EnCoRe

Ensuring Consent & Revocation

A collaborative IT research project being undertaken by UK industry & academia

Towards a Conceptual Model for Privacy Policies

Dr Nick Papanikolaou
International Digital Laboratory
University of Warwick
http://go.warwick.ac.uk/nikos

Joint work with **Sadie Creese**, **Michael Goldsmith** (Warwick),
Marco Casassa Mont, and **Siani Pearson** (HP Labs)

EnCoRe

Ensuring Consent & Revocation

A collaborative IT research project being undertaken by UK industry & academia

Introduction

- Central problem: How enterprises **administer** and **enforce privacy of personal data** of their customers
- Key contribution: a simple conceptual model which can express privacy requirements emerging at different levels in an enterprise
- Privacy requirements originate:
  - in current legislation
  - in industry regulation
  - in enterprise-wide privacy policies and practices

EnCoRe
Ensuring Consent & Revocation
A collaborative IT research project being undertaken by UK industry & academia

Current privacy practices

- **How are privacy requirements enforced within an enterprise today?**
- Typically, an enterprise will undertake **risk assessments** to determine at which stages in its business processes it is necessary to introduce control points
- Privacy policies are enforced by introducing:
    - **audits**
    - **technical policy enforcement mechanisms**

  at these control points

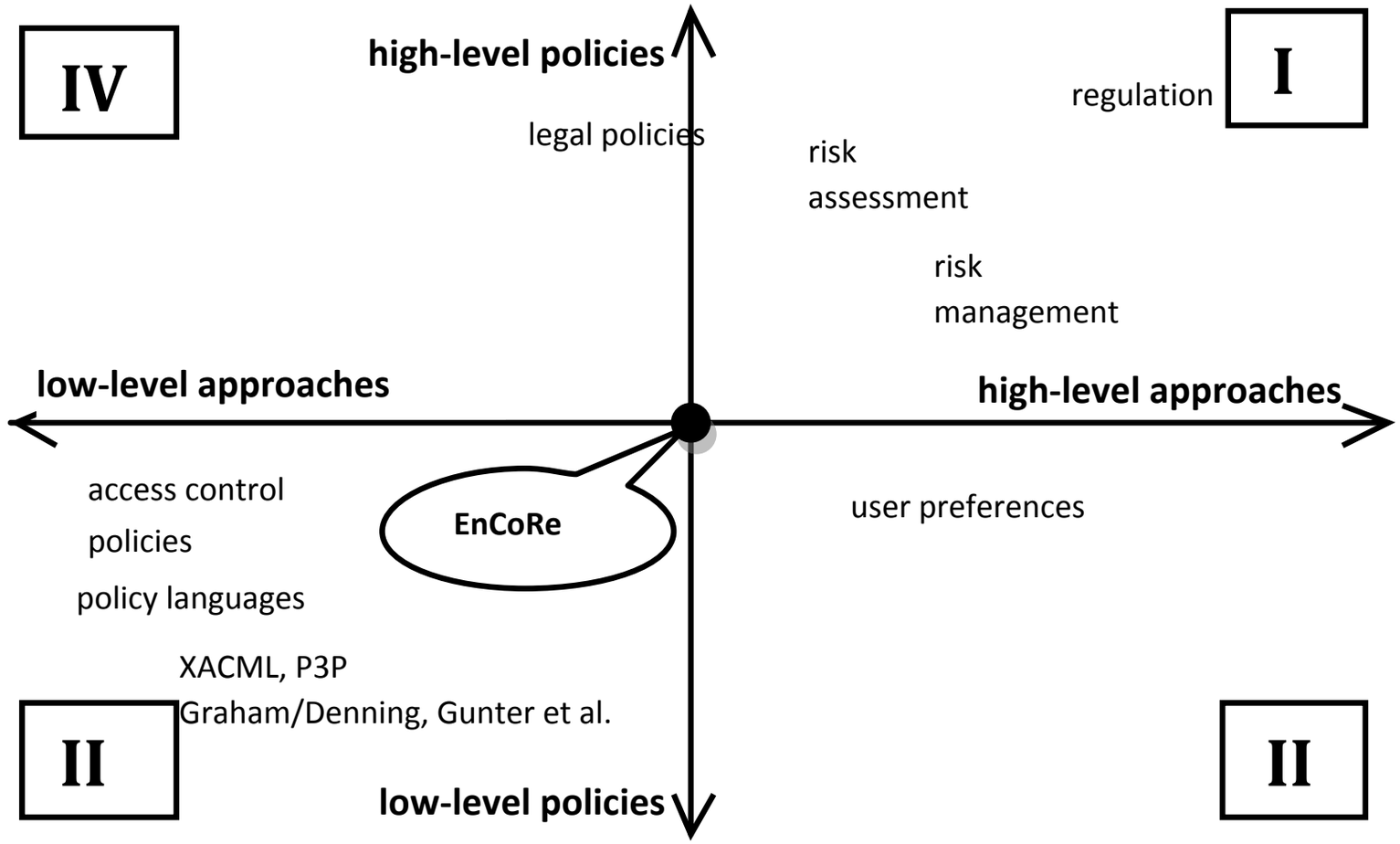
EnCoRe
Ensuring Consent & Revocation
A collaborative IT research project being undertaken by UK industry & academia

Problem with current practices

- The outcome of a risk assessment will be to determine **where privacy needs to be enforced** (what **control points** are needed)
  - the mechanisms to enforce privacy are chosen in an *ad hoc* manner
  - the result is enterprise-specific and not re-usable or easily extensible
- Technical approaches reduce privacy enforcement to access control
  - in this case, access control mechanisms are deployed throughout the enterprise, but privacy requirements are not always fully captured, and there is no universally accepted access control framework

Two extremes...

- Traditional risk assessments are therefore not suitable for designing a general privacy architecture
- Technical solutions to privacy are not enough either
- Can we bridge the two approaches?



EnCoRe
Ensuring Consent & Revocation
A collaborative IT research project being undertaken by UK industry & academia

Policy Layers

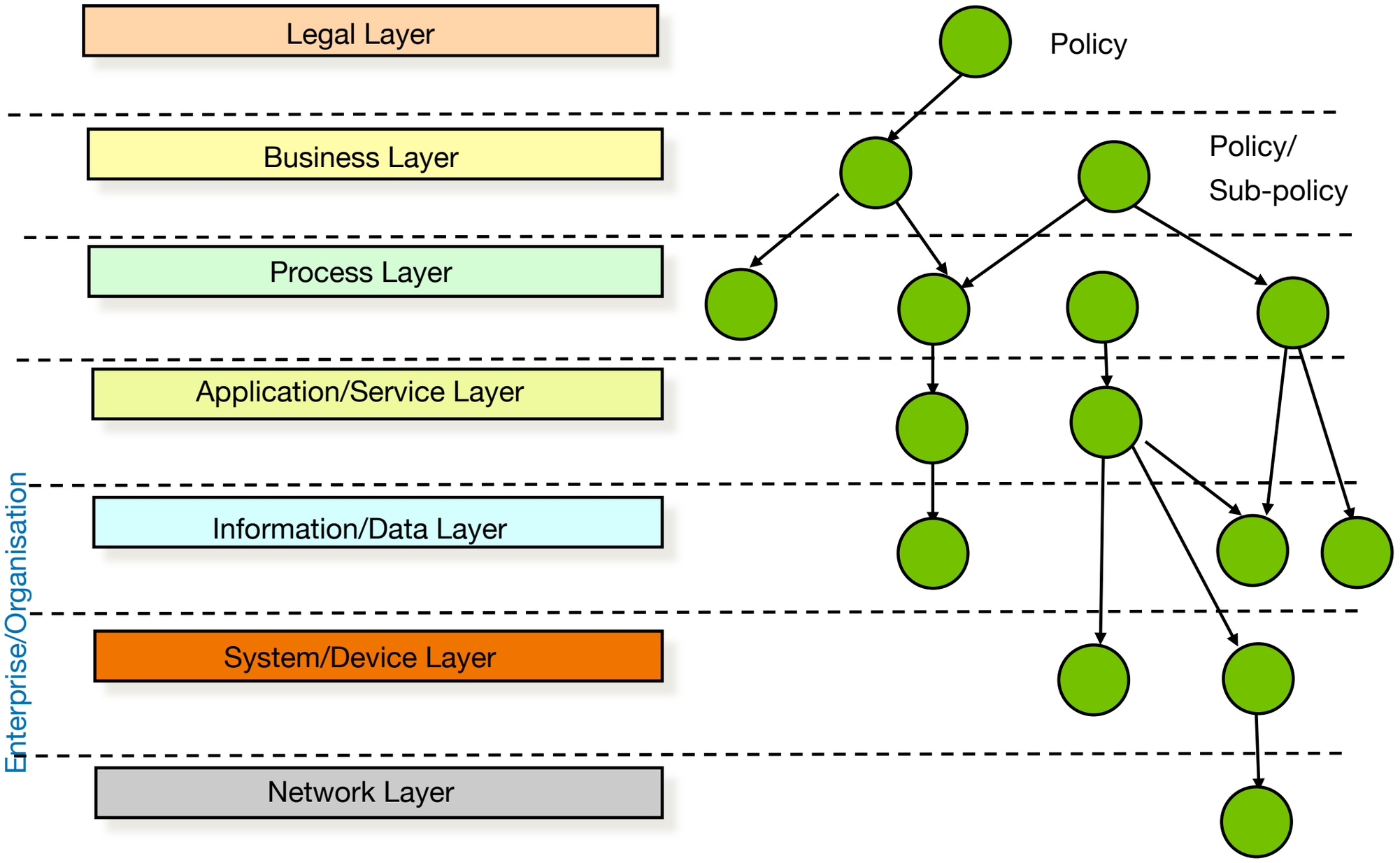
- Privacy requirements can be very **high-level**, such as those appearing in **national laws and international agreements**
  - e.g. EU Data Protection Directive, Data Protection Act (UK)
- **Privacy regulation** - transborder data flow, export restrictions
- **Security requirements** - financial reporting stipulations (cf. SOX)
- Enterprise: **internal guidelines**, **information lifecycle policies**, **contractual obligations**
- Operational policies
- **Technical / machine-readable policies**
  - cf. XACML, EPAL, P3P for privacy requirements

EnCoRe

Ensuring Consent & Revocation

A collaborative IT research project being undertaken by UK industry & academia

Policy layers



Key points

Key point: which privacy management approach is adequate for each different level of policy / requirement?

Key point: how to express privacy requirements at the different layers consistently?

EnCoRe
Ensuring Consent & Revocation
A collaborative IT research project being undertaken by UK industry & academia

The EnCoRe approach

- Rather than to match policy layers with approaches, in the EnCoRe project ("Ensuring Consent and Revocation") we seek an ideal means of expressing and reasoning about privacy requirements
  - See http://www.encore-project.info
- The conceptual model we are looking for should capture both high-level and low-level privacy requirements
- It should be capable of use and adaptation in risk assessment, and should abstract away from specific technical policy languages (XACML, PRIME, ...)
- Case studies - Employee data, Biobanking, Assisted Living

EnCoRe
Ensuring Consent & Revocation
A collaborative IT research project being undertaken by UK industry & academia

A Conceptual model

- Conceptual models are used in AI research as a means of capturing knowledge about a particular domain, so it can be used to build an **expert system**
- Structure of privacy requirements

  IF (condition on personal data or data requestor)
  THEN (privacy enforcement action)
  ELSE (enforcement action or notification)

- the task is to systematically identify the form of
  - conditions
  - enforcement actions

Enforcement Actions

- Classes of actions encountered in policies:
  - notification rules
  - access control rules
  - update/creation rules
  - protection rules
  - obligation rules [work-in-progress]

Example 1: Access control

- Privacy-aware access control
- **Target:** Personal Data D
  if (Data Requestor wants to access personal data D for Purpose P)
  and (data subject has given consent for this data)
  then Allow Access
  else Deny Access

Example 2: Transborder

- Transborder data flow

```
if (all source countries are members of
EEA and all target countries are members
of EEA)
then (no problems with transborder data
flow)
else (stop transaction)
```

EnCoRe
Ensuring Consent & Revocation
A collaborative IT research project being undertaken by UK industry & academia

Example 3: Notice

- Special rule for notification

```
if (<country legal entity resides in> is
member of [Belgium, Portugal])
then (provide notification)
```

Example 4: Security+Privacy

- Privacy-aware access control:

```
Target: Personal Data X
If (Data Requestor is User U/Role R in
Context C)
and (Data Requestor wants to access
personal data D for Purpose P)
and (Data Subject has given consent for
this data)
then (Allow access to X)
else (Deny access)
```

Example 5: Low-level

- Low-level access control policy

```
Target: <Database:DB1, Table:T1> if
(DataRequestor.role is “employee” and
DataRequestor.intent is “Marketing”)
then ((Allow access to T1.Condition,
T1.Diagnosis) & Enforce (Consent))
else if (DataRequestor.intent is
“Research”)
then (Allow access to T1.Diagnosis) &
Enforce (Consent))
else (Deny access)
```

Oversimplification?

- The purpose of the conceptual model is to promote understanding and to identify common structure in policy rules arising in the different layers
- Translation to low-level policies (e.g. generation of XACML) should be directly possible
- Integration with risk assessment should give rise to methods for privacy-aware risk assessment (not the same as privacy impact assessment)
- We believe that there is value in testing the model out with as many practical requirements as possible

EnCoRe
Ensuring Consent & Revocation
A collaborative IT research project being undertaken by UK industry & academia

Next steps

- Formalisation
  - development of logic and semantics of privacy from Data Subject's point of view
  - we have developed a Hoare logic and access control model for privacy (cf. PrimeLife 2010 Summer School)
- Mapping to low-level policy languages
- Integration with security risk assessment/compliance methods
- Use as aid to build UIs
- Use conceptual model to build policy analysis framework / inference engine / rule-based systems