Privacy by Design

The 7 Foundational Principles

Implementation and Mapping of Fair Information Practices

Ann Cavoukian, Ph.D.
Information & Privacy Commissioner
Ontario, Canada

Purpose:

This document provides readers with additional information, clarification and guidance on applying the 7 Foundational Principles of *Privacy by Design (PbD)*.

This guidance is intended to serve as a reference framework and may be used for developing more detailed criteria for application and audit/verification purposes.

Scope:

These information management principles – and the philosophy and methodology they express – can apply to specific technologies, business operations, physical architectures and networked infrastructure – entire information ecosystems.

The universal principles of the Fair Information Practices (FIPs)[1] are affirmed by those of *Privacy by Design*, but go beyond them to seek the highest global standard possible. Extending beyond FIPs, *PbD* represents a significant "raising" of the bar in the area of privacy protection.

1 Cavoukian, Ann, Ph.D., Information & Privacy Commissioner, Ontario, Canada. *Creation of a Global Privacy Standard* (November 2006), at www.ipc.on.ca/images/Resources/gps.pdf

Context:

With the shift from industrial manufacturing to knowledge creation and service delivery, the value of information and the need to manage it responsibly have grown dramatically. At the same time, rapid innovation, global competition and increasing system complexity present profound challenges for informational privacy.

While we would like to enjoy the benefits of innovation – new conveniences and efficiencies – we must also preserve our freedom of choice and personal control over our data flows. Always a social norm, privacy has nonetheless evolved over the years, beyond being viewed solely as a legal compliance requirement, to also being recognized as a market imperative and critical enabler of trust and freedoms in our present-day information society.

There is a growing understanding that innovation, creativity and competitiveness must be approached from a "design-thinking" perspective – namely, a way of viewing the world and overcoming constraints that is at once holistic, interdisciplinary, integrative, innovative, and inspiring.

Privacy, too, must be approached from the same design-thinking perspective. Privacy must be incorporated into networked data systems and technologies, **by default**. Privacy must become integral to organizational priorities, project objectives, design processes, and planning operations. Privacy must be embedded into every standard, protocol and process that touches our lives. This document seeks to make this possible by striving to establish a universal framework for the strongest protection of privacy available in the modern era.

The 7 Foundational Principles of Privacy by Design are presented below ***in Bold***, followed by the FIPs principles that map onto each one.

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. 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.

Whether applied to information technologies, organizational practices, physical design, or networked information ecosystems, *PbD* begins with an explicit recognition of the value and benefits of proactively adopting strong privacy practices, early and consistently (for example, preventing (internal) data breaches from happening in the first place). This implies:

- A clear commitment, at the highest levels, to set and enforce high standards of privacy – generally higher than the standards set out by global laws and regulation.
- A privacy commitment that is demonstrably shared throughout by user communities and stakeholders, in a culture of continuous improvement.
- Established methods to recognize poor privacy designs, anticipate poor privacy practices and outcomes, and correct any negative impacts, well before they occur in proactive, systematic, and innovative ways.

2. Privacy as the ***Default***

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.

This *PbD* principle, which could be viewed as **Privacy by Default,** is particularly informed by the following FIPs:

- **Purpose Specification** – the purposes for which personal information is collected, used, retained and disclosed shall be communicated to the individual (data subject) at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.
- **Collection Limitation** – 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 personally identifiable information should be kept to a strict minimum. The design of programs, information and communications 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.
- **Use, Retention, and Disclosure Limitation** – the use, retention, and disclosure of personal information shall be limited to the relevant purposes identified to the individual, for which he or she has consented, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.
- Where the need or use of personal information is not clear, there shall be a presumption of privacy and the precautionary principle shall apply: the default settings shall be the most privacy protective.

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.

Privacy must be embedded into technologies, operations, and information architectures in a holistic, integrative and creative way. Holistic, because additional, broader contexts must always be considered. Integrative, because all stakeholders and interests should be consulted. Creative, because embedding privacy sometimes means re-inventing existing choices because the alternatives are unacceptable.

- A systemic, principled approach to embedding privacy should be adopted – one that relies upon accepted standards and frameworks, which are amenable to external reviews and audits. All fair information practices should be applied with equal rigour, at every step in the design and operation.
- Wherever possible, detailed privacy impact and risk assessments should be carried out and published, clearly documenting the privacy risks and all measures taken to mitigate those risks, including consideration of alternatives and the selection of metrics.
- The privacy impacts of the resulting technology, operation or information architecture, and their uses, should be demonstrably minimized, and not easily degraded through use, misconfiguration or error.

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 pretence of false dichotomies, such as privacy vs. security, demonstrating that it is possible, and far more desirable, to have both.

Privacy by Design does not simply involve the making of declarations and commitments – it relates to satisfying all of an organization's legitimate objectives – not only its privacy goals. *Privacy by Design* is doubly-enabling in nature, permitting full functionality – real, practical results and beneficial outcomes to be achieved for multiple parties.

- When embedding privacy into a given technology, process, or system, it should be done in such a way that full functionality is not impaired, and to the greatest extent possible, that all requirements are optimized.
- Privacy is often positioned in a zero-sum manner as having to compete with other legitimate interests, design objectives, and technical capabilities, in a given domain. *Privacy by Design* rejects taking such an approach – it embraces legitimate non-privacy objectives and accommodates them, in an innovative positive-sum manner.
- All interests and objectives must be clearly documented, desired functions articulated, metrics agreed upon and applied, and trade-offs rejected as often being unnecessary, in favour of finding a solution that enables multi-functionality.

Additional recognition is garnered for creativity and innovation in achieving all objectives and functionalities in an integrative, positive-sum manner. Entities that succeed in overcoming outmoded zero-sum choices are demonstrating first-class global privacy leadership, having achieved the Gold Standard.

5. End-to-End Security – 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.

Privacy must be continuously protected across the entire domain and throughout the life-cycle of the data in question. There should be no gaps in either protection or accountability. The "Security" principle has special relevance here because, at its essence, without strong security, there can be no privacy.

- **Security** – Entities must assume responsibility for the security of personal information (generally commensurate with the degree of sensitivity) throughout its entire lifecycle, consistent with standards that have been developed by recognized standards development bodies.
- **Applied security** standards must assure the confidentiality, integrity and availability of personal data throughout its lifecycle including, *inter alia*, methods of secure destruction, appropriate encryption, and strong access control and logging methods.

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 both users and providers alike. Remember, trust but verify!

Visibility and transparency are essential to establishing accountability and trust. This PbD principle tracks well to Fair Information Practices in their entirety, but for auditing purposes, special emphasis may be placed upon the following FIPs:

- **Accountabilty** – The collection of personal information entails a duty of care for its protection. Responsibility for all privacy-related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual. When transferring personal information to third parties, equivalent privacy protection through contractual or other means shall be secured.

- **Openness** – Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

- **Compliance** – Complaint and redress mechanisms should be established, and information communicated about them to individuals, including how to access the next level of appeal. Necessary steps to monitor, evaluate, and verify compliance with privacy policies and procedures should be taken.

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 best *Privacy by Design* results are usually those that are consciously designed around the interests and needs of individual users, who have the greatest vested interest in the management of their own personal data.

Empowering data subjects to play an active role in the management of their own data may be the single most effective check against abuses and misuses of privacy and personal data. Respect for User Privacy is supported by the following FIPs:

- **Consent** – The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

- **Accuracy** – personal information shall be as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.

- **Access** – Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

- **Compliance** – Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal.

- *Respect for User Privacy* goes beyond these FIPs, and extends to the need for human-machine interfaces to be human-centered, user-centric and user-friendly so that informed privacy decisions may be reliably exercised. Similarly, business operations and physical architectures should also demonstrate the same degree of consideration for the individual, who should feature prominently at the centre of operations involving collections of personal data.

Appendix A: *The 7 Foundational Principles*

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***

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 – 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

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.

Appendix B: The Global Privacy Standard

The objective of the Global Privacy Standard was to create a single harmonized set of universal privacy principles, reflecting the best of those found in various sets of fair information practices presently in existence.

The Global Privacy Standard, tabled and accepted on November 3, 2006, at the 28th International Data Protection and Privacy Commissioners Conference, draws upon the collective knowledge and practical wisdom of the international data protection community, and presents it in a single, easily understood, standard format.

Scope

The Global Privacy Standard (GPS) reinforces the mandate of privacy and data protection authorities by:

- focusing attention on fundamental and universal privacy concepts;
- widening current privacy awareness and understanding;
- stimulating public discussion of the effects of new information and communication technologies, systems, standards, social norms, and laws, on privacy; and
- encouraging ways to mitigate threats to privacy.

The GPS informs developers and users of new technologies and systems that manage or process information. The GPS may be particularly useful when developing information and communication technology standards, specifications, protocols, and associated conformity assessment practices.

The GPS can assist public policymakers when considering laws, regulations, programs and the use of technologies that may impact privacy. The GPS can equally assist businesses and developers of technology that may have an impact on privacy and personally identifiable information.

The GPS addresses privacy concerns for decision-makers in any organization that may have an impact on the way in which personal information is collected, used, retained, and disclosed.

The GPS is intended to complement not pre-empt or contradict any existing laws or legal requirements bearing upon privacy and personal information, in various jurisdictions.

GPS Privacy Principles

1. Consent

The individual's free and specific consent is required for the collection, use or disclosure of personal information, except where otherwise permitted by law. The greater the sensitivity of the data, the clearer and more specific the quality of the consent required. Consent may be withdrawn at a later date.

2. Accountability

Collection of personal information entails a duty of care for its protection. Responsibility for all privacy related policies and procedures shall be documented and communicated as appropriate, and assigned to a specified individual within the organization. When transferring personal information to third parties, organizations shall seek equivalent privacy protection through contractual or other means.

3. Purposes

An organization shall specify the purposes for which personal information is collected, used, retained and disclosed, and communicate these purposes to the individual at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.

4. Collection Limitation

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.

5. Use, Retention, and Disclosure Limitation

Organizations shall limit the use, retention, and disclosure of personal information to the relevant purposes identified to the individual, except where otherwise required by law. Personal information shall be retained only as long as necessary to fulfill the stated purposes, and then securely destroyed.

6. Accuracy

Organizations shall ensure that personal information is as accurate, complete, and up-to-date as is necessary to fulfill the specified purposes.

7. Security

Organizations must assume responsibility for the security of personal information throughout its lifecycle consistent with the international standards that have been developed by recognized standards development organizations. Personal information shall be protected by reasonable safeguards, appropriate to the sensitivity of the information (including physical, technical and administrative means).

8. Openness

Openness and transparency are key to accountability. Information about the policies and practices relating to the management of personal information shall be made readily available to individuals.

9. Access

Individuals shall be provided access to their personal information and informed of its uses and disclosures. Individuals shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

10. Compliance

Organizations must establish complaint and redress mechanisms, and communicate information about them to the public, including how to access the next level of appeal. Organizations shall take the necessary steps to monitor, evaluate, and verify compliance with their privacy policies and procedures.

www.ipc.on.ca/images/Resources/gps.pdf

Appendix C: The Mapping of FIPs onto the 7 Foundational Principles

Privacy by Design **Foundational Principles**	***Fair Information Practice*** **Principle (GPS)**	**Extended Principles**
1. Proactive not Reactive; Preventative not Remedial		Demonstrable commitment to set and enforce high privacy standards. Evidence that methods to **recognize** poor privacy designs, to **anticipate** poor privacy practices and outcomes, and to correct the negative impacts proactively are established
2. Privacy as the Default	3. Purpose Specification 4. Collection Limitation, Data Minimization 5. Use, Retention and Disclosure Limitation	Privacy as the default starting point for designing and operating information technologies and systems represents the maximum personal privacy that one can have. That is, privacy becomes the prevailing condition - without the data subject ever having to ask for it - no action required.
3. Privacy Embedded into Design		Systemic program or methodology in place to ensure that privacy is thoroughly integrated into operations. It should be standards-based and amenable to review and validation All privacy threats and risks should be identified and mitigated to the fullest extent possible in a documented action plan.
4. Full Functionality – Positive-Sum, not Zero-Sum		All legitimate non-privacy interests and objectives are identified early, desired functions articulated, agreed metrics applied, and unnecessary trade-offs rejected in favour of achieving multi-functional solutions
5. End-to-End Security – Lifecycle Protection	7. Security	
6. Visibility and Transparency	2. Accountability 8. Openness 10. Compliance	
7. Respect for User Privacy	1. Consent 6. Accuracy 9. Access	

Notes:

Revised: October 2010
Originally Published: May 2010

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario • CANADA • M4W 1A8

Telephone: 416-326-3333 • 1-800-387-0073
Facsimile: 416-325-9195
Web: www.ipc.on.ca • www.privacybydesign.ca
E-mail: info@ipc.on.ca