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 & Privacy Commissioner, Ontario, Canada

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

January 21, 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

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

As the Information and Privacy Commissioner of Ontario, Canada, I welcome the opportunity to comment on the FTC's proposed *Framework for Protecting Consumer Privacy*, as set out in the preliminary staff report released December, 2010.

I applaud the FTC's leadership role, and the thoughtful consideration given to the key privacy challenges facing consumers, businesses and regulators today, both online and off.

The proposed Framework contains a wealth of fresh ideas and proposals. I would like to offer the following comments on each of the four Framework elements:

1. Scope
2. Privacy by Design
3. Consumer Choice
4. Transparency

1) Scope

I note the FTC's interest in broadening the scope of privacy protections, and strongly encourage taking that direction. As the staff report notes, the distinction between identifiable and non-identifiable data is rapidly eroding. If privacy protections are to continue to have meaning in our fast-evolving information economy, then the proposed Framework should apply to any business-related activity that generates data that may, "be reasonably linked to a specific consumer, computer, or other device." I strongly encourage a broad, principles-based approach to privacy oversight that is at once consistent with current international standards and practices, and yet adaptable to evolving market needs and commercial requirements.

Given the phenomenal growth in the collection and use of consumer data, limiting privacy protections solely to data that are demonstrably identifiable would ignore growing capabilities and risks that so-called "anonymized," "unidentifiable" or "meaningless" data may be subsequently decrypted, linked, and re-identified, with profound implications for individuals.

Personal information, be it biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, is the fabric that forms the basis of our modern identities. It must be managed responsibly. When it is not, individual privacy is compromised, business accountability is undermined, and market confidence and trust are eroded.

With respect to the level of protection extended to personal data, I strongly believe that personal information must be protected at a level commensurate with its sensitivity. For example, medical data is among the most sensitive types of data, followed perhaps by financial data. The collection, use, and disclosure of such sensitive information must be afforded the strongest protection possible.

Turning to another area – the Smart Grid – I have recently been flagging the emergent privacy concerns associated with the modernization of the electrical grid. The harvesting of detailed energy usage data and its linkage to identifiable individuals raises troubling questions about potential surveillance, profiling and other privacy concerns, by various third parties. It is far better to address the latent smart grid privacy issues systematically, early on, and avoid relying on after-the-fact breach detection, punishment and restitution. A broader definition of personal information, as proposed in the FTC report, is a desirable and necessary starting point.

2) *Privacy by Design*: The 7 Foundational Principles

I welcome the emphasis on systemic privacy and security protections in the proposed Framework. And I am grateful for the FTC's support of applied *Privacy by Design* – an approach to privacy protection that I have been advancing for some time now.

Privacy by Design (*PbD*) advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must be *proactive* in nature, ideally becoming an organization's default mode of operation, but in a positive-sum, not zero-sum manner.

The 7 Foundational Principles of *Privacy by Design*

1. ***Proactive*** not Reactive; ***Preventative*** not Remedial
2. Privacy as the ***Default Setting***
3. Privacy ***Embedded*** 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***

The principles of *Privacy by Design* are universal in nature and extend to a trilogy of areas: 1) information technologies; 2) accountable business practices; and 3) physical design and networked infrastructures. The objectives of *PbD* – ensuring informational control and privacy for individuals, while gaining a sustainable competitive advantage for businesses – may be achieved by observing The 7 Foundational Principles.

These principles, and how to apply them, are discussed in considerable detail at www.privacybydesign.ca, as well as a description of our *Privacy by Design* Ambassador program.

Implementing *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. This Resolution was unanimously passed and adopted by the entire assembly of Commissioners and Data Protection Authorities. Privacy regulators from around the world have now recognized *Privacy by Design* as "an essential component of fundamental international privacy protection."

The hyperlinks in the FTC report to my web site, www.privacybydesign.ca, lead to extensive guidance and illustrative case studies on applying PbD to business practices, to help "implement procedurally sound privacy practices throughout an organization," as sought out in the FTC report. The value of this collection of work is that it has been developed and written in partnership with the very businesses and organizations to which the FTC framework would apply. As the report notes, while concepts such as reasonable security and secure disposal may not be new, the time has come to implement them on a systematic basis. I couldn't agree with you more!

For businesses and organizations, the *Privacy by Design* solution involves more than applying substantive fair information practice principles (FIPPs), such as specifying purposes and placing limitations on uses, into business technologies, operations, or architectures. To be clear, the 7 Foundational Principles of *Privacy by Design* incorporate FIPPs, but go much further. Achieving *Privacy by Design*'s gold standard in a complex digital world involves going beyond FIPPs – to demonstrate leadership and commitment to the highest privacy standards, to driving those standards into information systems in a verifiable and trusted way, and to achieving innovative, positive-sum "win-win" results that effectively raise the bar for others to follow.

Indeed, the hallmark of strong privacy protection is not merely an organization's ability to implement strong privacy and security controls, but to consistently maintain those protections over time, in a systematic and verifiable way.

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.

Privacy Impact Assessments

The FTC report seeks to promote accountability and responsible information practices, encouraging businesses to "assess the privacy impacts of specific practices, products and services to evaluate risks and ensure that [they] follow appropriate procedures to mitigate those risks," and to carry out "periodic reviews of internal policies." Privacy Impact Assessments (PIAs) are an essential component of any serious effort to engineer privacy into the design of new technologies, business processes, and networked infrastructure, as a core functionality. In the context of *Privacy by Design* solutions, PIAs and risk assessments can support multiple business objectives and help to achieve innovative, positive-sum outcomes.

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

In Ontario, a PIA is understood to be a process – a living document to evaluate the privacy implications of information or technology systems. It involves first developing an information flow map, applying a set of privacy questions to the information flow, identifying risks and impacts, and then 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. A 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 resolved, then the PIA has little value, simply serving as an exercise to be completed. I have witnessed this many times, where the only value of conducting a PIA was to enable a staff person to check off the box requiring that on be completed: end-of-story.

Again, my office offers many PIA tools and risk assessment resources. I noted with interest the FTC's ideas on performing PIAs for emerging technologies. Here I would call attention to our work on Federated Privacy Impact Assessments, and Cloud Computing, both of which are relevant to PIAs that cut across organizational boundaries. This is an issue that would need to be considered if scenarios are contemplated where multiple organizations, operating under different implementation models, are asked to jointly prepare an assessment of a particular technology or system.

3) Simplified Consumer Choice

The FTC report seeks to simplify choice, especially consumer consent for some "commonly accepted practices." While I appreciate the intent of this proposal, I caution against relying upon overly broad categories of business purposes that may serve to threaten the principle of data minimization, which is essential to effective privacy protection. As noted in the report: "companies should collect only the information needed to fulfill a specific, legitimate business need" for all the reasons offered, including helping businesses think through what personal information is actually necessary to their business purposes, guarding against potential function creep and data breaches, and saving organizations much-needed resources by avoiding the expense of safeguarding personal information they may not actually need. I am in total agreement with this.

Accordingly, I encourage the FTC to interpret any categories of "common businesses uses" of data that exempt the need to obtain consumer consent in a restrictive manner. Simplified consumer choice should not mean less openness or transparency of business operations, or reduced consumer access to personal data, stored with a full account of any uses by the business involved. Indeed,

the FTC report later suggests that companies should increase the transparency of their data practices and provide reasonable access to consumer data, among other transparency-enhancing proposals. I support these proposals wholeheartedly!

4) Business Transparency

The FTC report calls for privacy notices to be clearer, shorter and more standardized, in order to enable better comprehension and comparison of privacy practices. There is no question that dense, lengthy notices about how personal information is intended to be collected, used, and disclosed are not effective in communicating meaningfully with 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 such as two-way communications for consent, as well as transparency and protection regarding the use of such features as encryption, geo-location (location-fuzzing, obfuscation, etc.) and wi-fi connectivity (ambient notices, etc.).

Similar work involving the online protection of not only all consumers, but in particular youth and vulnerable persons, who may be especially subject to fraud, cyber-bullying or online predators, is a priority. We welcome creative solutions in this area and anticipate considerable progress being made in the near future.

5) Conclusion

The FTC Framework touches on many of the most important privacy challenges facing businesses and consumers today.

In my view, *Privacy by Design* is the best way forward to a future where privacy – the very foundation of our freedom and democracy – continues to be recognized and protected as a social good. Not only do the principles of Privacy by Design go beyond FIPPs, but they do so in a way that emphasizes positive-sum outcomes. As a result, they lend themselves to practical "real world" applications that support business interests and consumer privacy, *simultaneously*.

The new "Ontario Two-Step" process announced on page four of this submission is a good example of how PbD can be implemented in a manner that recognizes the existence of multiple functionalities operating in a positive-sum manner. A clear opt-out opportunity, coupled with the implementation of that opt-out in a way that is both **persistent** and **global**, achieves the end state envisioned in the *Privacy Default* Principle, one-step removed. As a result, it achieves a win-win, positive-sum outcome for both online marketers and consumers.

I respectfully ask that you consider the new Two-Step process, and also consider more broadly the ways in which the principles of PbD may serve to support "real world" privacy solutions, that are both workable and effective.

I thank the FTC for the opportunity to comment on your proposed Framework. My office will be following future developments that flow from this important initiative, and stands ready to provide whatever assistance may be requested – rest assured, you have our complete support!

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

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