FTC’s proposed *Framework for Protecting Consumer Privacy*, a new development in the interpretation of the second *Privacy by Design* Foundational Principle: a new *two-step process*, which makes it possible to achieve the spirit of *Privacy as the Default Setting* in the limited situations where the existing industry practice presents a barrier to achieving the principle *directly*, right from the outset. Please see Appendix A for greater detail on the new process that we are calling, “The Ontario Two-Step.”

This interpretation arose in light of a question about how *Privacy as the Default Setting* could be applied to the privacy challenges of online tracking and, specifically, to the **FTC’s Do Not Track concept**. As market leaders continue to work with implementing *PbD*, I expect that other questions may arise as to how to interpret **The 7 Foundational Principles**. From my perspective, the key factor will be to implement *PbD* in a way that recognizes the existence of multiple functionalities, operating in a positive-sum manner – *not* one at the expense of another, but rather in a doubly-enabling, synergistic relationship.

Enhancing Transparency

You comment extensively on how “legalese” leads to a low level of effective transparency for consumers. There is no question that dense, lengthy notices about how personal information will be collected, used, and disclosed are not effective in communicating meaningfully to individuals.

My office has done extensive work on “Short Notices,” primarily in the health-care sector.

Working with the Ontario Bar Association and other health-care stakeholders, we developed and published a package of informational materials including a **poster** for hospitals, along with **brochures** for patients. These materials use a consistent format and plain language to explain how a patient’s personal health information will be used, and what rights and options are available to the patient in that regard. We published a similar **poster** and **brochures** for health-care facilities, and another set for medical offices. The health-care space in Ontario is quite heterogeneous, and so consistency of format for use across the sector was sought from the start, as a means of promoting effective transparency, patient empowerment, and organizational compliance with health-care privacy law and regulations in Ontario, Canada’s largest province. You may find these of interest as you consider the issue of simplified notice more fully in the online context.

We strongly encourage and promote the work of organizations to actively develop consumer protective features for small screens and mobile devices, such as privacy taxonomies, special icons and symbols, innovative presentation layouts, layered notices, and user options, as well as transparency regarding the use of such features as encryption, geo-location, and Wi-Fi connectivity.



Similar work being undertaken by public and private sector parties for online spaces where protecting all consumers, especially youth or vulnerable persons, who may be subject to fraud, cyber-bullying or online predators, is a priority. We welcome creative solutions in this area and anticipate considerable progress being made.

Privacy Impact Assessments (PIAs)

I also applaud your proposals concerning PIAs. As I am sure you know, this term is used very variably across different sectors and in different jurisdictions. It will be important, therefore, to be clear about what your requirements are, particularly if you envision a scheme where all or part of a PIA would be made public.

To be most effective, a PIA must be grounded in a solid understanding of fair information practices, such as the ones found in the [Global Privacy Standard \(GPS\)](#) for technology development, or those contained in the privacy and data protection laws of many jurisdictions. Of course, any applicable legal requirements must be considered as well, along with industry-specific guidelines. It is also of critical importance that the PIA process involve all the relevant departments in an organization, rather than being limited, for example, to an Information Technology exercise.

I noted with interest your ideas on performing PIAs for emerging technologies. Here I would direct you to my office's work on [Federated Privacy Impact Assessments](#), and also on [Cloud Computing](#), both of which are relevant to PIAs that may cut across organizational boundaries. I would also caution you that, in many instances, it is not the technology itself, but rather how it is implemented, that raises privacy concerns. This is an issue that would need to be considered if you contemplate 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 implementation. 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 not resolved, then the PIA has little value, simply serving as an exercise to be completed and a box to be checked off. We must always guard against this.

In my view, PIAs function optimally when they are used as a design tool, helping to guide the embedding of privacy, in a proactive manner.

Privacy Policy Office (PPO)

The Framework proposes the creation of a Privacy Policy Office to continue the work of the Internet Policy Task Force by acting as a convenor of diverse stakeholders and a center of Administration commercial data privacy policy expertise. I suggest you consider removing the word “policy” from the name of this office, and instead call it the Privacy Protection Office (or something similar), to underscore the fact that, while privacy policies are important, they are simply part of the arsenal of effective privacy protection. There is certainly room to think beyond the confines of policy, and to include, for example, the principles of *Privacy by Design*, which extend well beyond policy and are proactively embedded into design.

Further, policies are only as effective as their implementation. I believe that communicating a clear commitment to privacy protection will be important in providing assurances to other jurisdictions that the Office is committed not only to policy, but to concrete implementation actions. I also think that calling the office the Privacy Protection Office or Privacy Office will go farther in reassuring the public of the office’s motives and orientation, thereby contributing to the building of consumer trust that is so essential to the continued growth of the Internet economy.

Conclusion

I thank you again for the opportunity to comment on your proposed Framework, and wish you all the best as you move this important issue forward. If I can be of any assistance to you, please do not hesitate to call upon me.

Ann Cavoukian, Ph.D.

Information and Privacy Commissioner
Ontario, Canada

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

www.ipc.on.ca
www.privacybydesign.ca

Appendix A

**Extract from Response to the FTC *Framework*
for *Protecting Consumer Privacy in an Era of Rapid Change***

Announcing a New PbD Interpretation, Applicable to the FTC's Do Not Track Proposal

Privacy as the Default Setting:

The FTC report requested feedback on how the elements of the proposed Framework might apply to “the real world.” Accordingly, we have given this considerable thought and devised a new interpretation of the second Foundational Principle, directly applicable to an online tracking or targeted advertising. We call it the “Ontario Two-Step.”

Recently, I was asked by leading privacy strategist, Peter Cullen, Chief Privacy Strategist of Microsoft Corporation, how the second PbD principle, *Privacy as the Default Setting*, could be applied to the privacy challenges of online tracking, specifically, to the **FTC's Do Not Track concept**.

I acknowledge that the *Default* Principle is the most difficult to achieve, in this context. Nonetheless, organizations must strive to achieve it.

Conceptually, *Privacy as the Default* requires that personal data be **automatically** protected in IT systems and business practices. Whether it be a business practice or service, a consumer technology or tool, the principle is to be applied equally, with the effect that individuals should not be required to take additional steps to protect their privacy – it should be built into the system, ideally as a precondition – by default.

But context is key. Applying this principle to online consumer marketing would oblige organizations to request consumers to “opt-in” to tracking and receiving of targeted messages, a largely non-existent practice in this area. It is critical, however, that PbD principles be applied in a thoughtful manner *and* in their entirety, for they must serve the best interests of both consumers *and* businesses. We call this “positive-sum,” which represents the essence of the fourth principle of *Privacy by Design: Full Functionality* – Positive-Sum, not Zero-Sum.

We must also recognize that we don't often have the opportunity to design systems and services from the bottom up – from scratch – without regard to existing regulatory structures, privacy norms, prevailing business practices, and legacy protocols. For these reasons, it is imperative to consider the current and prevailing standard of practice in a given culture or domain.

In North America, and I suspect in many other jurisdictions, the dominant privacy consent model for online consumer marketing and targeted advertising is currently “opt-out.” Recognizing this fact, I would like to announce a new development in the interpretation of the second Foundational Principle in the context of online tracking and marketing: a new “two-step” process, which makes it possible to achieve the spirit of *Default Privacy* in situations where the existing industry practice presents a barrier to achieving the principle *directly*, right from the outset.

The process is predicated on assessing the context. Where the prevailing norms and industry standards of practice are “opt-out,” as in the case of online targeted advertising and marketing (which may be based on a variety of tracking technologies), proceeding directly to an “opt-in” model would not only be impractical, but perhaps also harmful to the industry involved. Instead, we recommend that the following two-step process be followed:

The “Ontario Two-Step” Process:

Step 1: Present a clear and “in process”¹ opportunity for the consumer to opt-out of subsequent on-line tracking, targeted advertising or marketing communications.

Step 2: Once an individual has chosen to “opt-out” of future tracking or receipt of subsequent advertising or marketing information, then their choice must remain **persistent** over time and be **global** in nature (with respect to that organization).

This two-step process achieves the end state envisioned in the *Privacy Default* Principle, but one step removed. While it does not provide an automatic default, it gets you there once you have chosen to opt-out. This two-step process recognizes legitimate business practices, but is driven by the consumer, and is persistent in its effect. Most important, the consumer’s choice triggers the default. It also creates a choice mechanism that is universal in nature, while providing more granular control over the types of advertising they receive (wishing perhaps to receive some, but not others).

Most important, this approach puts *Privacy as the Default* in the context of the entire set of 7 Principles by ensuring that the fourth principle of *Full Functionality* (Positive Sum, not Zero-Sum), is equally respected. Since the existing industry standard of practice in marketing pursuits is “opt-out,” moving immediately to a full opt-in may serve to harm one of the legitimate functionalities involved: the business interest of advertising and marketing. Operationalizing the second principle in the form of a persistent, global opt-out, however, enables *both* principles to be satisfied, and provides a universal choice mechanism. Perhaps a prominent online social network such as Facebook could be persuaded to add an “out” button that could ultimately serve this purpose, given their emerging role as a universal sign-in authority. In our view, there is no reason to limit such a uniform choice mechanism to *online* behavioral advertising – mobile applications would present an equally suitable venue.

There is a precedent for this pragmatic approach taken from my own jurisdiction. Under the Ontario *Personal Health Information and Protection Act* (PHIPA), which regulates the health sector in Canada’s largest province, my office worked with hospital foundations to develop a robust and standard opt-out practice for patients to deal with future marketing efforts, whereas before, there had been no such guidance in place.

¹ “In process” refers to presenting opt-out information and options available to consumers, in the course of normal use and operation. That is, the consumer does not have to search for them – they are clearly visible and accessible during the course of the normal process involved at the time, and presented in plain language – making them easy to understand.

Opting-in was not considered to be a viable option because it would effectively shut down a valuable source of revenue for hospital foundations. Instead, it was decided that hospitals could offer a prominent “opt-out” on their first mailing to discharged patients, which would then allow them to globally and persistently “opt-out” of any future contact, from that point on, making it the default condition thereafter.² While the process began with an “opt-out” as the first step, *Privacy by Design* principles kicked in at the 2nd step, in an innovative, persistent manner, thereby approximating the conditions of a default setting, one step removed.

The FTC’s Do Not Track proposal may benefit from a similar two-step process in the application of this *Privacy by Design* principle.

As market leaders continue to work with implementing PbD, I expect that other questions may arise as to how to interpret **The 7 Foundational Principles**. From my perspective, the key factor will be to implement PbD in a manner that recognizes the existence of multiple functionalities, operating in a positive-sum manner – not one at the expense of another, but rather in a doubly-enabling, synergistic relationship.

In summary, we must always strive to satisfy the totality of *Privacy by Design*, as reflected in the entire set of 7 Foundational Principles. If the existing standard of practice in an area is “opt-out,” then reversing this could serve to disrupt the functionality of a given sector’s interests, in this case, advertising and marketing, which would serve to violate the fourth principle of seeking a positive-sum solution. This principle contemplates the existence of **multiple** functionalities, operating in a positive-sum manner – not one at the expense of another, but rather operating in unison, in a doubly-enabling manner.

Ultimately, PbD must represent a win-win solution for businesses and consumers alike, thereby paving the way for continued creativity and innovation.

² Note that the personal information disclosed is restricted only to the name and address of discharged patients.



**Information and Privacy
Commissioner of Ontario**

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

416-326-3333
1-800-387-0073
Fax: 416-325-9195
TTY (Teletypewriter): 416-325-7539
Website: www.ipc.on.ca