Privacy Rights Management Using DRM
Is this a good idea?

Larry Korba
Information Security Group

Black Hat Europe, May 19-20, 2004
Agenda

• Introduction
  – Caveats
  – About this Work and the Speaker
• Privacy in the EU
  – Laws, Elements, Principles
• Mark-Up and Privacy Expression
• Using DRM for PRM
• Pitfalls
• Conclusions
Introduction: Caveats

• **High Level view**
  – Talk/email me for more detail

• **Translate into Technology**
  – From Policy to Processes

• **Ask Questions**
  – We will all learn more.
Introduction: About the Speaker

• Researcher, Group Leader, Information Security Group
• 8 Researchers
  – Security Intelligence to Privacy
• Research Collaborations
  – Europe, Taiwan, CSE
  – Consult with SME
Introduction: About this Work

• Privacy Incorporated Software Agent (PISA) Collaboration (2001-2004)
  – http://www.pet-pisa.nl/

• Me – Leader for the Canadian Parts of the PISA project
  – Network Privacy, Scalability, & Trustworthy HCI
  – This work: PISA Engendered
Privacy Basics: What is Privacy

• The right to be left alone
  – Free from surveillance or interference
    • from other individuals,
    • from organisations or
    • from the state
• A Fundamental Human Right in the EU
Privacy in the EU: The Basics

• EU is in the vanguard. Also Canada, Australia, Hong Kong
• In US: Privacy Legislation Patchwork
• Individual Rights and Custodian Responsibilities, are described in the EU Data Directive 95/46/EC, (99/33/EC, 2002/58/EC)
• In EU, Different Countries Deal with the Directive differently
• Privacy Principles explain general requirements
Privacy in the EU: The Elements

- **Personally Identifiable Information (PII)**
- **Data Subject**
  - Citizen of the EU
- **Data Controller**
  - Custodial Responsibility for PII
- **Data Processor**
  - Processes PII
  - May be part of the Controller
Legislation: Relationship Between Elements

Data Subject

Data Controller

Data Processor

The Directive
The Privacy Principles

• Express the Essence of the Legislation (Directive)
• Useful guidelines for understanding requirements
• Different Countries have slightly different Principles
Legislation: Privacy Facilitation Principles
• Express legislation intentions

– Reporting the processing
– Transparent processing
– Finality & Purpose Limitation
– Lawful basis for data processing
– Data quality
– Rights
– Data traffic outside EU
– Data processor processing
– Security
Reporting the Processing

- *Processing of PII must be reported to Data Protection Authority, unless processing is exempt (e.g. anonymity)*
Transparent Processing

- *Data Subject must be able to see who is processing what data for what purpose.*
Finality & Purpose Limitation

• PII may only be processed for the explicit, agreed upon, and legitimate purposes
Lawful Basis for Data Processing

• PII processing must be:
  – legal for the type of data involved
  – Depends on the type of PII
Data Quality

- PII must be
  - correct and as accurate as possible,
  - sufficient,
  - to-the-point
- not excessive.
Rights

• Data Subject has right to improve data and raise objections.
Data Traffic Outside EU

• Sending PII Data outside EU
  – Only if adequate data protection offered
Data Processor Processing

• If Controller outsources processing
  – Must assure control over processor
Security

- Suitable technical and organizational procedures are required
  - Limit Access
  - Maintain Integrity
  - Secure Storage, Processing
EPAL, P3P, and other XML Variants

- **EPAL (ZKS, IBM)**
  - Formalize Internal Privacy Policies
  - Fine grained Control
  - Authorization scheme for centralized control
  - Flexible
  - XML Standard track

- **P3P**
  - Website privacy policy specification
  - Predefined data categories, data user list, purposes
  - Only a Use action
What about Enforcement?

- EPAL must be built into systems.
  - IBM’s Enterprise Architecture shows some promise
- But how do those systems help to enforce the privacy principles?
Approach for this Work…

• **DRM**: used to control and meter use of digital information
• **Adapt Digital Rights Management** to form a system for **Privacy Rights Management**
• **Use this approach to describe how to “Enforce” privacy principles**
• **Describe drawbacks**…
Digital Rights Management (Simplified)
**Entity Relationships**

- **Converting from DRM to PRM**

<table>
<thead>
<tr>
<th>PRM</th>
<th>DRM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Subject</td>
<td>Owner</td>
</tr>
<tr>
<td>Data Controller</td>
<td>Distributor/DRM System</td>
</tr>
<tr>
<td>Data Processor</td>
<td>User</td>
</tr>
</tbody>
</table>
Privacy Rights Management (Simplified)
**Data Directive Fit: Behaviors**

### Privacy Principles
- Reporting the processing
- Transparent processing
- Finality & Purpose Limitation
- Lawful basis for data processing
- Data quality
- Rights
- Data traffic outside EU
- Data processor processing
- Security

### DRM Function
- Log use
- Know use
- Work used for specific purpose
- Appropriate use: Transform Law to Code
- Maintain quality
- May improve works
- Special Handling Software
- Protected Access/Storage
- Distribution
System Behavior: Some Examples & Ideas

• Finality
• Data Quality

• Lawful Basis
• Data Processing
Finality

- PII may only be processed for the explicit, agreed upon, and legitimate purpose.
Data Quality

- PII must be: correct and as accurate as possible, sufficient, to-the-point, not excessive.
Lawful Basis

• PII processing must be:
  – legal for the type of data involved
  – Depends on the type of PII
• How?
  – Labor-Intensive Review
• What are we in store for in the Near Future?
Lawful Basis: Legal & Regulatory Compliance

Ontology Developers
- Legal Experts
- Laws, Directives, Decisions, etc.
- Compliance Officials

Ontology Platform
- Legal Ontology

Ontology Users
- Law Enforcement
- Application Developers
- Citizens
- Judicial System
- Legislators

Viewer
Editor
Search
Analysis & Interpretation
Data Processing

• Must limit Processing, Distribution, Retention, Maximize Correctness
• Ideas:
  – Audited Contracts (Controller ↔ Processor)
    • Security Standards, Record Keeping
  – Metered Access
    • But.. Data still in Clear for processing
  – Certified 3rd Party Processor?
  – Processing Container
    • Processing & Data Bound Together
Good & Bad: Using DRM for PRM

• DRM for PRM appears a good fit
  – Useful way of approaching system development
  – Offers security, finality, processing reporting but…

• Millions of Data Subjects: Scalability an issue for Reporting processing

• Assuring proper personal data processing: difficult or impossible

• Beyond DRM, PRM must allow maintenance of Personal Data by data subjects
  – In EU, Privacy a basic human right.
  – In US, People tend to give up PII readily
Commoditization of PII?
- Potential approach under consideration for US
- Free Market sort of model
- Citizen in Control
  - May bargain for good/services in exchange for PII
- Quite different than the EU Model
Conclusions

• Privacy Management Pressures
  – Legislation forces Compliance, More Data
• EU: Leads World in legislation and enforcement
• Privacy Principles Analysis + DRM adapted for PRM
  – Offers a way to understand system requirements
• Particular challenges:
  – Scalability, Secure processing, Lawful Basis
• Zero Knowledge, IBM, Others
  – Privacy Languages and Architectures
  – Dealing with Legacy Systems, still a challenge
Thank You…

Questions?

Larry.Korba@nrc-cnrc.gc.ca

http://www.iit-iti.nrc-cnrc.gc.ca