

PRIVACY HORIZONS: TERRA INCOGNITA

29th International Conference of
Data Protection and Privacy Commissioners

September 25 to 28, 2007
Montreal, Canada



LES HORIZONS DE LA PROTECTION DE LA VIE PRIVÉE : TERRA INCOGNITA

29^e Conférence internationale des commissaires
à la protection des données et de la vie privée

du 25 au 28 septembre 2007
Montréal, Canada

OECD Work on RFID: Information Security & Privacy

Laurent Bernat

www.oecd.org/sti/security-privacy

Context

- RFID : first step in OECD work on sensor-based environments
- Work in progress: draft report to be discussed week in Ottawa.*
Ministerial Meeting on the Future of the Internet Economy (June 2008, Seoul, Korea)
- Scope
 - Economic aspects of RFID
 - Information Security and Privacy Protection
- Key Reference Policy Frameworks
 - OECD 1980 Guidelines for the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines)
 - OECD 2002 Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security (Security Guidelines)

* OECD work is ongoing and the view expressed are those of the speaker

Characteristics of RFID

- Wireless (invisible)
- Economic potential
- Variety
- Technical complexity
- Vague boundaries
- Possibility of covert collection
- Possibility to track individuals, not just objects
- Could enable or facilitate profiling
- Susceptible to information security risks

When is privacy at stake ?

- **Directly** : when RFID systems collect/process data related to an identified or identifiable individual (personal data)
 - ➔ When personal data is collected/processed, OECD Privacy Guidelines apply
- **Indirectly**: when tags are provided to individuals but data has yet to be collected/processed (risk of data collection)

Key messages (tentative)

Privacy protection requires a mix of legal, technical & educational measures

1. Knowledge & consent
2. Impact Assessment
3. Holistic approach
4. Technical measures
5. Proactive measures

1. Knowledge & Consent are key

- Knowledge can be challenging
 - Real time, complex information, small space
 - Need for consensus on what information to provide and how
 - Need for innovative and efficient transparency mechanisms
- Consent can be challenging ?
 - Exceptions to consent (practical aspects, public interest). Need to reach a consensus on these exceptions.
 - Does consent always provide sufficient protection ?

2. Privacy Impact Assessment

- Privacy impact varies with technology used
- Personal data
- Sensitive data
- Reassessment
- Tags beyond data controller's reach

3. Holistic approach

- Not all solutions are at the RFID level

Need to consider:

- Each stage of the systems' life cycle
- Each component of the system and steps in the RFID data life cycle

4. Technical measures

- Critical success factor for RFID
- Preventative / mitigating
- No one-size-fits-all
- Cost and complexity
- R&D and incentives for adoption needed

5. Proactive measures

- When tags are provided to individuals but no data has been collected/processed yet
 - Tags could create a privacy risk for the person
 - Who should be responsible for removing or deactivating tags / providing appropriate information ?
 - Cf. consumer protection (OECD 1999 Guidelines on Consumer Protection in the Context of Electronic Commerce) and product safety.
 - Role for DPAs to flag this issue

Terra incognita

- Evolving technology
- Tag interoperability
- Open Loop RFID
- B2C and C2C uses
- Pervasive RFID
- Connected RFID ("Internet of Things")
- Sensor based environments
- Ubiquitous computing & other paradigm shifts