Privacy by Design in the Clouds: You Can't Outsource Accountability

David Goodis

Director of Legal Services

Office of the Information and Privacy Commissioner, Ontario

Centre for Innovation Law and Policy
University of Toronto – Faculty of Law

October 14, 2011

The 21st Century Privacy Challenge

The Power and Promise of Cloud Computing:

- Limitless flexibility;
- Better reliability and security;
- Enhanced collaboration;
- Portability;
- Simpler devices.

The Cloud and Privacy Concerns

- **Fraud and security concerns** are inhibiting confidence, trust, and the growth of e-commerce, e-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**

Privacy by Design Meets the Cloud: Current and Future Privacy Challenges

- What is Privacy by Design? building privacy into technology from the ground up
- The goal is to establish ***trust*** in:
  - Data (that travels through the cloud);
  - Personal devices (that interact with cloud-based services);
  - Software;
  - Service providers.

Privacy by Design:
The 7 Foundational Principles

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**.

PbD

www.privacybydesign.ca

Privacy by Design

The 7 Foundational Principles

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

Privacy by Design is a concept I developed back in the 90's, to address the ever-growing and systemic effects of Information and Communication Technologies, and of large-scale networked data systems.

Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.

Initially, deploying Privacy-Enhancing Technologies (PETs) was seen as the solution. Today, we realize that a more substantial approach is required — extending the use of PETs to PETS *Plus* — taking a positive-sum (full functionality) approach, not zero-sum. That's the "*Plus*" in PETS *Plus*: positive-sum, not the either/or of zero-sum (a false dichotomy).

Privacy by Design extends to a "Trilogy" of encompassing applications: 1) IT systems; 2) accountable business practices; and 3) physical design and networked infrastructure.

Principles of *Privacy by Design* may be applied to all types of personal information, but should be applied with special vigour to sensitive data such as medical information and financial data. The strength of privacy measures tends to be commensurate with the sensitivity of the data.

The objectives of *Privacy by Design* — ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage — may be accomplished by practicing the following 7 Foundational Principles *(see over page)*:

www.ipc.on.ca/images/Resources/7foundationalprinciples.pdf

Privacy by Design Meets the Cloud: Outsourcing

- Cloud computing services present similar privacy challenges to outsourcing: Where is the personal data? Which jurisdiction and laws apply? Who is accountable for the data and its uses? Is there effective oversight?

Some things to consider:

- Conduct a Privacy Impact Assessment;
- Only use identifying information when necessary;
- Identify and minimize privacy and security risks;
- Use privacy enhancing technological tools;
- Exercise due diligence;
- Ensure transparency, notice, education & awareness;
- Develop a privacy breach management plan;
- Create and enforce contractual clauses.

Contractual Provisions to Consider when Outsourcing to Other Jurisdictions

- Require the service provider to agree not to use personal information to which it has access except as necessary in the course of providing services;
- Require the service provider to agree not to disclose personal information to which it has access in the course of providing services;
- Set out the administrative, technical and physical safeguards that must be employed by the service provider to ensure that records of personal information are retained, transferred and disposed of in a secure manner;
- Require the service provider to notify the organization, at the first reasonable opportunity, of any summons, order or similar requirement to compel production of the information issued outside Canada;
- Require the service provider to notify the organization, at the first reasonable opportunity, if the personal information is stolen, lost or accessed by unauthorized persons;
- Require the establishment of an oversight and monitoring program, including audits of the service provider's compliance with the terms of the agreement; and
- Prohibit the service provider from permitting its employees or any person acting on its behalf from having access to the personal information unless the employee or person acting on its behalf agrees to comply with the restrictions set out in the agreement.

You can outsource services …

… but you can't outsource accountability.

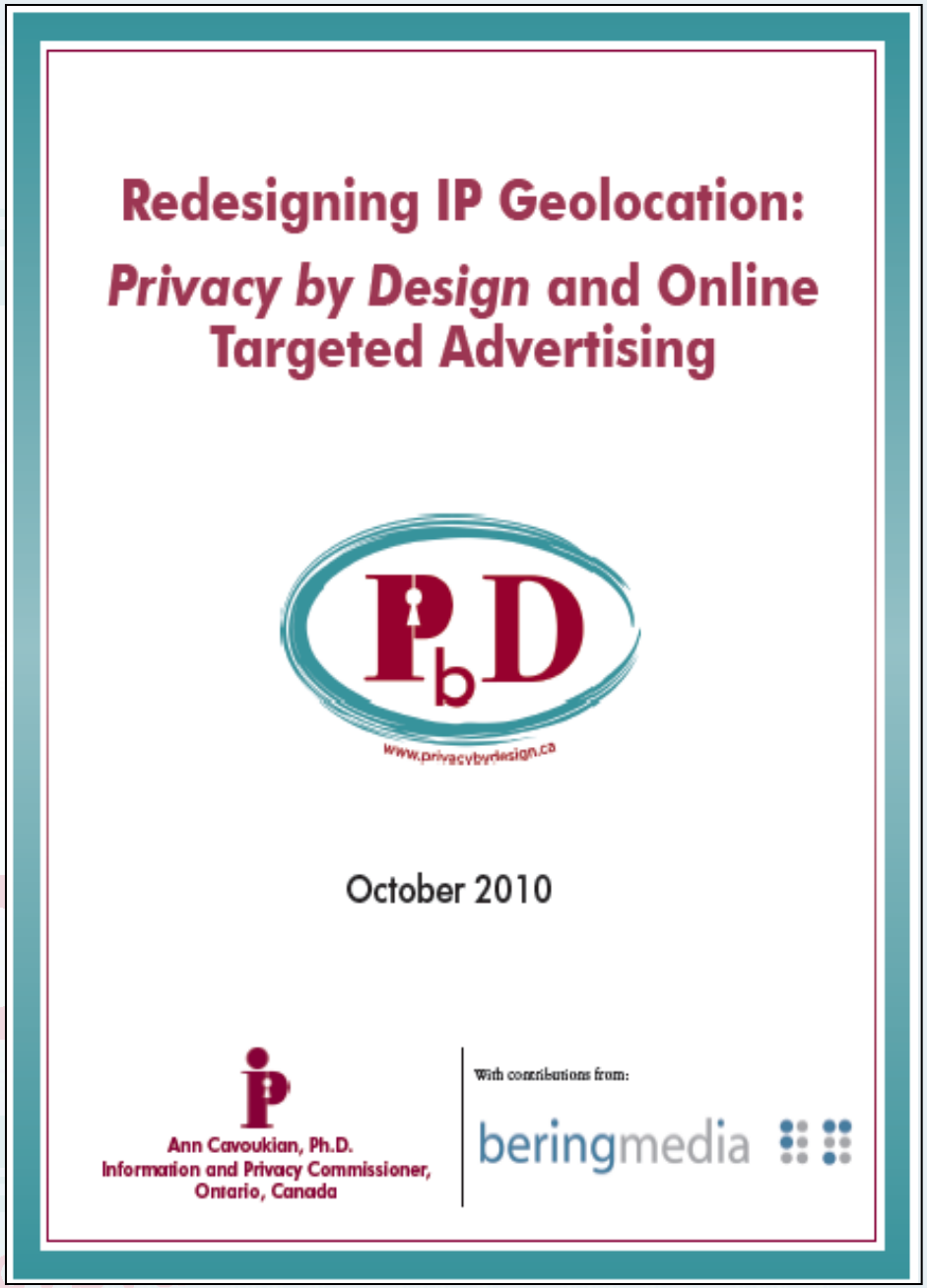
You always remain accountable.

USA *Patriot Act* and Cloud Computing

- The Dutch Minister of Safety has recently voiced concerns about U.S. cloud providers operating in the Netherlands due to requirements of the *Patriot Act*;
- British Columbia and Nova Scotia have enacted restrictive legislation on the government's ability to outsource beyond Canadian border;
- There will always be laws that allow law enforcement to gain access to information in their jurisdictions – the important question is what steps can an organization take to help ensure privacy and security, regardless of jurisdiction;
- Organizations considering outsourcing or cloud computing should ensure accountability through appropriate contractual provisions and a *Privacy by Design* approach that ensures privacy is built in as an integral part of the proposed technologies and business practices.

Privacy by Design in Action

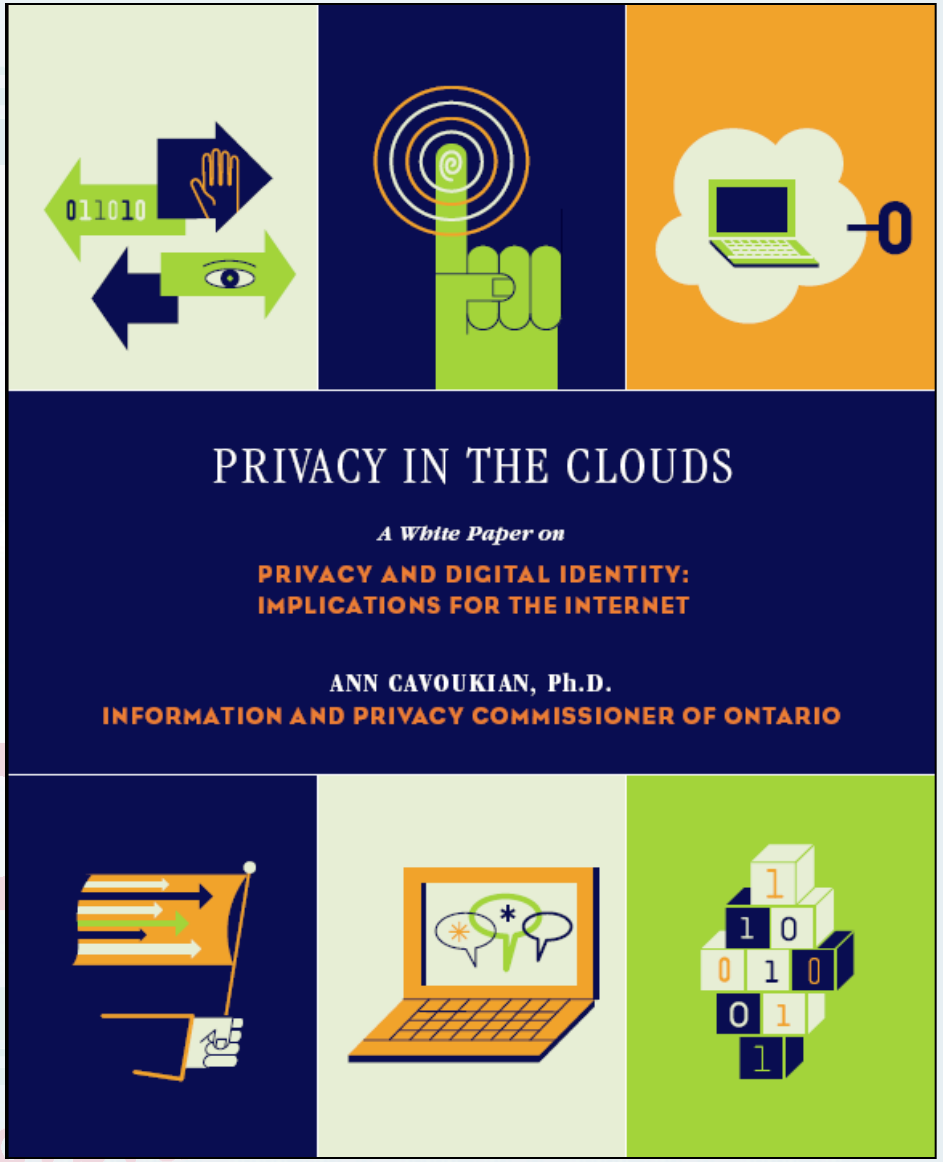
- **Bering Media** has built Privacy into IP Geolocation:
- Using a unique double-blind privacy architecture;
- With minimum-match thresholds/ Anti-inference algorithms;
- Dynamic IP address management;
- Persistent, permanent opt-out.



www.ipc.on.ca/images/Resources/pbd-ip-geo.pdf

Privacy in the Clouds

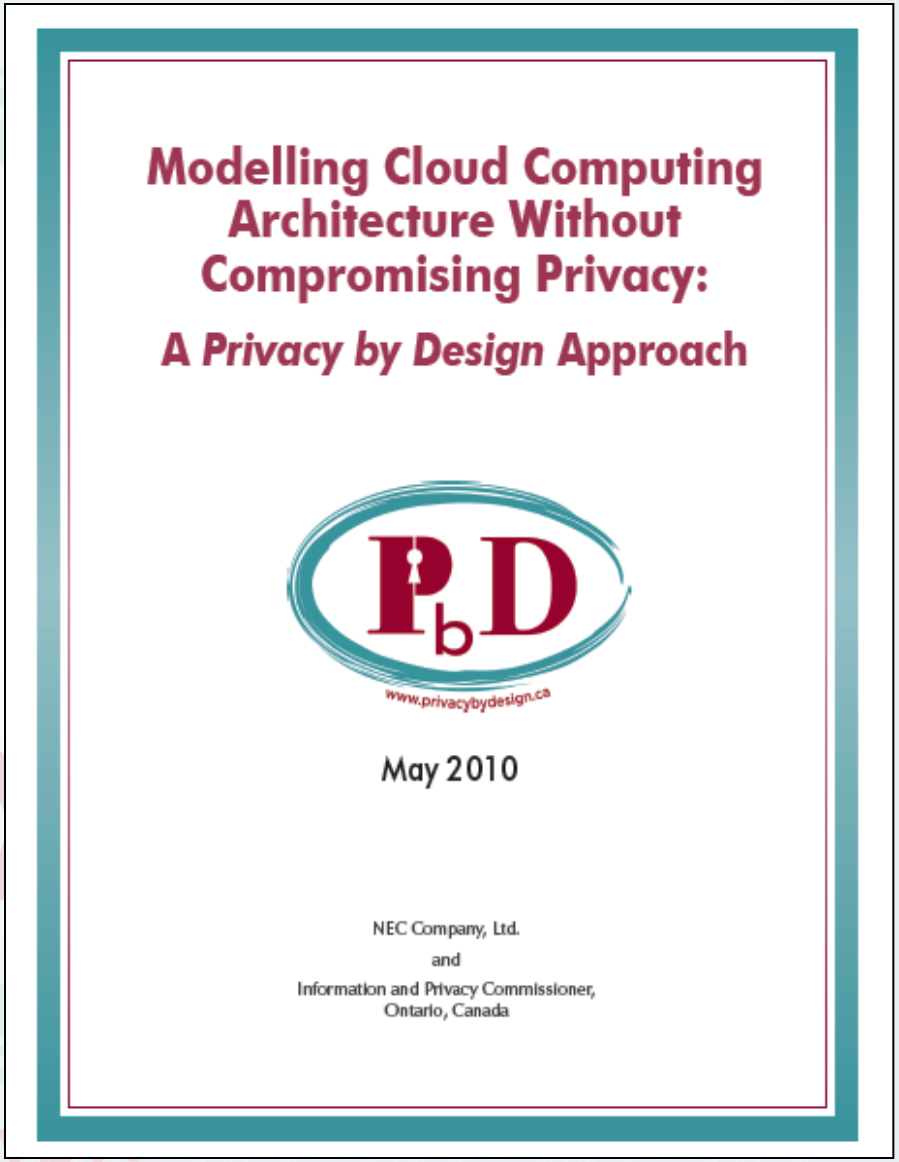
- The 21st Century Privacy Challenge;
- Creating a User-Centric Identity Management Infrastructure;
- Using Technology Building Blocks;
- A Call to Action.



www.ipc.on.ca/images/Resources%5Cprivacyintheclouds.pdf

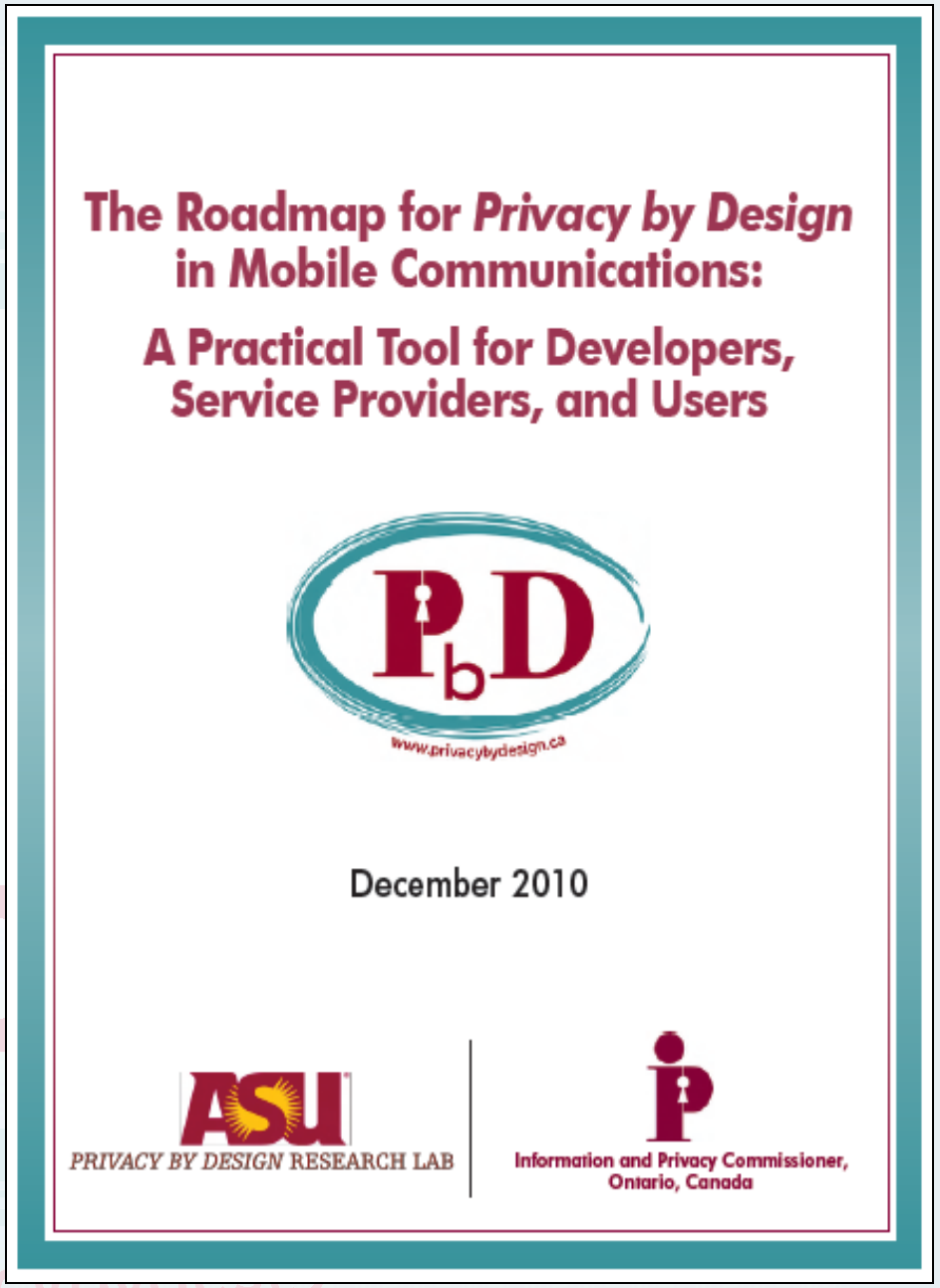
Cloud Computing Architecture and Privacy

- Cloud Delivery Models
- Use cloud in privacy protective manner – user control
- e.g. encryption, segregation



www.ipc.on.ca/images/Resources/pbd-NEC-cloud.pdf

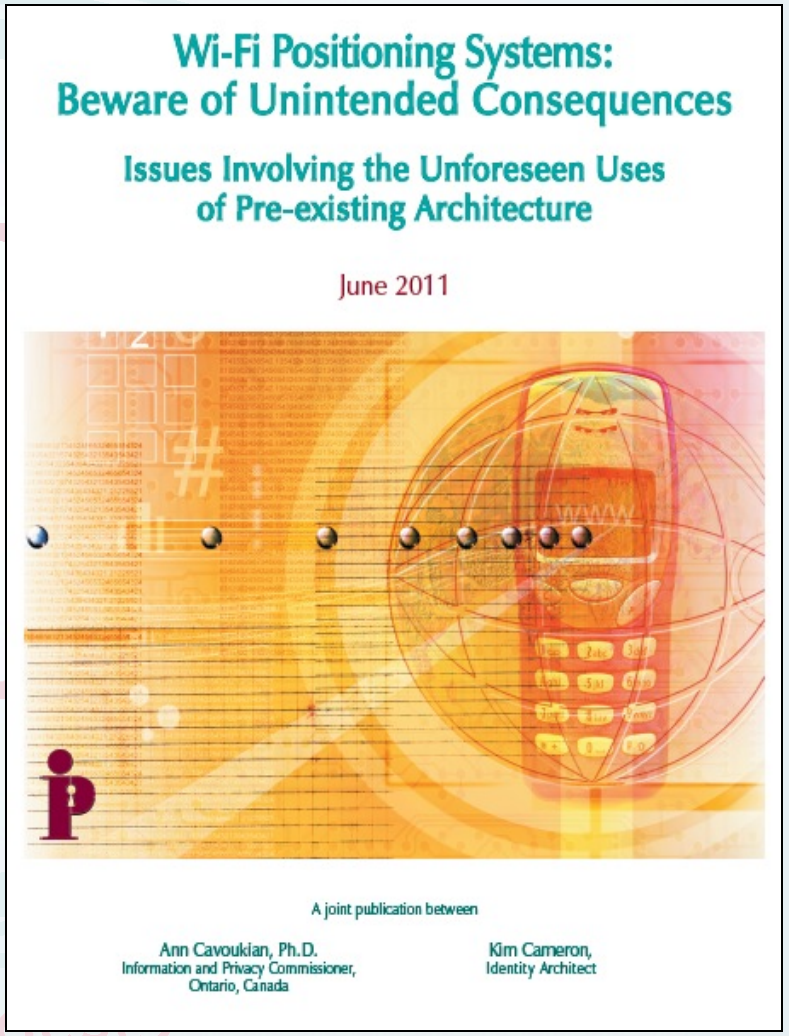
- Widespread Adoption of Mobile Communications Technology;
- Privacy and Mobile Communications;
- Roadmap for *PbD* in the Mobile Communications Industry:
  - Device Manufacturers;
  - OS/Platform & Application Developers;
  - Network Providers.



www.privacybydesign.ca/content/uploads/2011/02/pbd-asu-mobile.pdf

Wi-Fi Positioning Systems: Beware of Unintended Consequences

- Advances in location-based technology and services;
- Overview of major mobile positioning systems;
- Wi-Fi Positioning System "location aggregators;"
- *Privacy by Design*: Removing the "Informant" from WPS Location Architecture.



www.privacybydesign.ca

Conclusions

- **Lead with *Privacy by Design;***
- **Change the paradigm from the dated "zero-sum" to the doubly-enabling "positive-sum;"**
- **Deliver *both* privacy AND security or any other functionality, in an empowering "win-win" paradigm;**
- **Build *PbD* into the Cloud infrastructure;**
- **Embed privacy as a core functionality: the future of privacy may depend on it.**

How to Contact Us

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner of Ontario

2 Bloor Street East, Suite 1400

Toronto, Ontario, Canada

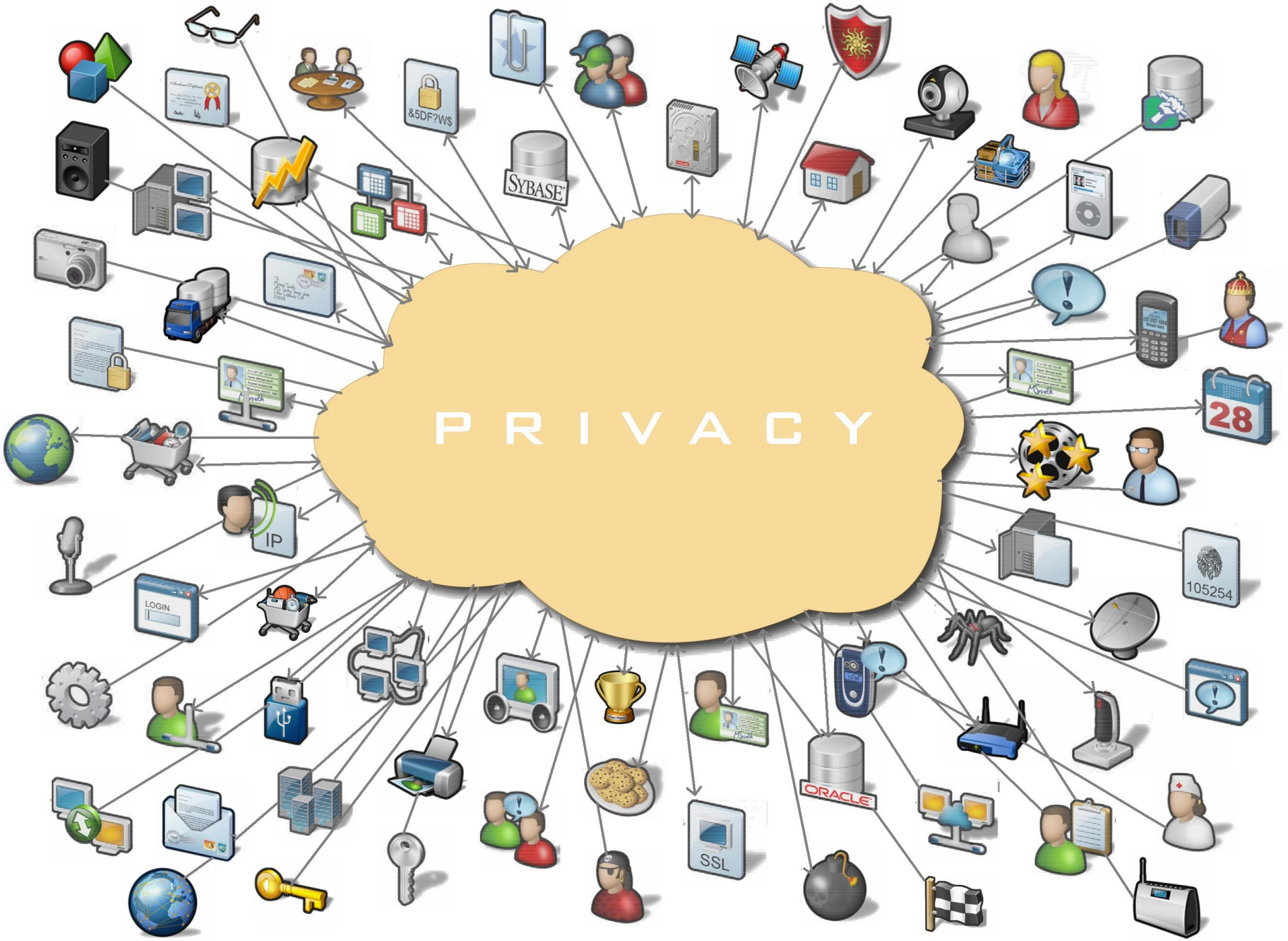
M4W 1A8

Phone: (416) 326-3948 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca

For more information on *Privacy by Design*, please visit: www.privacybydesign.ca


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