



Can You Read Me Now?

The Privacy Implications of RFID

Fred Carter

Senior Policy & Technology Advisor

Information & Privacy Commissioner/Ontario

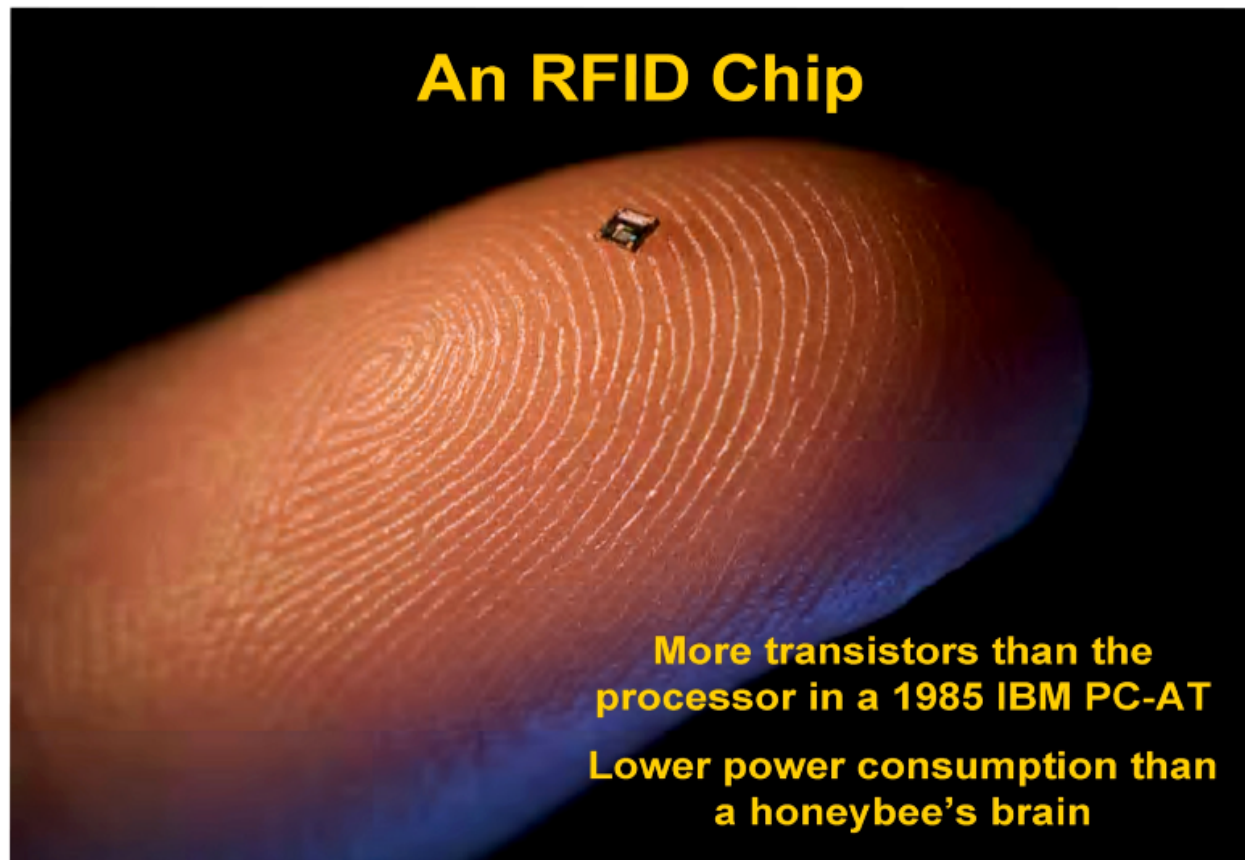
MGS Access & Privacy Conference

Toronto, Canada

September 15, 2006



RFID: What Is It?





RFID: What Is It?

(Radio Frequency Identifiers)

- A means of identifying a unique object using radio frequency transmission of data
- Tags (or transponders) store information, which can be transmitted wirelessly in an automated fashion
- Readers (or interrogators) both stationary and hand-held readers and/or write information from/to tags



RFID: What Is It?

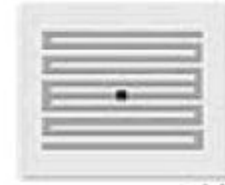
Inlays and Tags

Chip + Antennae + Substrate = Tag



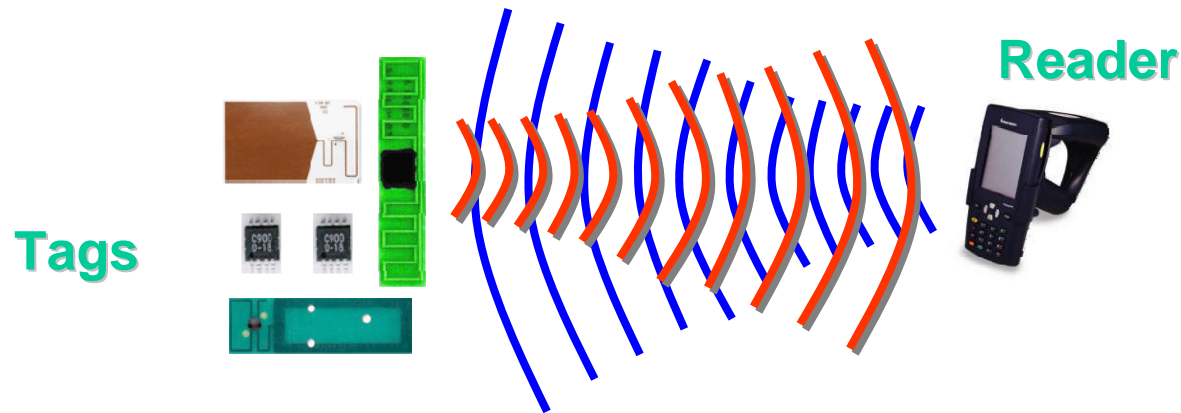
Chip

Antenna





RFID: What Is It?



- 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



RFID: What Is It?





RFID: What Is It?





RFID: What Is It?



Tag

- Embedded in devices or objects (e.g. handsets)
- RF data transfer with reader



Reader

- Receives & processes tag level data
- Writes data to active tags



Controller

- Aggregates/assembles data from multiple tags & readers
- Controls actuators based on RFID business rules



Local Computer

- Aggregates/assembles data from readers & controllers
- Executes RFID business processes
- Integrates to the enterprise



Enterprise IT System

- Executes enterprise business processes
- Integrates RFID data from multiple sites with enterprise apps



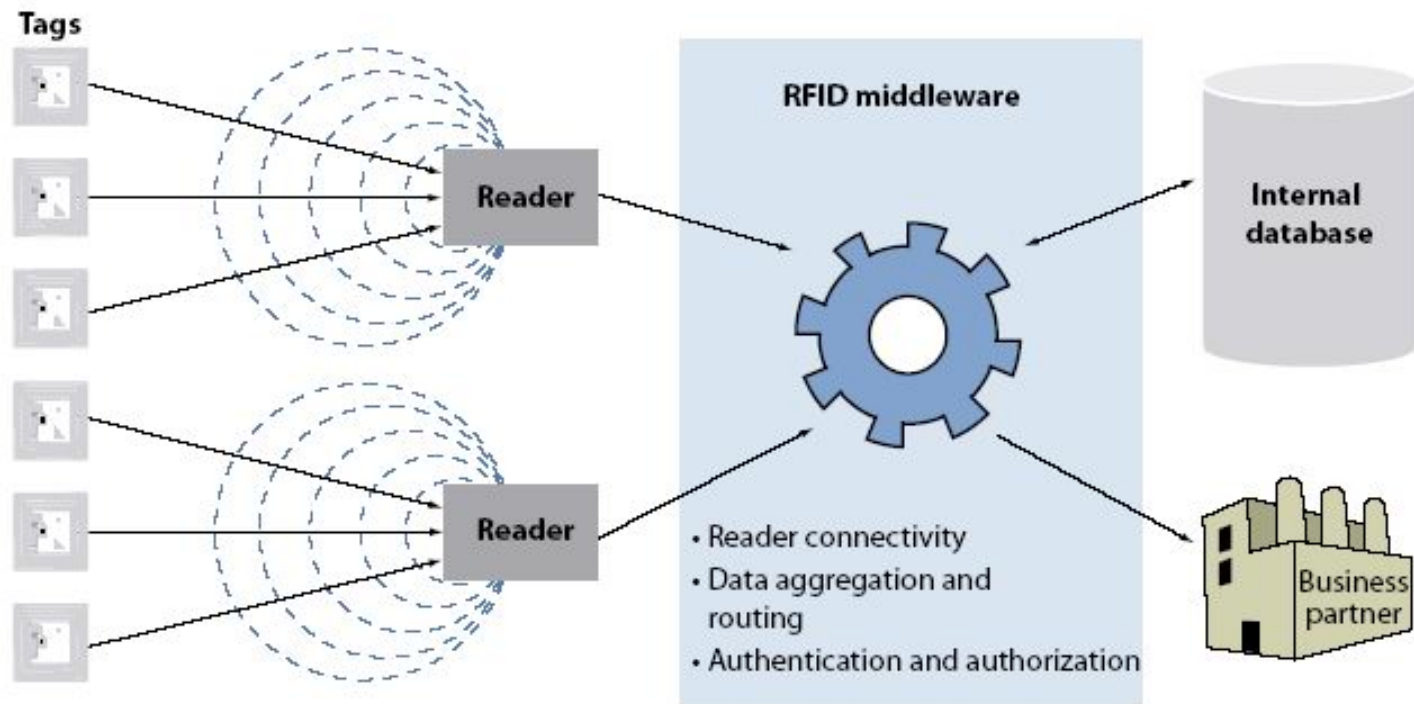
- Supply Chain Mgmt
- Enterprise Resource Planning
- Other apps



RFID: What Is It?

(Radio Frequency Identifiers)

Example RFID Architecture



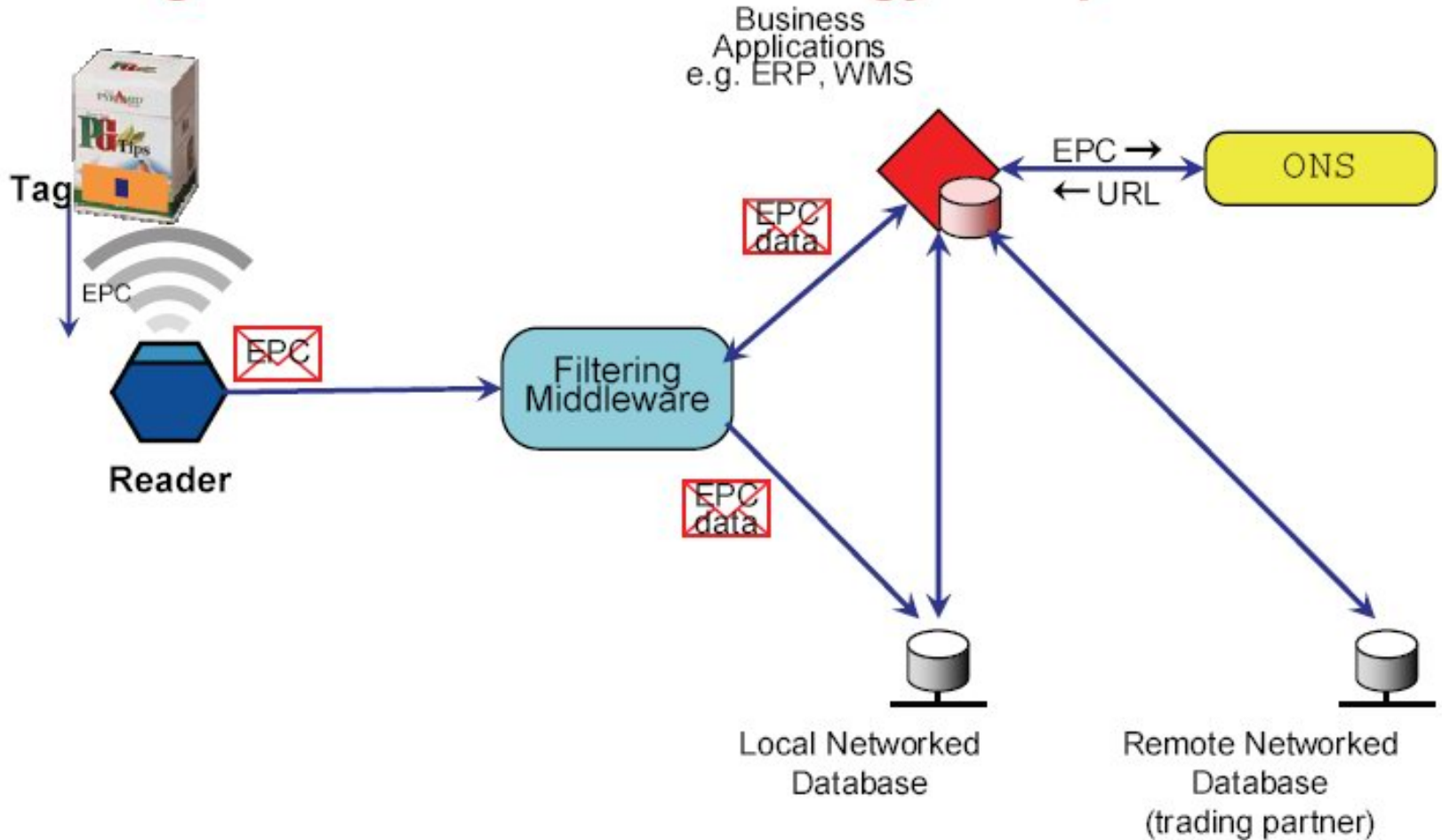
Source: Forrester Research, Inc.



RFID: What Is It?

(Radio Frequency Identifiers)

EPCglobal Network - Technology Components





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 knowledge or involvement of people;
- *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 labour costs (e.g., no manual scanning of individual items is required)
- Better detection of counterfeits, fraud
- Better post-sale service for consumers: returns, warranty servicing, recalls, etc;



RFID Applications

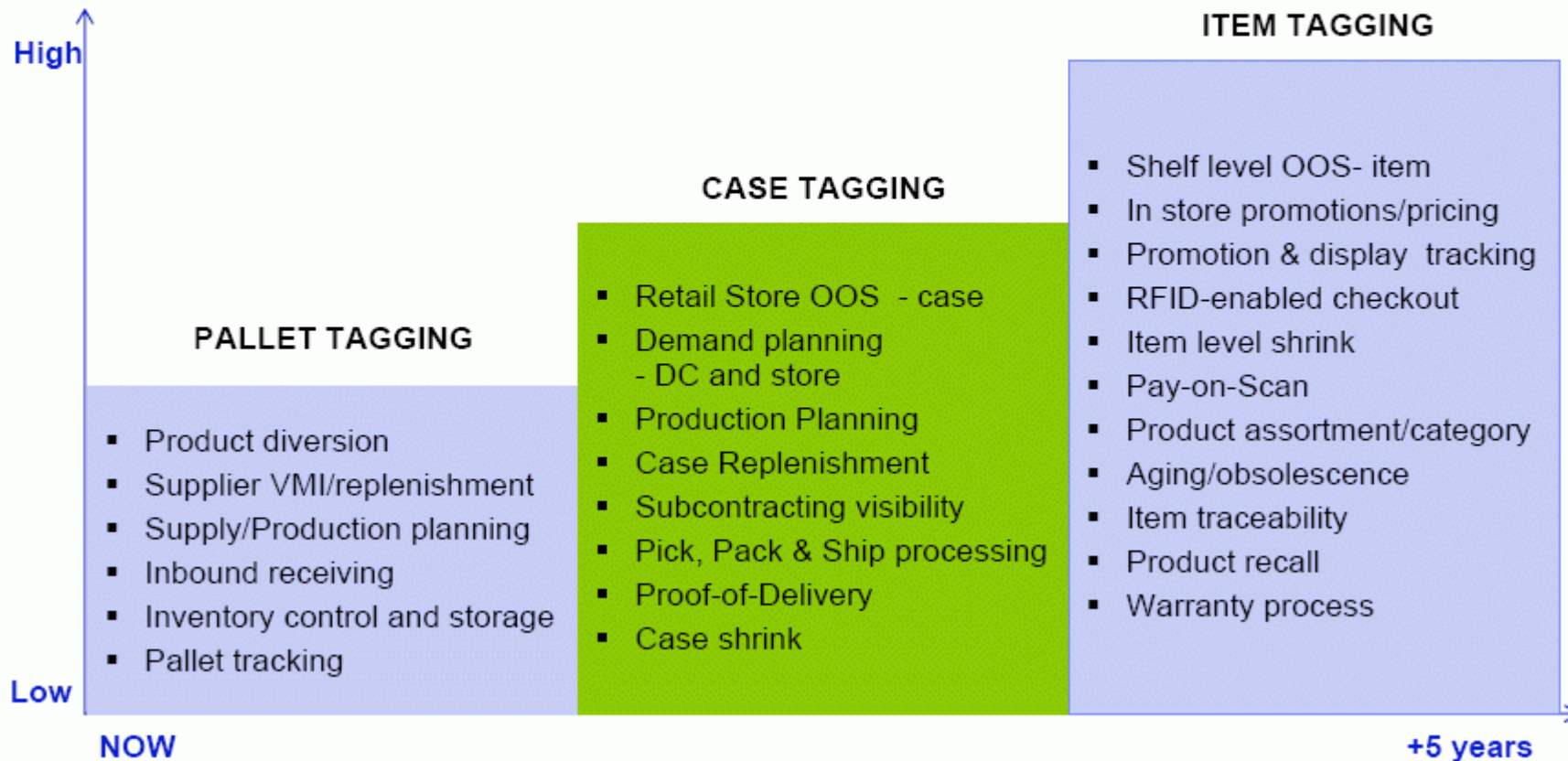
Examples of RFID applications in all industries

- Retail
 - Lower labour costs
 - Out-of-stock triggers
 - Reducing shrinkage
 - Reducing inventories
 - Locating products
 - Real-time supply/demand data
 - Smart shelves
 - Self check-out
 - Reverse logistics
 - Customer convenience
- Healthcare/ Pharma
 - Tracking hospital equipment
 - Patient ID and tracking
 - Preventing medication errors
 - Tracking samples/ vials etc
 - Environmental monitoring (e.g. blood samples)
 - Anti-counterfeit measures
 - Product recalls
- Manufacturing
 - Quality control
 - Lot Tracking
 - Recalls
 - Government regulations
 - Inventory accuracy and visibility
 - Labour & material costs
 - Asset utilization
 - Contract manufacturing
 - Supplier Management
 - Customer relations
 - Supply chain management
 - WMS
 - Inventory
 - Gray markets/ theft
 - Shrinkage
 - Shop floor execution
- Government
 - Homeland security
 - Military/ defense asset tracking
- Transportation & Logistics
 - Asset utilization and tracking
 - Volume planning
 - Automated sorting
 - Automated data capture
 - Shipment route tracing
 - Delivery reliability/ efficiency
 - Contract pricing verification
 - Reduced claim costs
- Construction
 - Asset utilisation and tracking
 - Automated data capture
 - Yard control
 - Safety equipment tracking
- Other
 - Farm animal tracking
 - Contactless payment systems
 - Sensor/ sensing applications
 - Theme park applications
 - Airport tracking of baggage/ passengers



RFID Applications

Benefit potential increases as companies transition from pallet to case to item level tagging





RFID Applications

Supply Chain Mgmt



- Shipment tracking, inventory & materials management, material location & tracking

Asset Tracking



- Life cycle management, managing recalls, verifying authenticity, and tracking assets or products for regulatory compliance, food traceability

Work In Process



- Assembly automation, just-in-time/just in sequence parts management, and tool/equipment tracking

Security & Access Control



- Access control, authentication for matching, location tracking for sensitive/hazardous materials and restricted areas

Consumer Application



- Real-time merchandising and shelf replenishment, automated payment systems, personal identification, patient identification, and toll collection



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.



Public Sector Uses

Public facing applications:

- **Public and private transportation**
- **Health care / Life Sciences**
- **Environment / Controlled goods**
- **Identity & access cards**
- **Tracking people (e.g. convicts)**

Non-public facing applications:

- **Libraries / File systems**
- **Access Control (pass cards)**
- **Inventory control, etc**
- **Tracking employees**



RFID Industry Outlook

- Highly versatile technology: used wherever visibility and identifiability of items is desired;
- Currently in widespread use: building access cards, car keys; payment tokens; toll roads;
- Good for tracking and tracing items: assets and inventory; library books; hospital sponges;
- Item-level use on retail goods expected in 5-10 years;
- Standardization and interoperability will promote RFID tags to be used across domains;
- RFID industry poised for “hockey-stick” growth?



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); “4-wall” uses
 - Convenience services (payment systems, e.g., PayPass, EasyPay, Speedpass; Dexit)
 - Identification and access control: loyalty and access cards, ignition immobilizer; VeriChip
 - Consumer Safety: for recalls, recycling, etc.



Obstacles to Growth

- Costs
- Reliability
- Security
- Privacy



Security Concerns

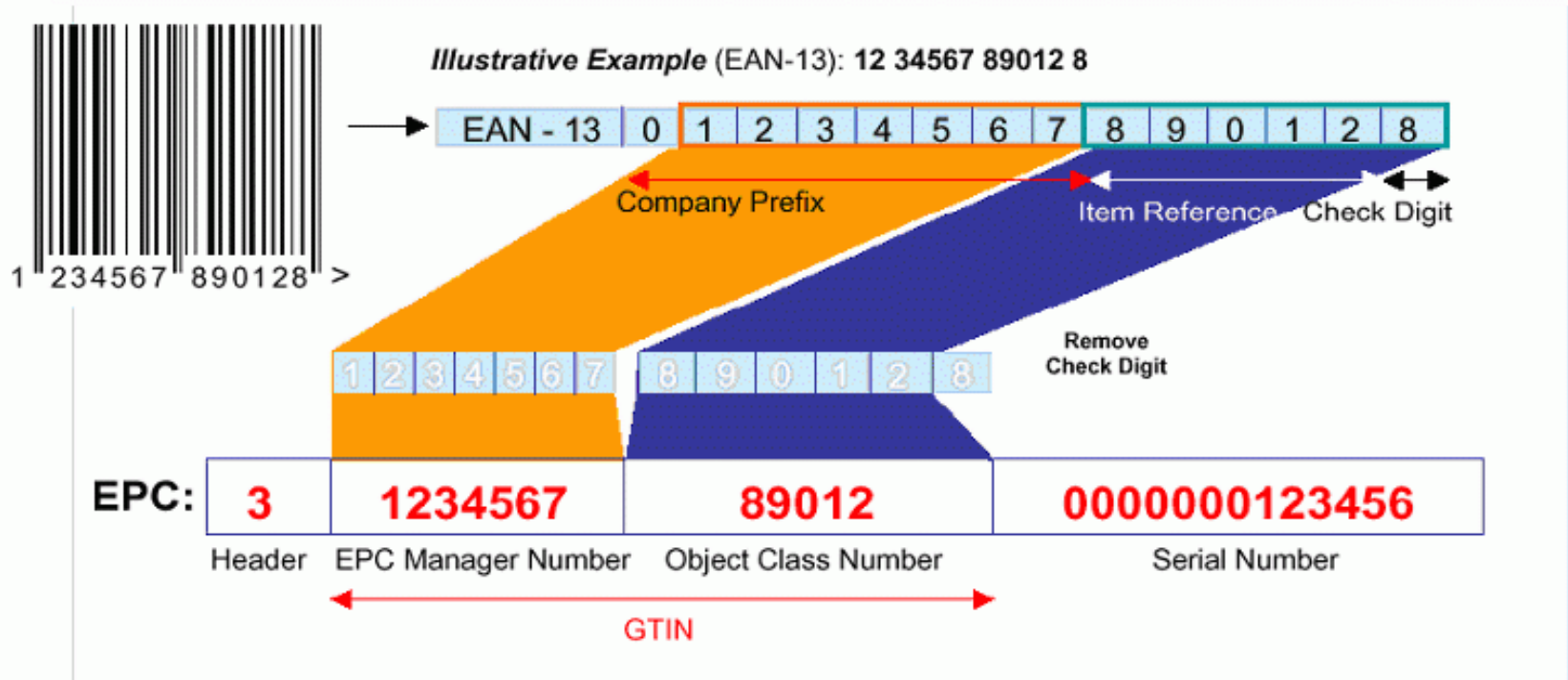
- As a wireless technology, RFID technology is still grappling with data security issues;
- Passive tags will respond automatically to any reader that interrogates them;
- Data on RFID tags are vulnerable to skimming, eavesdropping, cloning;
- RFID systems may also be vulnerable to jamming, denial of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



Privacy and RFIDs

- RFID tags contain data about products, not people:

Bar Code Numbers Map Into EPC Numbers



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



Consumer Perceptions

Consumer Advocates Believe!

“RFID has the potential to jeopardize consumer privacy, eliminate, anonymity, and threaten civil liberties.”

“RFID is a nightmare scenario that uses technology to invade privacy.”

“There is an invisible surveillance structure around us now.”

“There is no end to the mischief retailers will do to consumers with this new technology.”

“These new instruments will surely doom our civilization.”



Consumer Perceptions

Why Are Privacy Issues Important to You?

- In US, information security and misuse of consumer data is #1 consumer protection issue of the day
- Consumers have immediate negative reaction to “tracking” and “profiling”
- Consumer trust critical to end user’s success
- Public unease can lead to regulation/legislation
- Federal regulators taking a studied approach but states are moving quickly --privacy approaches crafted by lawmakers tend to be unfriendly to technology



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; loss of control
 - More transparency and accountability needed.



Consumer Backlash

- How real are consumer concerns?
- Could privacy issues potentially deter the roll-out of RFIDs?



Business Cases

- **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
- **2003, Benetton** – Italian clothier sparked a furor after it announced plans to implant RFID tags in its apparel



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.”



RFID Privacy Challenges

- **Perceived Lack of Transparency, Credible promises, 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.**



Restoring RFID

Privacy and Trust

Effective governance can come from:

1. Laws, legislation, regulation;
2. Industry self-regulation, codes of conduct, best practices, guidelines, standards, policies, etc;
3. Technological solutions;
4. Public opinion / market acceptance.



1. Law & Regulation

Law and Legislative Activity:

- U.S. state bills, laws;
- Canadian & European privacy laws;
- Enhanced Regulatory scrutiny, E.G.:
 - U.S. Congress RFID Caucus;
 - EU RFID consultation.



Examples of U.S. Laws Relating to RFID

Examples of state bills that have been passed:

- **California AB1489** – requires certain point-of-sale devices to be equipped with a “tactually discernible numerical keypad” or other technology (such as a RFID device), in order to provide visually impaired persons “... the same degree of privacy ... available to all individuals;”
- **New Hampshire HB1738** – prohibits the state use of surveillance devices (including a RFID device) on highways to identify motor vehicles, unless authorized by statute or in certain other circumstances;
- **Wisconsin AB290** – Prohibits requiring an individual to undergo the implanting of a microchip.



Trends - U.S. Bills relating to RFID *introduced in 2006*

- Bills may be advancing through the legislative process, or they may be vetoed, stalled or have died;
- **Task Forces** – Bills that would establish task forces to study RFID technology in the public and/or private sector
e.g.: New York, Washington;
- **Consumer Privacy** – Bills that would require notification of consumers of RFID tags and/or removal of tags at point of sale; e.g.: Illinois, Missouri, New York, Tennessee;
- **Prescription Drug Packaging** – Bills that would require packaging to incorporate RFID tagging technology (or similar trace and track technologies), among other things;
e.g.: Federal bills



Trends - U.S. Bills relating to RFID *introduced in 2006 (cont'd)*

Human Identification:

- ***Microchips in Individuals*** – Bills that would prohibit requiring microchips in individuals, e.g.: New Jersey, Ohio;
- ***Identification Documents*** – Bills that would restrict or prohibit the broadcasting or remote scanning of personal information on government ID documents via “contactless integrated circuits” or “radio waves,” e.g.: Alabama, Illinois, Washington;
- ***Other Tracking*** – Bills that would restrict the use of RFID devices by state or municipal agencies for the purpose of tracking the movement or identity of individuals as a condition of obtaining a benefit or services, e.g.: Rhode Island.



1. Law & Regulation

Canada:

- Public- and private-sector privacy laws: broad applicability;
- Federal *Privacy Act*, *PIPEDA* (review this year);
- Provincial privacy laws (QC, BC, AB, ON) and sectoral (health);
- In Canada, provincial privacy laws pre-empt federal law;
- Independent oversight agencies (e.g. commissioners);
- European Union Data protection directives, national data protection commissioners' findings, Art. 29 Working Party opinions.



2. 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.



Industry Best Practices, Codes of Conduct, Policies

- EPCglobal *Guidelines on EPC for Consumer Products* at: www.epcglobalinc.org/public_policy/public_policy_guidelines.html
- ICC principles for responsible deployment, operation of e-product codes: www.iccwbo.org/home/statements_rules/statements/2005/EPC_Principles.pdf
- CDT Working Group on RFID: Privacy Best Practices for Deployment of RFID Technology: www.cdt.org/privacy/20060501rfid-best-practices.php
- *RFID Position Statement of Consumer Privacy and Civil Liberties Organizations* at: www.privacyrights.org/ar/RFIDposition.htm
- *Guidelines on Commercial use of RFID Technology* at: www.epic.org/privacy/rfid/rfid_gdlnes-070904.pdf
- *RFID Bill of Rights* at: www.ftc.gov/os/comments/rfid-workshop/508920-0034.pdf



Guidance for Commercial RFID Uses (*Oversight / Regulatory Bodies*)

- Tag, You're It: Privacy Implications of RFID Technology
at: www.ipc.on.ca
- Resolution on Radio-Frequency Identification
at: www.privacyconference2003.org/resolutions/res5.DOC
- Working document on data protection issues related to RFID technology
at: http://europa.eu.int/comm/justice_home/fsj/privacy/docs/wpdocs/2005/wp105_en.pdf
- U.S. FTC, Radio Frequency Identification: Applications and Implications for Consumers (Workshop Report, Mar 2005) available at:
www.ftc.gov/os/2005/03/050308rfidrpt.pdf
- *Work is underway by other Canadian legislators, regulators, U.S Senate RFID Caucus, EC RFID consultation, etc.*



IPC RFID Privacy Guidelines

- Developed with leading industry standards-setting organization (GS1/EPCglobal Canada);
- Based upon the 10 fair information practices of the CSA Privacy Code;
- 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 (Cont'd)

Three Overarching Principles:

- Focus on entire RFID information systems, not just tags/technology;
- Privacy and Security Must be Built in from the Outset – at the Design Stage;
- Maximal Individual Participation and Consent.



IPC RFID Privacy Guidelines

Scope

- Based on 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

Accountability

- Organizations with the most direct contact and primary relationship with the individual should bear the strongest responsibility for ensuring privacy and security;
- Privacy policies & procedures must be put in place;
- Assurances for transfers of PII to third parties;
- Addresses major consumer trust issue: who's in charge?



IPC RFID Privacy Guidelines

Knowledge and Consent

- Higher privacy thresholds than “notice and choice;”
- Consent is pivotal for item-level uses if personal info is to be linked with the RFID tag, then collected and retained by the company;
- Required by law across Canada.



IPC RFID Privacy Guidelines

Data Minimization

Limiting Purposes, Collection, Use, Disclosure and Retention of PII:

- These privacy practices express the fundamental principle of *data minimization*;
- Data minimization is most effective when built early into the RFID information architecture;
- Data minimization enhances information security and improves confidence in privacy practices.



IPC RFID Privacy Guidelines

Access and Redress

- In Canada, consumer access to their info and redress mechanisms are statutory requirements;
- Strengthened by openness, accountability;
- Many business benefits, e.g.:
 - improved accuracy of customer data;
 - opportunities for building trusted 1:1 consumer relationships.



IPC RFID Privacy Guidelines

Tag De-Activation

- Automatic de-activation at point of sale is the objective;
- De-activation directly addresses many consumer privacy and security concerns;
- De-activation followed by re-activation at the choice of the consumer, is the ultimate goal;
- We point to the IBM ‘Clipped Chip’ solution;
- De-activation may not be appropriate in certain, limited RFID uses.



3. Technology: Build It In

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



Technology & Privacy

- 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

- IBM Clipped Chip 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.



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.

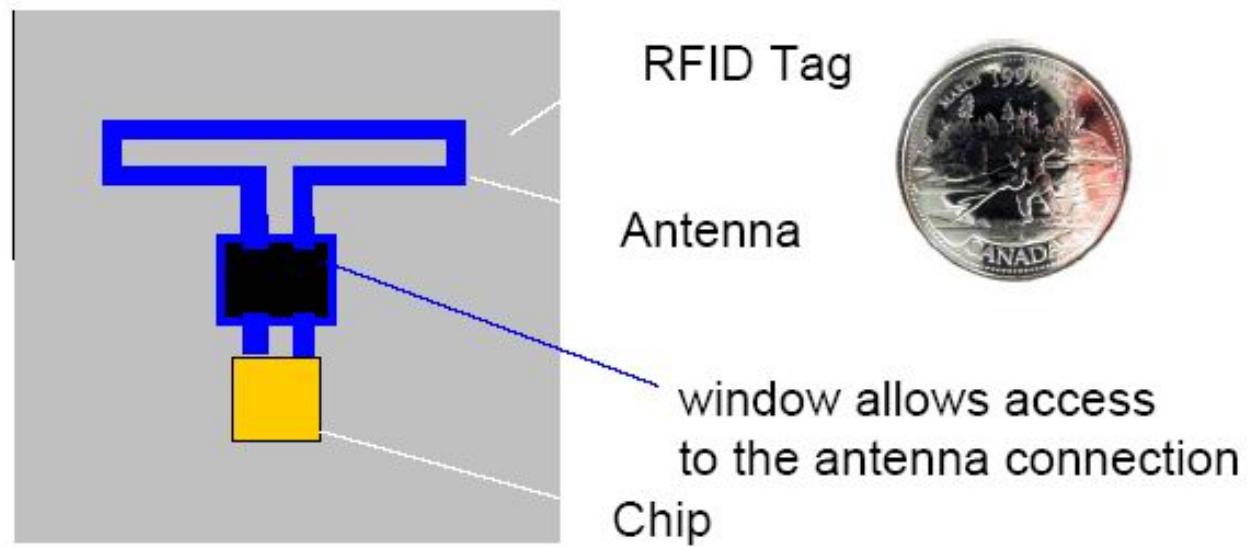


Example:

Consumer Disabled Tag

Clipped RFID Tags

- Example 1: Removable Electrical Connection – “scratch-off” for the chip-to-antenna connection

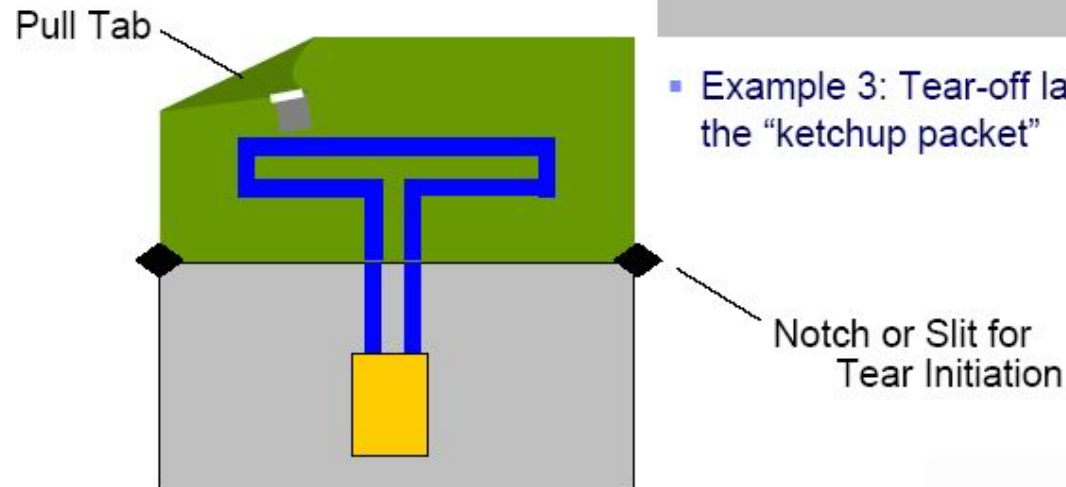
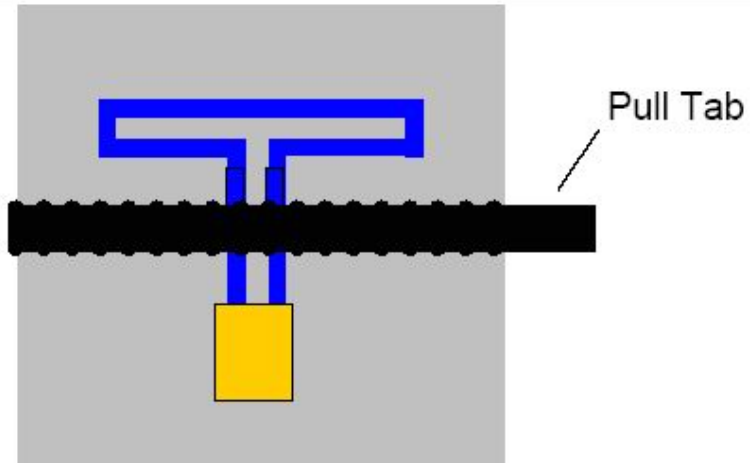




Example: *Consumer Disabled Tag*

Clipped RFID Tags

- Example 2: Perforation – “zipper” or “postage stamp” method



- Example 3: Tear-off layer – the “ketchup packet”





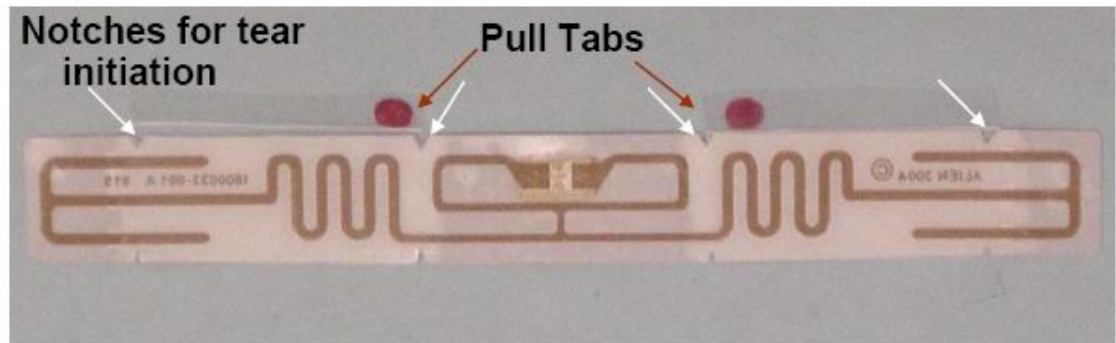
Example:

Consumer Disabled 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 RFIDs

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.



Building Privacy Safeguards into RFIDs (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, e.g;
- 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);
- 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 RFIDs (Cont'd)

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

- Technologies can serve consumers by ensuring meaningful user involvement, choice and control in the RFID information lifecycle processes;
- Detect the presence and location of both 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 rights to any data associated with a given tag;
- Assign effective control over tag behaviour to consumers and other end-users;
- Quickly and easily de-activate tags, either temporarily or permanently.



4. Education and Awareness

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



Education and Awareness (Cont'd)

- No covert uses of the technology;
- Benefits of enhanced visibility and interoperability of supply chain goods;
- RFID use not a trade-off with privacy;
- There should always be strong privacy protection in place;
- Accountability is vital.



IPC Engagement

- Involvement in issue in 2003;
two discussion papers published 2004;
- Member of EPCglobal Privacy Public Committee;
- Canada Public Policy Steering Committee;
- Participation in EU public RFID consultation;
- Encourage adoption of high privacy standards.



IPC RFID Privacy Guidelines

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.



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.



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 Kananoff,

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



The Bottom Line

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



How to Contact Us

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

Phone: **(416) 326-3333 / 1-800-387-0073**

Web: **www.ipc.on.ca**

E-mail: **info@ipc.on.ca**