Can You Read Me Now?
The Privacy Implications of RFID

Ann Cavoukian, Ph.D.

Information & Privacy Commissioner/Ontario

International Association of Privacy Professionals
KnowledgeNet Toronto
March 13, 2007

IPC

Presentation Outline

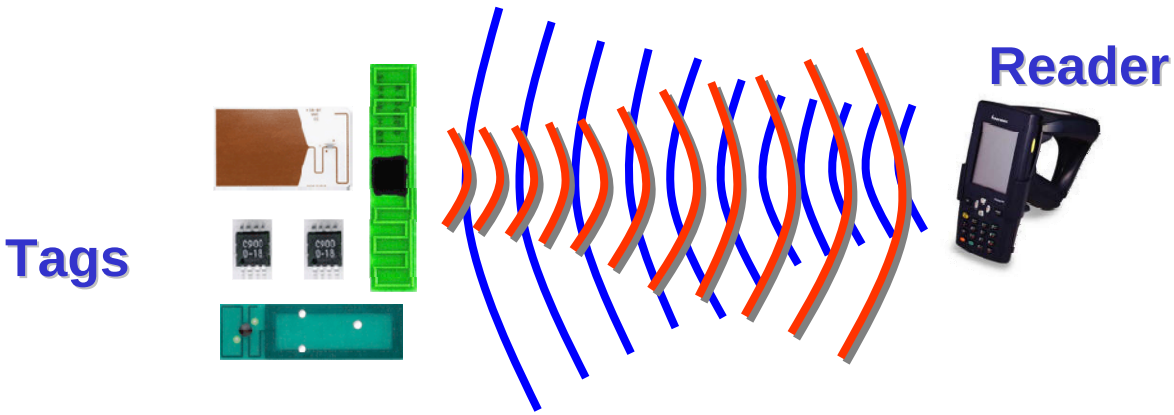
1. *What is an RFID?*
2. *RFID and Consumers*
3. *Supply-Chain vs. Item-Level RFID*
4. *Legislation and Regulation*
5. *Proposed Solutions*
6. *IPC RFID Guidelines*
7. *Good Privacy is Good Business*
8. *Conclusion*

IPC

What is an RFID?

IPC

RFID: What Is It? (Cont'd)



- RFID tags are affixed to objects and stored information may be written and rewritten to an embedded chip in the tag;
- Tags can be read remotely when they detect a radio frequency signal from a reader over a range of distances;
- Readers either send tag information over the enterprise network to back-end systems for processing or display it to the end user.

Properties of RFID Systems

- RFID systems are *information* systems;
- RFID tags contain a *unique object identifier*;
- Data from RFID tags can be collected remotely and automatically – without any user knowledge;
- *Time* and *location* data may also be collected.

Benefits of RFIDs

RFID Technology promises many benefits:

- More efficient tracking, tracing of goods through the supply chain; reduced inventory "shrinkage;"
- Improved business process efficiencies and reduced labor costs (e.g., no manual scanning of individual items required);
- Better detection of counterfeit, fraud;
- Better post-sale service for consumers: returns, exercising product warranties, responding to recalls, etc.

IPC

RFID Applications

RFID Addresses Many Usage Scenarios

Supply Chain Management		Leverage RFID technologies to transform supply chains by providing end-to-end visibility of goods and enabling improved inventory management.
Work In Process Manufacturing		Apply RFID technologies to the in process manufacturing processes to enable effective inventory tracking and management, product line efficiencies, and JIT manufacturing advantages.
Asset Management		Companies have physical assets (plants, truck fleets, PCs etc) that are needed to make, and to deliver products and services to customers - knowing where an item or vehicle is on route, tracking depreciation of goods – tools, equipment, leased items.
Security & Access Control		Monitor the movement and use of valuable equipment and personal resources.
Consumer Applications		Monitoring peoples movements, personal security, convenience and Point of sale applications.

One of Many Benefits of RFIDS: *Health Care: Pharmaceuticals*

- Tracking the pedigree of pharmaceutical products;
- Confidence relating to drug pedigree (re: statement of origin), is becoming increasingly important;
- Tracking and inventory of patient specimens (blood samples, test tubes, etc.);
- Tracking and inventory of pharmaceutical equipment.

IPC

RFID and Consumers

IPC

Consumer Deployments

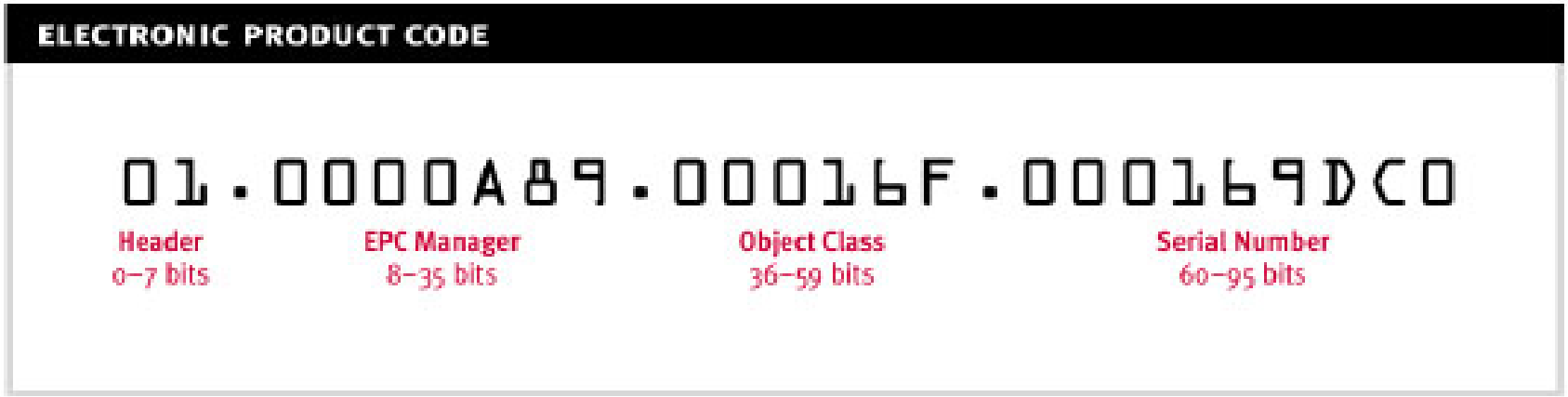
- **Limited deployment in the next 5 years:**
  - Retail item-level: limited deployment on pilot basis only, for certain high-value items (e.g. electronics);
  - Convenience services (payment systems, e.g., MasterCard PayPass, Exxon/Mobil Speedpass,;
  - Identification and access control: loyalty and access cards, ignition immobilizer; VeriChip
  - Consumer Safety: for recalls, recycling, etc.

RFID Privacy Challenges

- **Perceived Lack of Transparency, Consumer Trust:**
- RFID technology, current uses, still not well known or understood by public. Public opinion on RFID still developing; highly volatile;
- Perceived as a privacy issue: public concerns about possible surveillance, secondary and unethical data uses;
- Lack of consumer voice, input; possibility of backlash;
- Need to be proactive, **take action now**.

Privacy and RFIDs

- RFID tags contain information about products, not people:



- Despite that, many consumers perceive a threat to privacy – ***why?***

IPC

Consumer Perceptions

- **Consumers perceive that RFID may facilitate tracking and surveillance:**
  - Carried items may be surreptitiously tracked;
  - Tagged items can be linked to the individual;
  - Linked data assembled into profiles may be used in unaccountable ways;
  - RFID data can be stolen and cloned: a formula for identity theft;
  - The consumer is not a participant;
  - More transparency and accountability needed.

The Background

- **2003, Benetton** – Italian clothier sparked a furor after it announced plans to implant RFID tags in its apparel;
- **2004, Metro AG** – Began issuing loyalty cards with RFID chips embedded – did not tell consumers; triggered a worldwide boycott;
- **2004, Verichip** – Ethical and religious issues engaged by sub-dermal RFID implants and registration services.

Consumer Backlash
Auto-ID Centre, P&G Survey, 2001

How real are consumer concerns?

- 78% of respondents had a negative reaction to RFID use, with the majority claiming to be extremely or very concerned:
  - 90% of consumers did not want "smart tags" in their homes;
  - 83% thought the technology was beneficial;
  - The reassurance that the "tags" could be turned off and privacy guaranteed was not compelling.

http://cryptome.org/rfid/pk-fh.pdf

Get Ready for a Good Fight

- CASPIAN, a U.S.-based consumer rights group, claimed:
  - Checkpoint was developing RFID “spychips” for three well-known clothing labels;
  - Consumers wearing the tagged clothing could potentially be identified and tracked by readers;
  - “[We] will be working with consumers on an aggressive response to this privacy threat. Roll up your sleeves and get ready for a good fight.”
- **UK consumer group**: ThoughtCrime News: “RFID is not only the harbinger of heavy personal surveillance. It may bring an end to civilization as we know it.”

Supply-Chain vs. Item-Level RFID

IPC

Supply-Chain vs. Item-Level *The Difference*

- Every RFID tag contains unique-identifying data, such as a serial number;
- Privacy issues can arise when the RFID tag is associated with a specific item (rather than several items grouped together) ***and an identifiable individual (consumer);***
- **Supply-chain management**: involves tagging bulk goods, cases, pallets. Also some individual products for business uses in manufacturing, wholesale distribution, and for back-end retail inventory management purposes;
- **Item-level consumer product tagging**: involves tagging commercial products in the retail space that are owned, carried and used by individual consumers, such as apparel, electronics, and identity or payment cards.

Security Concerns

- As a wireless technology, RFID technology is still grappling with data security issues;
- Passive tags will respond automatically to any reader that interrogates them;
- Data on RFID tags are vulnerable to skimming, eavesdropping, cloning;
- RFID systems may also be vulnerable to jamming, denial of service, viruses, etc.

Legislation and Regulation

IPC

RFID Legislative Activity in the United States

- **Two*** states have passed bills that directly address RFID:
  - 2006 – New Hampshire (HB203)
  - 2006 – Wisconsin (AB290)
- An additional **five*** states have passed bills referring to RFID:
  - 2006 – New Hampshire (HB1738)
  - 2006 – Washington (HB2407)
  - 2005 – Wyoming (HB0258)
  - 2005 – California (AB1489)
  - 2002 – New Jersey (S573/S890)
- In 2006, **twenty-six*** bills were introduced dealing with RFID. In 2007, **twenty-four*** bills have been introduced.

IPC

* Estimated

Trends:
U.S. Bills Relating to RFIDs

Since January 2006, bills were introduced on the following issues:

- **Task Forces** (New York, Washington, Arkansas);
- **Consumer Privacy** (Illinois, Missouri, New York, Tennessee, Virginia, Arkansas, Washington, New Jersey, Massachussetts, New Hampshire);
- **Prescription Drug Packaging** (Federal);
- **Human Identification: Microchips in Individuals / Identification Documents / Other Tracking** (New Jersey, Ohio, Michigan, North Dakota, Oklahoma, Colorado, New Hampshire, California / Alabama, Illinois, Washington, California, New Hampshire / Rhode Island, Florida, New Hampshire, California, Washington, Georgia, West Virginia, Texas);
- These bills may be advancing through the legislative process, or they may be vetoed or stalled.

IPC

Canada
Legislative Landscape

Canadian Privacy Laws:

- In Canada, we prefer to pass general-purpose privacy laws, based upon Fair Information Principles, with oversight agencies/authorities;
- Canadian privacy laws are technology-neutral; little specific guidance to IT industry;
- *PIPEDA* is such a law: based upon the 10 principles of the CSA Privacy Code (Schedule 1);
- Emergence of substantially similar provincial privacy laws (AB, BC, QC) and Ontario for health, *PHIPA*.

Self-Regulation, Codes Best Practices, Standards

- ICAO standards for machine readable travel documents;
- Industry Standards: *e.g.* EPCglobal Canada;
- Advocacy Groups: *e.g.* EPIC, CDT, PRC;
- Oversight & regulatory guidance: *e.g.* FTC, EU, DPAs, IPC;
- Joint guidance: IPC-EPC RFID privacy guidelines.

www.ipc.on.ca/docs/rfidgdlines.pdf

Proposed Solutions

IPC

Restoring Privacy and Trust

Effective governance can come from:

- Industry self-regulation, codes of conduct, best practices, guidelines, standards, policies, etc;
- Technological solutions;
- Public education.

Technology

- Build privacy early into the design and operation of RFID information systems, e.g.: minimize linkages, access to PII;
- Ensure strong security controls on tag data, e.g. use encryption;
- Empower consumers to make privacy-enhancing decisions and actions, e.g. quick and easy de-activation of tags, with later possibility of re-activation.

Technology: “Build It In”

Embed privacy protective measures into the design and infrastructure of any new technology, including RFIDs.

IPC

Technology: Build It In (Cont'd)

- IBM Clipped Tag Solution;
- Backend "middleware" information systems, integration with legacy systems;
- Improved RFID tag security and privacy features;
- Privacy and security defaults can and should be built into RFID technologies.

Retail Privacy Solution: *De-activation*

- RFID tags should be deactivated at the point of sale, or when the consumer comes into contact with the tag (e.g., through blocking technology carried by the consumer or pervasive in the vicinity);
- Deactivation at point of sale should be the default, but it is not without its problems;
- Deactivation limits post-sale benefits of RFIDs.

Mechanical Destruction of an RFID Tag

- Provide RFID tag structures that permit a consumer to disable a tag by mechanically altering the tag in such a way as to inhibit the ability of a reader to interrogate the tag or transponder by wireless means:
  - Provides visual confirmation that tag has been deactivated;
  - May be read later on by mechanical contact if desired by consumer.

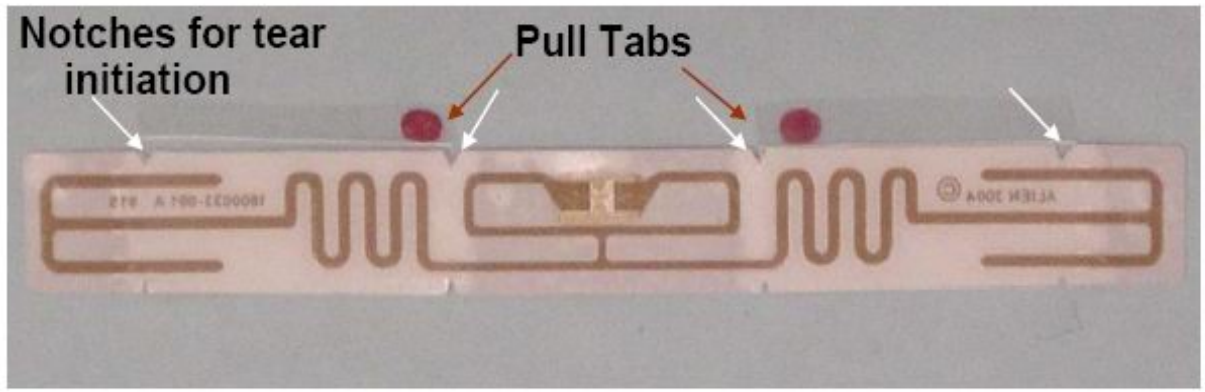
IPC

Consumer Disabled IBM Clipped Tag

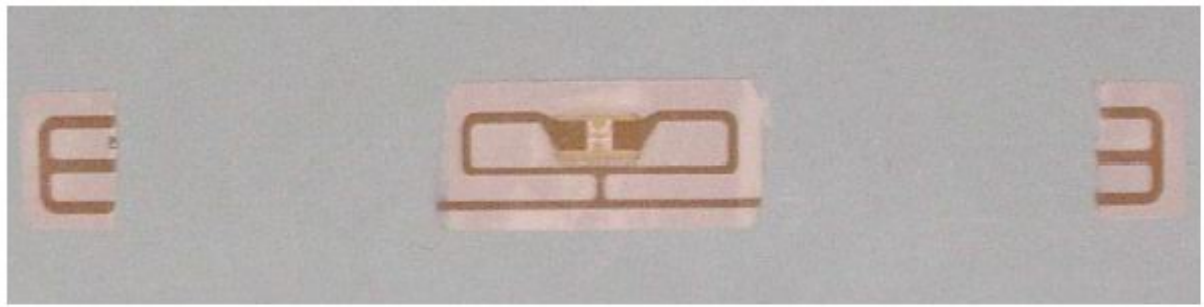
Clipped RFID Tags

- Implementation on real tags – the tag substrate can be perforated or notched for tear initiation

Before: Range is over 2 metres with handheld reader



After: Range is less than 5 cm with handheld reader



Scale: Tag length ~ 10 cm (4 inches)

Building Privacy Safeguards into RFID Systems

Technology solutions exist that can convey FIPs and ensure privacy:

- System designers, integrators and commercial adopters can *minimize* the collection & use of personally-identifiable data in RFID information systems, e.g.:
  - No personally-identifiable information (PII) is ever written to the RFID tags;
  - Readers cannot “resolve” or associate RFID tag data to PII;
  - There are built-in controls and limits on access to “lookup” databases
  - Read ranges are sharply limited;
  - Backend data transactions remain anonymous (or at least pseudonymous);
  - Backend information systems and databases are strongly segregated;
  - Interoperability of tags with other RFID systems is circumscribed.

IPC

Building Privacy Safeguards into RFID Systems (Cont'd)

Ensure strong security controls on tag data:

- Technology manufacturers can design RFID tags to maximize data protection and to minimize the risks of tag data being "leaked" or misused in an unauthorized manner:
- Tag data can be encrypted, masked or otherwise scrambled;
- Tags only responds to proprietary readers, using proprietary protocols;
- Wireless transmission of tag data is done in secure manner (i.e. shielded);

Building Privacy Safeguards into RFID Systems (Cont'd)

Ensure strong security controls on tag data (cont'd):

- Access to tag data, significance requires additional steps, such as use of password or access to lookup database;
- Tags can be "put to sleep" and/or "awoken" under specified conditions;
- Tags can be re-purposed for exclusive consumer uses and control;
- Tags can be killed or deactivated in convenient, verifiable manner.

Building Privacy Safeguards into RFID Systems (Cont'd)

Empower consumers and end-users to make privacy-enhancing decisions and actions:

- Involve consumers in the RFID information lifecycle process;
- Detect the presence and location of RFID tags and readers;
- Identify and disclose tag contents;
- Provide audio-visual confirmation of tag data queries, reads, and uses;
- Provide consumers with full access to any data associated with a given tag;
- Assign effective control over tag behaviour to consumers;
- Quickly and easily de-activate tags, either temporarily or permanently.

Education and Awareness

- Public opinion, consumer trust and confidence will impact market acceptance;
- Trusted public sources of information and expertise are vital for informed discussion;
- **Businesses need to get the message out that they are tracking products, not people;**
- Openness and transparency are key, pivotal on consent.

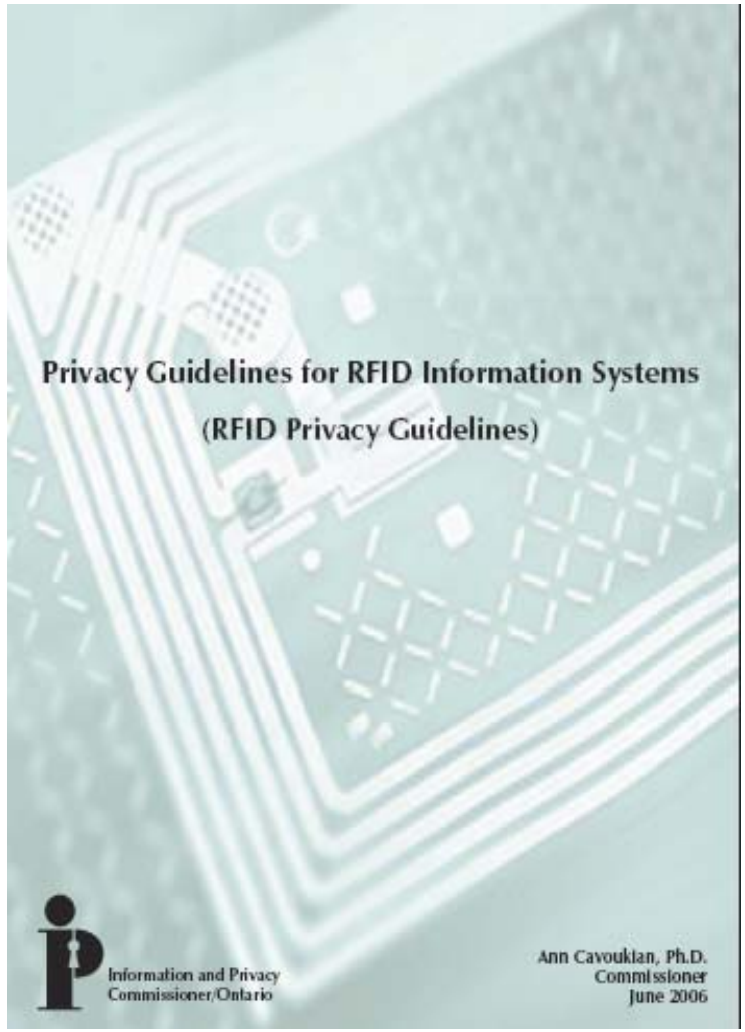
IPC RFID Privacy Guidelines

IPC

IPC RFID Privacy Guidelines

- Developed with leading industry standards-setting organization (GS1/EPCglobal Canada);
- Promotes compliance with Canadian federal and provincial privacy laws;
- Strongest, most complete set of RFID guidelines developed to date – promotes compliance and consumer trust around the world.

www.ipc.on.ca/docs/rfidgdlines.pdf



IPC RFID Privacy Guidelines

Scope of The Guidelines

- Based upon the 10 Fair Information Practices of the general-purpose CSA Privacy Code, which applies to all organizations, basis for privacy law in Canada;
- Focus on item-level tagged consumer goods;
- Limited to RFID-linked PII: data linkages considered to constitute personal info;
- Guidelines a reference for *all* RFID industry stakeholders, *e.g.* product manufacturers, hardware and software vendors, consumers – everyone must be part of privacy solutions.

IPC RFID Privacy Guidelines

Three Overarching Principles:

1. Focus on entire RFID information systems, not just tags/technology;

2. Privacy and Security Must be Built in from the Outset – at the Design Stage;

3. Maximal Individual Participation and Consent.

IPC

IPC RFID Privacy Guidelines

Based on the 10 Fair Information Practices

1. Accountability
2. Identifying Purposes
3. Consent
4. Limiting Collection
5. Limiting Use, Disclosure and Retention
6. Accuracy
7. Safeguards
8. Openness
9. Individual Access
10. Challenging Compliance

IPC

IPC and RFID
Next Steps

- Ongoing work with industry, associations, retailers on implementing the Guidelines;
- Input into EU and Canada RFID consultations;
- Urge broad use of Guidelines as reference point for design and adoption by industry players;
- Basis for industry self-regulation;
- Possible sector-specific guidance, e.g. health care; transportation; identification; implants.

Good Privacy is Good Business

IPC

The Bottom Line

Privacy should be viewed as a **business** issue, not a ***compliance*** issue

Privacy is Good for Business

- Evidence that firms are scaling back RFID trial and rollout plans pending clarification of the privacy and security questions;
- We're on the cusp of ubiquitous item-level tagging, so need to ensure privacy controls are built in early to the design and operation of the next generation of RFID-enabled applications;
- Good privacy is good business – can be a source of competitive advantage.

IPC

Privacy is Good for Business (Cont'd)

"One thing is certain: Technological advances will force changes in the laws around the globe that protect individual privacy. If you wait for these changes to become obvious, you will forfeit a powerful competitive advantage. People trust leaders, not followers. Once legislation creates new standards for appropriate behavior, the public will be drawn to companies that can claim to have followed such standards before they were mandatory."

— Bruce Kasanoff,

Making it Personal: How to profit from personalization without invading privacy.

Conclusion

- Strong need to address the public's concerns about privacy, in a proactive manner;
- Strong need to balance privacy with other interests - ***Practical Privacy****;*
- Ignoring privacy problems in the short-term, will only create bigger problems in the long-term;
- Build privacy into the design and implementation of RFID tags – ***"Privacy by Design;"***
- Immunize consumers against the extreme messaging advanced by some privacy fundamentalists;
- Follow universally accepted privacy principles;
- Be prepared for a ***"good fight."***

IPC

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) 326-3333 / 1-800-387-0073

Web: www.ipc.on.ca

E-mail: info@ipc.on.ca