Fred Carter

Senior Policy & Technology Advisor
IPC Ontario

Information Privacy Engineering

SC/CSE 3000 Computer Ethics

York University, Keele Campus

13 October 2015

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

Overview / Objectives

What is Privacy?

What Threatens Privacy?

Solution: Privacy Engineering

Who We Are

Commissioner Brian Beamish

- Appointed by Ontario Legislature
- Independent from government
- Oversees 3 privacy & access to information laws

Mandated to:

- Investigate privacy complaints
- Resolve appeals of decisions related to providing access to information
- Ensure organizations comply with the access and privacy provisions of the acts
- Educate public about Ontario access and privacy laws
- Conduct research on access /privacy issues
- Provide advice and comment on proposed government legislation & programs

What is Privacy?

- **Information privacy** refers to the right or ability of individuals to exercise control over the collection, use, retention and disclosure of their personal information by others
- **Personally-identifiable information ("PII")** can be biographical, biological, genealogical, historical, transactional, locational, relational, computational, vocational or reputational, and is the stuff that makes up our modern identity

Personal information must be managed responsibly. When it is not, accountability is undermined and confidence in our information society is eroded.

Privacy Challenges

- Social ● Mobile ● Cloud ● IoT ● Big Data
- Oceans of (Personal) Data
- Global Scale
- Network Complexity, Opaque Data Flows
- Personalization, Profiling, Discrimination
- Identity Theft
- Loss of *information Self-Determination*

Privacy Crises

- **Fraud and security concerns** are inhibiting confidence, trust, and the growth of e-commerce and digital government
- **Fears of surveillance** and excessive collection, use and disclosure of personal information by others are also diminishing confidence and use
- **Lack of individual user empowerment and control** over one's own personal data is diminishing confidence and use
- **Function creep, power asymmetries, discrimination, *harm***

Privacy Responses

- **Consumer**
  - Avoidance
  - Privacy Enhancing Technologies
- **Organizational**
  - Adherence to standards
  - Professionalization of privacy
- **Legal**
  - Breach disclosure / reporting
  - Contracts, remedies, Safe Harbour

Principles of Fair Information Practices (FIPPs)

- Based upon the **1980 OECD principles**:
  - **Collection limitation**
    - PIPEDA: Knowledge and consent
  - **Data quality**
  - **Purpose specification**
  - **Use limitation**
  - **Security safeguards**
  - **Openness**
  - **Individual participation**
    - PIPEDA: Individual access and challenging compliance
  - **Accountability**

Meta Principles

• Safeguards	**Safeguards**
• Purpose Specification • Collection Limitation • Limits on Use, Retention and Disclosure	**Data Minimization**
• Consent • Accuracy • Access • Redress	**User Participation**
• Accountability • Openness • Challenging compliance	**Accountability (beyond data subject)**

Safeguards

Organizations are responsible for the security of personal information in their custody, consistent with its sensitivity and recognized standards and benchmarks.

- **Applied security standards** must assure the confidentiality, integrity and availability of personal information from creation to destruction and include, *inter alia*,
  - use of strong encryption
  - appropriate access controls
  - logging and audit controls

Safeguards

- **Encrypt by Default:** Whether at rest, in transit, or in use, data should be protected, by default
- **Authenticate Privileges, Not Identities:** Seek privacy enhanced identity, authentication and access controls
- **Trust, But Verify:** Activity monitoring, logging and auditing are credible deterrents but should not introduce new privacy risks

Data Minimization

- **Purpose Specification** – purposes for collection, use, retention and disclosure shall be communicated at or before the time the information is collected. Specified purposes should be clear, limited and relevant to the circumstances.
- **Collection Limitation** – collection of personal information must be fair, lawful and limited to that which is necessary for the specified purposes.
- **Data Minimization** – collection of personal information should be kept to a strict minimum. Design of programs, information technologies, and systems should begin with non-identifiable interactions and transactions as the default. Wherever possible, identifiability, observability and linkability 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.

Data Minimization

- **Just Say No:** The first line of privacy defence is always non-collection, non-retention and non-use of PII
- **Process at the Edge:** Shift data processing away from the center to the periphery / user-controlled devices
- **Distribute Processing:** Data processing functions and roles should be split to defeat linkage, aggregation and collusion
- **Default settings** should be maximally privacy-enhancing

User Participation

- **Consent** – The individual's free and specific consent is required for the collection, use, retention 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. Human-machine interfaces should be user-centric and person-friendly so that informed privacy decisions may be reliably exercised.
- **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.
- **Transparency** – Organizations must establish complaint and redress mechanisms and communicate them to the public, including how to access the next level of appeal.

User Participation

- **Anticipate and Inform:** Technologies, operations and networks should be designed with user privacy interests in mind, and convey privacy attributes to users in a timely, useful, and effective way
- **Support User Input and Direction:** Technologies, operations and networks should allow users to express their privacy preferences and controls in a persistent and effective way
- **Encourage Direct User Access:** Technologies, operations and networks should be designed to provide users direct access to data held about them, and an account of uses and disclosures

Accountability

The collection of personal information entails a duty of care to protect it. Responsibility for privacy-related policies and procedures shall be documented and communicated, 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.
- **Challenging 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 law, privacy policies and procedures should be taken.

Accountable Processes

- **Open Collaboration:** Privacy requirements, risks, methods and outcomes should be documented throughout the project lifecycle and communicated to project participants
- **Open to Review:** The design and operation of technologies, operations and networks should demonstrably satisfy the strongest privacy laws, contracts, policies and norms
- **Tell the World:** The design and operation of privacy-enhanced information technologies and systems should be open to scrutiny, praise and emulation by all

Proactive Leadership

Adopt strong privacy practices early and consistently

- **Leadership**: A clear commitment, at the highest levels, to prescribe and enforce high standards of privacy protection, generally higher than prevailing legal requirements
- **Community of Practice**: Demonstrated privacy commitment shared by organization members, user communities and stakeholders
- **Proactive and iterative**: Continuous processes to identify privacy and data protection risks arising from poor designs, practices and outcomes, and to mitigate unintended or negative impacts in proactive, systematic, and innovative ways

Systemic, Verifiable Methods

- **Holistic, Integrative and Creative**: Privacy commitments must be embedded in holistic, integrative, and creative ways
- **Systematic and Auditable:** A systematic, principled approach should be adopted that relies upon accepted standards and process frameworks, and amenable to external review
- **Review and Assess:** Detailed privacy impact and risk assessments should be used as a basis for design decisions
- **Human-Proof:** The privacy risks of information technologies, processes, and networks should be demonstrably minimized, and not degraded through use, misconfiguration, or error

Full Functionality/ Quantitative Results

- **No Loss of Functionality:** Embedding privacy should not impair functionality of a given technology, process or network architecture
- **Legitimate Objectives Accommodated**: All interests and objectives must be documented, desired functions articulated, metrics agreed, and trade-offs rejected, when seeking a solution that enables multi-functionality
- **Practical and Demonstrable Results**: Optimized outcomes should be published for others to emulate and become best practice.

Summary

- Management of (personal) information is a growth industry!
- Trust is real currency – we need to go beyond compliance mentality to embrace richer privacy objectives, tools, and processes
- There is a market for privacy engineering in the consumer and enterprise spaces
- Engineers can apply FIPPs to information and communication technologies, organizations, and architectures in holistic, robust, and verifiable ways
- Be leaders: set new “best-in-class” benchmarks


Questions
PRIVACY
???
&5DF?W$
SYBASE
IP
LOGIN
ORACLE
SSL
105254
28

Contact

Office of the
Information & Privacy Commissioner of Ontario

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

1-416-326-3333 / 1-800-387-0073
www.ipc.on.ca | {Firstname.Lastname}@ipc.on.ca