Semantics-Enabled Web Policies for Privacy Protection and Digital Rights Management: Current Status and Future Trends

Prof.(Dr.) Yuh-Jong Hu

Emerging Network Technology (ENT) Lab.
Department of Computer Science
National Chengchi University, Taipei, Taiwan

March-11-2009

NRC IIT Colloquium
Part I

Research Goals
SemPIF Framework: PIF + Meta-PIF

- SemPIF: Semantic PIF and Semantics-enabled meta-PIF
- Policy Interchange Format (PIF)
- Meta-PIF
- SemPIF for privacy protection
- SemPIF for DRM
- SemPIF for multiple domains
- SemPIF for policies legalized
Short Term Research Goals
Privacy Protection

Semantics-Enabled privacy protection policies
- Formal semantic model of P3P and EPAL
- Semantic enforcement of privacy protection policies
- Semantics-enabled privacy protection system on the Web

Current Status [15]
- DL + log-based ontology + rule on P3P
- Ontology-based privacy protection policies
- Rule-based privacy protection policies
- Semantics-enabled privacy protection policies
- Policies alignment between semantics-enabled P3P and EPAL
LONG TERM RESEARCH GOALS

Short Term Research Goals
Privacy Protection

SEMANTICS-ENABLED PRIVACY PROTECTION POLICIES

- Formal semantic model of P3P and EPAL
- Semantic enforcement of privacy protection policies
- Semantics-enabled privacy protection system on the Web

CURRENT STATUS[15]

- DL + log-based ontology+rule on P3P
- Ontology-based privacy protection policies
- Rule-based privacy protection policies
- Semantics-enabled of privacy protection policies
- Policies alignment between semantics-enabled P3P and EPAL
Short Term Research Goals
Digital Rights Management (DRM)

**Semantics-Enabled DRM policies**
- Formal semantic model of ODRL/XrML
- Semantics-enable of DRM policies
- Semantic enforcement of DRM system on the Web

**Current Status**[14]
- SWRL-based ontology+rule on ODRL
- Ontology-based usage and delegation rights of DRM
- Rule-based usage and delegation rights of DRM
- DRM policies for fair use of Intellectual Property (IP)
Short Term Research Goals
Digital Rights Management (DRM)

**Semantics-Enabled DRM policies**
- Formal semantic model of ODRL/XrML
- Semantics-enable of DRM policies
- Semantic enforcement of DRM system on the Web

**Current Status[14]**
- SWRL-based ontology+rule on ODRL
- Ontology-based usage and delegation rights of DRM
- Rule-based usage and delegation rights of DRM
- DRM policies for *fair use* of Intellectual Property (IP)
Part II

SemPIF: PIF + Meta-PIF
Well-Known Semantic Web Layer Cake (2007 Version)

User Interface & Applications

Trust

Proof

Unifying Logic

Query: SPARQL

Ontology: OWL

Rule: RIF

Data interchange: RDF

URI/IRI

Crypto

XML
SemPIF Extends Semantic Web
SemPIF’s Related Work

**Where Are Current Available Policy Frameworks?**

- W3C PLING
- OMG SBVR
- MIT DIG Rein
- FP6 REWERSE Protune
- FP6 IST-ESTRELLA LKIF

**What Is the Features of SemPIF**

- Extends from the Semantic Web architecture
- Explicitly decoupling meta-PIF from PIF
- Applying a combination of ontology+rule for PIF and meta-PIF
- SemPIF for various protection domains, e.g. privacy protection and DRM
SemPIF’s Related Work

WHERE ARE CURRENT AVAILABLE POLICY FRAMEWORKS?
- W3C PLING
- OMG SBVR
- MIT DIG Rein
- FP6 REWERSE Protune
- FP6 IST-ESTRELLA LKIF

WHAT IS THE FEATURES OF SemPIF
- Extends from the Semantic Web architecture
- Explicitly decoupling meta-PIF from PIF
- Applying a combination of ontology+rule for PIF and meta-PIF
- SemPIF for various protection domains, e.g. privacy protection and DRM
Part III

Semantics-Enabled Web Policies
What Do You Mean Policies?

- Declared as knowledge bases, i.e., ontologies or/and rules
- Reducing program coding to a minimum level
- Enabling automated documentation
- Framework supports policy interoperability
- Low deployment and maintenance cost
- Context of policy is machine understandable
- Maybe supports automatic negotiation between agents

Policy Specification, Enforcement, and Integration, **WG I2, REWERSE FP6**
What Do You Mean **Meta-Policy**?

- A policy about policies
- Providing a set of rules to enforce the adding and changing management services of multi-policies
- Setting up priority of polices to coordinate, enforce, and even negotiate multi-policies on the Web

Hosmer, H. H., Metapolicies I, ACM SIGSAC Review, 1992
XML-based Policy Lacks Semantics

**XML-based policies**

- XrML [17] ← digital rights expression language
- ODRL [16] ← digital rights expression language
- P3P [5] ← privacy rights expression language
- EP3P(EPAL) [1] ← privacy rights expression language
- XACML [1] ← general policy language
Pure FOL-based Policy Is Not Web-Enabled

**Formal semantics of DL (⊂ FOL) or LP for policies**

- Semantic ODRL [26] ⇐ FOL semantics
- Semantic XrML [10] ⇐ FOL semantics
- Semantic P3P [33] ⇐ relational semantics
- FAF [18] ⇐ LP semantics
- Semantic E-P3P (or EPAL) [1] ⇐ FAF semantics
- Rein, KAoS [31] ⇐ DL-based FOL semantics
- Protune [3] ⇐ LP semantics
Web policies from semantic web languages

- Ontology Languages: RDF(S), OWL-DL, OWL2
- Rules Languages: N3, RuleML, RIF
- Ontology+Rule Language: SWRL, OWL2+RIF

Web policies from ontology+rule

- Policy vs. Regulation (or Law)
- Policy Language vs. Policies
- Semantics-enabled Policy Language
- Semantic PIF
- Semantics-enabled Meta-PIF
Semantics-Enabled Web Policies

**Web Policies from Semantic Web Languages**
- Ontology Languages: RDF(S), OWL-DL, OWL2
- Rules Languages: N3, RuleML, RIF
- Ontology+Rule Language: SWRL, OWL2+RIF

**Web Policies from Ontology+Rule**
- Policy vs. Regulation (or Law)
- Policy Language vs. Policies
- Semantics-enabled Policy Language
- Semantic PIF
- Semantics-enabled Meta-PIF
Semantics-Enabled Web Policies

**Why use ontology+rule?**

- Exploiting semantic web research
- Two major knowledge representations
- Automatic machine processing of policies
- Choosing which ontology+rule is not easy!

**Why not use ontologies or rules alone?**

- Policies might be DL-based semantics and LP-based semantics
- Power enhancement of policies from ontologies and rules
- Different knowledge integration, interchange, and interoperation
- Options to use ontologies, rules or both
Semantics-Enabled Web Policies (conti.)

**Why use ontology+rule?**
- Exploiting semantic web research
- Two major knowledge representations
- Automatic machine processing of policies
- Choosing which ontology+rule is not easy!

**Why not use ontologies or rules alone?**
- Policies might be DL-based semantics and LP-based semantics
- Power enhancement of policies from ontologies and rules
- Different knowledge integration, interchange, and interoperation
- Options to use ontologies, rules or both
Which ontology+rule combination for Web Policies?

- We do not know yet!
- Decidability of computation
- Expressive power of ontology+rule
- Semantics differences between DL and LP
- Uni-(or bi-)directional of knowledge flow
- Homogeneous of ontology+rule
- Heterogeneous (or Hybrid)) of ontology+rule
Semantics-Enabled Web policies

**Homogeneous ontology + rule** [29]

- CARIN [20] (limited expressive power)
- Description Logic Program (DLP) [8] (too restricted)
- Semantic Web Rule Language (SWRL) [12] (undecidable unless DL-safe rules)
Future Semantics-Enabled Web Policies (conti.)

Hybrid ontology+rule [29]

**Positive Datalog rules**

- (Disjunctive)AL-log [6] $\iff$ decidability of $ALC$ plus positive, recursive DL-safe rules
- DL-safe rules [23] $\iff$ decidability of $SHOIN$ plus positive, recursive DL-safe rules

**Non-monotonic Datalog rules**

- DL-log safe hybrid Knowledge Bases [27] $\iff$ decidability of DLs/FOL plus non-monotonic, recursive DL-safe rules
- DL+log [28] $\iff$ decidability of arbitrary DLs plus non-monotonic, recursive weakly DL-safe rules
- Hybrid MKNF Knowledge Bases [22] $\iff$ mixing OWA and CWA reasoning in DL-safe rules
Future Semantics-Enabled Web Policies (conti.)

Hybrid ontology+rule [29]

Positive Datalog rules

- (Disjunctive)AL-log [6] ⇐ decidability of $ALC$ plus positive, recursive DL-safe rules
- DL-safe rules [23] ⇐ decidability of $SHOIN$ plus positive, recursive DL-safe rules

Non-monotonic Datalog rules

- DL-log safe hybrid Knowledge Bases [27] ⇐ decidability of DLs/FOL plus non-monotonic, recursive DL-safe rules
- Hybrid MKNF Knowledge Bases [22] ⇐ mixing OWA and CWA reasoning in DL-safe rules
Part IV

Privacy Protection
Privacy Protection on the Web

**Privacy Protection on Web 1.0**
- Privacy protection policies representation through natural language
- Static personal profile and digital traces
- Information disclosure policies and mechanisms are embedded together
- Does the website comply the policies announcement is unknown!

**Privacy Protection on Web 2.0**
- APPEL/P3P provides information disclosure’s opt-in/opt-out and negotiation mechanisms
- More challenging to protect a variety of dynamic digital traces
- Does the website comply the policies announcement is still unknown!
Privacy Protection on the Web

Privacy Protection on Web 1.0

- Privacy protection policies representation through natural language
- Static personal profile and digital traces
- Information disclosure policies and mechanisms are embedded together
- Does the website comply the policies announcement is unknown!

Privacy Protection on Web 2.0

- APPEL/P3P provides information disclosure’s opt-in/opt-out and negotiation mechanisms
- More challenging to protect a variety of dynamic digital traces
- Does the website comply the policies announcement is still unknown!
Privacy Protection on the Web

Privacy Protection on Web 3.0

- We have a separation of privacy protection protection policies and mechanisms.
- Personal profile and digital traces are semantics-enabled data model.
- Automatic enforcement of the semantics-enabled privacy protection policies
- Auditing and verifying the compliance of privacy policies to the laws
- Do we need Sound and complete semantics-enabled policies from the legal privacy laws?
Privacy Protection on Different Web Generations
Non-disclosure of recipient’s email address

1. Alice wants to send e-mail to Bob and Charlie

- **e-mail of Bob:**
  - from: Alice@gmail.com
  - to: Bob@yahoo.com.tw, Charlie@hotmail.com
  - Subject: Data-Auditing

- **e-mail of Charlie:**
  - from: Alice@gmail.com
  - to: Charlie@yahoo.com.tw
  - Subject: Data-Auditing

2. Bob doesn’t want to disclose his e-mail address to other recipients not in subsidiary company

3. Charlie will receive the e-mail without displaying the e-mail address of Bob
Data User Ontologies (conti.)
Data Type Ontologies (conti.)

```
DATA_TYPE
    PROFILE_DATA
    DIGITAL_TRACE
        MAIL_TRACE
        LOGIN_TRACE
    OFFICE_PROFILE
        O_PHONE
        O_EMAIL
        O_ORG
        NAME
    HOME_PROFILE
    MAIL_TRACE_ONLINE
    MAIL_TRACE_OFFLINE
    O_EMAIL_SENDER
    O_EMAIL_RECEIVER

Datatype property:

HAS_MAIL_TRACE
    domain
    range
    MAIL_TRACE
    EMAIL
    O_EMAIL_SENDER
    O_EMAIL_RECEIVER

HAS_MAIL_TRACE_ONLINE
    domain
    range

HAS_EMAIL_ADDRESS
    domain
    range
    NAME
    EMAIL

HAS_PHONE_NUMBER
    domain
    range
    NAME
    PHONE
```
Purpose Ontology (conti.)

- PURPOSE
  - MARKETING
    - EMAIL_MARKETING
    - PHONE_MARKETING
  - AUDIT Annunci.
    - ACCOUNT_AUDIT Annunci.
    - DATA_AUDIT Annunci.
  - ADMIN
Ontology Module

Example (Ontology Module’s Axiom)

- \textit{COMPANY} \sqsubseteq \textit{PRIVATE}
- \textit{PRIVATE} \sqsubseteq \textit{ORGANIZATION}
- \textit{OWNER} \sqsubseteq \textit{PERSON}
- \textit{COMPANY} \xrightarrow{\text{domain}} \text{HAS\_COOPERATIVE} \xrightarrow{\text{range}} \text{COMPANY}
- \textit{COMPANY} \xrightarrow{\text{domain}} \text{HAS\_SUBSIDIARY} \xrightarrow{\text{range}} \text{COMPANY}
- \text{HAS\_COOPERATIVE} \equiv \text{HAS\_COOPERATIVE}^-
- \textit{PERSON} \xrightarrow{\text{domain}} \text{IS\_STAFF\_OF} \xrightarrow{\text{range}} \text{ORGANIZATION}
- \text{MAIL\_TRACE} \xrightarrow{\text{domain}} \text{HAS\_MAIL\_TRACE} \xrightarrow{\text{range}} \text{EMAIL}
- \text{EMAIL} \sqsubseteq \exists \text{HAS\_MAIL\_TRACE\_ONLINE}^- . \text{O\_EMAIL\_SENDER}
- \text{EMAIL} \sqsubseteq \forall \text{HAS\_MAIL\_TRACE\_ONLINE} . \text{O\_EMAIL\_RECEIVER}
- \text{DATA\_AUDIT\_ANNOUN.} \sqsubseteq \text{AUDIT\_ANNOUN.}
Example (Ontology Module’s Axiom)

- \( COMPANY \sqsubseteq PRIVATE \)
- \( PRIVATE \sqsubseteq ORGANIZATION \)
- \( OWNER \sqsubseteq PERSON \)
- \( COMPANY \xrightarrow{\text{domain}} \text{HAS_COOPERATIVE} \xrightarrow{\text{range}} COMPANY \)
- \( COMPANY \xrightarrow{\text{domain}} \text{HAS_SUBSIDIARY} \xrightarrow{\text{range}} COMPANY \)
- \( \text{HAS_COOPERATIVE} \equiv \text{HAS_COOPERATIVE}^- \)
- \( PERSON \xrightarrow{\text{domain}} \text{IS_STAFF_OF} \xrightarrow{\text{range}} ORGANIZATION \)
- \( MAIL_TRACE \xrightarrow{\text{domain}} \text{HAS_MAIL_TRACE} \xrightarrow{\text{range}} EMAIL \)
- \( EMAIL \sqsubseteq \exists \text{HAS_MAIL_TRACE_ONLINE}^- . O_EMAIL_SENDER \)
- \( EMAIL \sqsubseteq \forall \text{HAS_MAIL_TRACE_ONLINE} . O_EMAIL_RECEIVER \)
- \( DATA_AUDIT_ANNO. \sqsubseteq AUDIT_ANNO. \)
Example (Ontology Module’s Facts)

- ORGANIZATION(G)
- HAS_SUBSIDIARY(G, J-Corp.)
- HAS_COOPERATIVE(G, Q-Corp.)
- IS_STAFF_OF(Alice, J-Corp.)
- IS_STAFF_OF(Bob, J-Corp.)
- IS_STAFF_OF(Charlie, Q-Corp.)
- HAS_EMAIL_ADDRESS (Charlie, Charlie@hotmail.com)
- O_EMAIL_RECEIVER(Bob@yahoo.com.tw)
- HAS_EMAIL_ADDRESS (Alice, Alice@gmail.com)
- HAS_EMAIL_ADDRESS (Bob, Bob@yahoo.com.tw)
- O_EMAIL_SENDER(Alice@gmail.com)
- O_EMAIL_RECEIVER (Charlie@hotmail.com)
- HAS_MAIL TRACE ONLINE (Alice@gmail.com, Bob@yahoo.com.tw)
- HAS_MAIL TRACE ONLINE (Alice@gmail.com, Charlie@hotmail.com)
Rule Module

Example (Rule Module’s Rules)

- \textit{cando(?c,?b-email, display)}
  \[ \Leftarrow \text{opt-in(?b,?b-email,?p)), data-user(?c), data-owner(?b), HAS_EMAIL_ADDRESS(?b,?b-email).} \quad \Leftarrow (a1) \]

- \textit{cando(?c,?b-email, nil)}
  \[ \Leftarrow \text{opt-out(?b,?b-email,?p)), data-user(?c), data-owner(?b), HAS_EMAIL_ADDRESS(?b,?b-email).} \quad \Leftarrow (a2) \]

- \textit{opt-in(?b,?b-email,?p)}
  \[ \Leftarrow \text{data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email), IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c,?c2), HAS_SUBSIDIARY(?c1,?c2), HAS_MAIL_TRACE_ONLINE(?a-email,?c-email), O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email).} \quad \Leftarrow (a3) \]

- \textit{opt-out(?b,?b-email,?p)}
  \[ \Leftarrow \text{data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email), IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c,?c2), HAS_COOPERATIVE(?c1,?c2), HAS_MAIL_TRACE_ONLINE(?a-email,?c-email), O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email).} \quad \Leftarrow (a4) \]
Example (Rule Module’s Rules)

- \textbf{cando(?c,?b-email, display)}
  \[ \Leftarrow \text{opt-in(?b,?b-email,?p)), data-user(?c), data-owner(?b), HAS_EMAIL_ADDRESS(?b,?b-email).} \quad \Leftarrow \text{(a1)} \]

- \textbf{cando(?c,?b-email, nill)}
  \[ \Leftarrow \text{opt-out(?b,?b-email,?p)), data-user(?c), data-owner(?b), HAS_EMAIL_ADDRESS(?b, ?b-email).} \quad \Leftarrow \text{(a2)} \]

- \textbf{opt-in(?b,?b-email,?p)}
  \[ \Leftarrow \text{data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email), IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_SUBSIDIARY(?c1,?c2), HAS_MAIL_TRACE_ONLINE(?a-email,?c-email), O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email).} \quad \Leftarrow \text{(a3)} \]

- \textbf{opt-out(?b,?b-email,?p)}
  \[ \Leftarrow \text{data-owner(?b), data-user(?c), purpose(?p), data-type(?b-email), IS_STAFF_OF(?b,?c1), IS_STAFF_OF(?c, ?c2), HAS_COOPERATIVE(?c1,?c2), HAS_MAIL_TRACE_ONLINE(?a-email,?c-email), O_EMAIL_SENDER(?a-email), O_EMAIL_RECEIVER(?c-email).} \quad \Leftarrow \text{(a4)} \]
Example (Rule Module’s Facts)

- data-user(Bob),
  data-owner(Bob),
- data-user(Charlie),
  data-owner(Charlie),
- purpose(data-auditing),
- data-type(Bob@yahoo.com.tw),
- data-type(Charlie@hotmail.com),
- opt-in(c,Charlie@yahoo.com,
  data-auditing),
- cando(Bob,Charlie@yahoo.com,display),
- cando(Charlie,Bob@yahoo.com.tw,nill),
- opt-out(b,Bob@yahoo.com.tw,
  data-auditing)
Part V

DIGITAL RIGHTS MANAGEMENT
**Definition (License Agreement)**

A principal $Prin_o$ allows another principal $Prin_{ui}$ to use an asset $r$ presumably owned by $Prin_o$, where $Prin_o$ is an asset owner, $Prin_{ui}$ is one of $n$ asset users, where $i \in (1, \cdots, n)$. 
Prerequisites Expressions

**Definition (Prerequisites of Agreement)**

A prerequisite is either a constraint, a requirement, or a condition of rights agreement. If all of the prerequisites are met, then policies say that the agreement’s users may perform the action for the license agreement’s assets.

**Definition (Prerequisites as Ontology Expressions)**

- MaxCardinality: $\leq \exists_u \text{hasUsageCount}_{\exists_p}\cdot\text{Asset}$
- MaxCardinality: $\leq \exists_t \text{hasTransferCount}_{\exists_p}\cdot\text{Asset}$
- Cardinality: $= \exists_a \text{hasPrepaid}_{\exists_p}\cdot\text{Party}$
- Validity of time interval $\forall \text{Time} \in (t_1, t_2)$:
  $\geq \exists_{t_1} \text{hasDateTime}_{\exists_p}\cdot\text{Time} \land \exists \leq_{t_2} \text{hasDateTime}_{\exists_p}\cdot\text{Time}$
Prerequisites Expressions

**Definition (prerequisites of agreement)**
A prerequisite is either a constraint, a requirement, or a condition of rights agreement. If all of the prerequisites are met, then policies say that the agreement’s users may perform the action for the license agreement’s assets.

**Definition (prerequisites as ontology expressions)**
- \(\text{MaxCardinality: } \leq \exists u \ hasUsageCount_{\exists p}.\text{Asset}\)
- \(\text{MaxCardinality: } \leq \exists t \ hasTransferCount_{\exists p}.\text{Asset}\)
- \(\text{Cardinality: } = \exists a \ hasPrepaid_{\exists p}.\text{Party}\)
- \(\text{Validity of time interval } \forall \text{Time } \in (t_1, t_2): \)
  \(\geq \exists t_1 \ hasDateTime_{\exists p}.\text{Time } \land \exists \leq t_2 \ hasDateTime_{\exists p}.\text{Time}\)
A Rights Delegation Ontology
Rights Delegation Policies

**Definition (usage (or transfer) rights delegation)**

The class and property terms in this rights delegation ontology will be considered as antecedents or conclusion(s) in the usage and transfer rights delegation rules to enforce real rights delegation inference.
Transfer Rights Delegation

**Definition (hasTransferRights)**
- **hasTransferRights** is an abstract property describing the transfer rights delegation of usage rights.
- The domain class of **hasTransferRights** is **Party** and the range class is **Asset**.

**Definition (delegate_g AND delegate_t)**
- **Prin_o** might use **delegate_g** to transfer usage rights only to **Prin_{ui}**, but does not delegate his transfer rights.
- **Prin_o** might use **delegate_t** for both usage and transfer rights to propagate further.
**Transfer Rights Delegation**

**Definition** \((\text{hasTransferRights})\)
- \(\text{hasTransferRights}\) is an abstract property describing the transfer rights delegation of usage rights.
- The domain class of \(\text{hasTransferRights}\) is \(\text{Party}\) and the range class is \(\text{Asset}\).

**Definition** (\(\text{delegate}_g\) AND \(\text{delegate}_t\))
- \(\text{Prin}_o\) might use \(\text{delegate}_g\) to transfer usage rights only to \(\text{Prin}_{ui}\), but does not delegate his transfer rights.
- \(\text{Prin}_o\) might use \(\text{delegate}_t\) for both usage and transfer rights to propagate further.
**Rules for Rights Transfer Delegation**

**Definition (rules for usage rights delegation)**

- \( \text{hasUsageRights}(?x, ?r) \land \text{hasTransferRights}(?x, ?r) \implies \text{hasUsageTransferRights}(?x, ?r) \iff (o1) \)

- \( \text{hasUsageTransferRights}(?x, ?r) \land \text{delegate}_g(?x, ?y) \land \text{hasPrepaid}(?y, ?a) \land < \exists_u \text{hasUsageCount}(?r) \implies \text{hasUsageRights}(?y, ?r) \iff (o2) \)

**Definition (rules for transfer rights delegation)**

- \( \text{hasUsageRights}(?x, ?r) \land < \exists_u \text{hasUsageCount}(?r) \land \geq \exists_{t_1} \text{hasDateTime}(?t) \land \leq \exists_{t_2} \text{hasDateTime}(?t) \implies \text{Permitted(Usage, ?r)} \iff (o3) \)

- \( \text{hasUsageTransferRights}(?x, ?r) \land \text{delegate}_t(?x, ?y) \land \text{hasPrepaid}(?y, ?a) \land \geq 1 \text{hasTransferCount}(?r) \implies \text{hasUsageTransferRights}(?y, ?r) \iff (o4) \)
**Definition (rules for usage rights delegation)**

- $\text{hasUsageRights}(\text{?x}, \text{?r}) \land \text{hasTransferRights}(\text{?x}, \text{?r}) \implies \text{hasUsageTransferRights}(\text{?x}, \text{?r}) \Leftarrow (o1)$

- $\text{hasUsageTransferRights}(\text{?x}, \text{?r}) \land \text{delegate}(\text{?x}, \text{?y}) \land \text{hasPrepaid}(\text{?y}, \text{?a}) \land \leq \exists u \\
\quad \text{hasUsageCount}(\text{?r}) \implies \text{hasUsageRights}(\text{?y}, \text{?r}) \Leftarrow (o2)$

**Definition (rules for transfer rights delegation)**

- $\text{hasUsageRights}(\text{?x}, \text{?r}) \land \leq \exists u \text{hasUsageCount}(\text{?r}) \land \geq \exists \text{hasDateTime}(\text{?t}) \land \leq \exists t_2 \\
\quad \text{hasDateTime}(\text{?t}) \implies \text{Permitted}(\text{Usage}, \text{?r}) \Leftarrow (o3)$

- $\text{hasUsageTransferRights}(\text{?x}, \text{?r}) \land \text{delegate}(\text{?x}, \text{?y}) \land \text{hasPrepaid}(\text{?y}, \text{?a}) \land \geq 1 \\
\quad \text{hasTransferCount}(\text{?r}) \implies \text{hasUsageTransferRights}(\text{?y}, \text{?r}) \Leftarrow (o4)$
Example

Content distributor Charlie c makes an agreement with two content consumers, Alice a and Bob b. After each paying five dollars, and then both receiving acknowledgement from Charlie, Alice and Bob are given the usage rights and may each display an eBook asset, Harry Potter and the Deathly Hallows, up to five times. They may each print it only once. However, the total number of actions, either displays or prints done by Alice and Bob, may be at most ten. The usage rights validity period is between 2007/05/07/09:00 - 2007/05/10/24:00.
Abstract Syntax of License Agreement

**Example**

agreement between Charlie and \{Alice, Bob\} about Harry Potter and the Deathly Hallows with inSequence[prePay[5.00], attribution[Charlie]]

\[⇒ \text{not[and[Time < 2007/05/07/09:00, Time > 2007/05/10/24:00]]} \implies \text{with count[10]}
\]

\[⇒ \text{and[forEachMember[Alice, Bob; count[5]]]}
\]

\[⇒ \text{display, forEachMember[Alice, Bob; count[1]]}
\]

\[⇒ \text{print]}

FOL of License Agreement

**Example**

\[\forall x ((x = Alice \lor x = Bob) \implies \exists t_1 \exists t_2 (t_1 < t_2 \land \text{Paid}(5, t_1) \land \text{Attributed}(Charlie, t_2))) \implies \]
\[\forall t \land \text{hasDateTime}(t) \geq 2007/05/07/09:00 \land \text{hasDateTime}(t) \leq 2007/05/10/24:00 \implies \]
\[\text{count}(Alice, id_1) + \text{count}(Alice, id_2) + \text{count}(Bob, id_1) + \text{count}(Bob, id_2) < 10 \implies \]
\[\text{count}(Alice, id_1) < 5 \land \text{count}(Bob, id_1) < 5 \implies \text{Permitted}(x, display, ebook)) \land\]
\[\text{count}(Alice, id_2) < 1 \land \text{count}(Bob, id_2) < 1 \implies \text{Permitted}(x, print, ebook))\]
Example (Ontology for content distributor Charlie)

- $\text{hasDisplayRights} \subseteq \text{hasUsageRights}$
- $\text{hasPrintRights} \subseteq \text{hasUsageRights}$
- $\leq (\text{hasDisplayCount}_{\{a,b\}}.\text{eBook}, \text{hasUsageCount}_c.\text{eBook})$
- $\leq (\text{hasPrintCount}_{\{a,b\}}.\text{eBook}, \text{hasUsageCount}_c.\text{eBook})$

- $\{\text{Alice, Bob}\} \overset{\text{domain}}{\leftarrow} \text{hasUsageRights} \overset{\text{range}}{\rightarrow} R_1$, where $R_1 = \leq 10 \text{hasUsageCount}_c \wedge 
\geq 2007/05/07/0900 \text{hasDateTime}_c.\text{Time} \wedge \leq 2007/05/10/2400 \text{hasDateTime}_c.\text{Time}$

- $\exists = \alpha \exists = \sum(\exists \leq 5 \text{hasDisplayCount}_i.\{\text{HarryPotter}\}), i \in \{a, b\}$, where $\alpha$:
  $\exists \text{hasDisplayCount}_c.\{\text{HarryPotter}\}$

- $\exists = \beta \exists = \sum(\exists \leq 1 \text{hasPrintCount}_i.\{\text{HarryPotter}\}), i \in \{a, b\}$, where $\beta$:
  $\exists \text{hasPrintCount}_c.\{\text{HarryPotter}\}$

- $\exists = \delta \sum(\alpha, \beta)$, where $\delta$:
  $\exists \text{hasUsageCount}_c.\{\text{HarryPotter}\}$
Ontologies for License Agreement

Example (Ontology for content distributor Charlie)

- hasDisplayRights ⊆ hasUsageRights
- hasPrintRights ⊆ hasUsageRights
- ≤ (hasDisplayCount\{a,b\}.eBook, hasUsageCount\_c.eBook)
- ≤ (hasPrintCount\{a,b\}.eBook, hasUsageCount\_c.eBook)
- \{Alice, Bob\} domain hasUsageRights range R\_1, where R\_1 = ≤10 hasUsageCount\_c \∧ ≥2007/05/07/0900 hasDateTime\_c.Time \∧ ≤2007/05/10/2400 hasDateTime\_c.Time
- ∃ = \_α \exists = sum(∃ ≤\_5 hasDisplayCount\_i.{HarryPotter}), \_i \in \{a, b\}, where \_α: \exists hasDisplayCount\_c.{HarryPotter}
- ∃ = \_β ∃ = sum(∃ ≤\_1 hasPrintCount\_i.{HarryPotter}), \_i \in \{a, b\}, where \_β: \exists hasPrintCount\_c.{HarryPotter}
- ∃ = \_δ sum(\_α, \_β), where \_δ: ∃ hasUsageCount\_c{HarryPotter}
Example (Rules for content distributor Charlie)

- \(\text{hasDisplayRights}(\text{x}, \text{r}) \land \text{hasSell}_d\text{Rights}(\text{x}, \text{r}) \implies \text{hasDisplaySell}_d\text{Rights}(\text{x}, \text{r})\)
- \(\text{hasPrintRights}(\text{x}, \text{r}) \land \text{hasSell}_d\text{Rights}(\text{x}, \text{r}) \implies \text{hasPrintSell}_d\text{Rights}(\text{x}, \text{r})\)
- \(\text{hasDisplaySell}_d\text{Rights}(\text{x}, \text{r}) \land \text{delegate}_g(\text{x}, \text{y}) \land \text{hasPrepaid}(\text{y}, \text{a}) \implies \text{hasDisplayRights}(\text{y}, \text{r})\)
- \(\text{hasPrintSell}_d\text{Rights}(\text{x}, \text{r}) \land \text{delegate}_g(\text{x}, \text{y}) \land \text{hasPrepaid}(\text{y}, \text{a}) \implies \text{hasPrintRights}(\text{y}, \text{r})\)
Example (Rules for content distributor Charlie)

- $\text{hasDisplayRights}(?x, ?r) \land \text{hasSell}_d\text{Rights}(?x, ?r) \implies \text{hasDisplaySell}_d\text{Rights}(?x, ?r)$
- $\text{hasPrintRights}(?x, ?r) \land \text{hasSell}_d\text{Rights}(?x, ?r) \implies \text{hasPrintSell}_d\text{Rights}(?x, ?r)$
- $\text{hasDisplaySell}_d\text{Rights}(?x, ?r) \land \text{delegate}_{g}(?x, ?y) \land \text{hasPrepaid}(?y, ?a) \implies \text{hasDisplayRights}(?y, ?r)$
- $\text{hasPrintSell}_d\text{Rights}(?x, ?r) \land \text{delegate}_{g}(?x, ?y) \land \text{hasPrepaid}(?y, ?a) \implies \text{hasPrintRights}(?y, ?r)$
Example (Facts for content distributor Charlie)

- eBook(HarryPotter)
- hasDisplayRights(Charlie,HarryPotter)
- hasPrintRights(Charlie,HarryPotter)
- hasSell_d_Rights(Charlie,HarryPotter)
- hasDisplaySell_d_Rights(Charlie,HarryPotter)
- hasPrintSell_d_Rights(Charlie,HarryPotter)

- ∃ =_5 hasPrepaid(Alice)
- hasDisplayRights(Alice,HarryPotter)
- hasPrintRights(Alice,HarryPotter)
- ∃ =_5 hasPrepaid(Bob)
- hasDisplayRights(Bob,HarryPotter)
- hasPrintRights(Bob,HarryPotter)

... ... ... ...
Part VI

SemPIF for DRM and Privacy Protection
What Are the Research Issues in SemPIF?

- Policy representation and enforcement in terms of knowledge systems, e.g., ontology + rule
- Multiple Web policies interoperability and management services
- Policies conflicts resolution for agents (or facilitators) to use SemPIF architecture
SemPIF framework for a Client Server Model

SemPIF Framework

- PIF
  - Ontologies + Rules
  - Meta-PIF

Facilitator

- Policy uploading
- Policy reconciliation

Client

NCCU library portal

Digital library portal

- Ontologies + Rules
- Semantic DRM / PP Policies
- ODRL, XACML
- XrML, EPAL, P3P

Ontology mapping, rule interchange

Policy modifying, deleting, reconciling, etc.
A PIF-based Privacy Protection Ontology
A PIF-based DRM Ontology
A Web Server’s DRM Policy
Natural (Controlled) Language

**EXAMPLE** *(Policy ID: drm1-IEEE)*

*If a Student owns a valid student ID (StudentID) issued by the Registrar of a University and the Library of the University is one of the subscribers in the IEEE publisher list, then the student is endowed with DRM usage rights \{download, view, print\} of an EJournal from a Web server of the IEEE publisher.*
EXAMPLE (Policy ID: drm1-IEEE)

\[\text{?st#Student} \land \text{?id#StudentID} \land \text{?uni#University} \land \text{?rg#Registrar} \land \text{?lib#Library} \land \text{?ejr#EJournal} \land \text{?usrgt#UsageRight} \land \text{?st[own \rightarrow ?id]} \land \text{?uni[hasPart \rightarrow ?rg]} \land \text{?st[enrolledAt \rightarrow ?uni]} \land \text{?rg[issue \rightarrow ?id]} \land \text{?uni[hasPart \rightarrow ?lib]} \land \text{?lib[subscribedTo \rightarrow IEEE]} \land \text{IEEE[hasPublished \rightarrow ?ejr]} \land \text{IEEE[endowedWith \rightarrow ?usrgt]} \land \text{?usrgt[appliedTo \rightarrow ?ejr]} \mapsto \text{IEEE[delegate \rightarrow ?st]} \land \text{?st[endowedWith \rightarrow ?d]} \land \text{?st[endowedWith \rightarrow ?v]} \land \text{?st[endowedWith \rightarrow ?p]} \land \text{?d# Download} \land \text{?d[appliedTo \rightarrow ?ejr]} \land \text{?v#View} \land \text{?v[appliedTo \rightarrow ?ejr]} \land \text{?p#Print} \land \text{?p[appliedTo \rightarrow ?ejr]}\]
EXAMPLE (Policy ID: drm1-IEEE)

If a Student owns a valid student ID (StudentID) issued by the Registrar of a University and the Library of the University is one of the subscribers in the IEEE publisher list, then the student is endowed with DRM usage rights \{download, view, print\} of an EJournal from a Web server of the IEEE publisher.
A Web Server’s Privacy Policy

**OWL2+RIF**

**EXAMPLE (Policy ID: pp1-IEEE)**

\[
\text{\texttt{\texttt{\texttt{\texttt{?per#Person} \land \?usrgt#UsageRight} \land \?ejr#EJournal} \land \land \?prfl#Profile} \land \?trc#Trace} \\
\land \?prrgt#PrivacyRight} \land \?per[endowedWith} \rightarrow \?usrgt]} \land \?usrgt[appliedTo} \rightarrow \?ejr]} \\
\land \text{\texttt{IEEE[hasPublished} \rightarrow \?ejr]} \land \text{\texttt{IEEE[hasPrivacyOf} \rightarrow \texttt{DRMControl}}} \\
\land \text{\texttt{?per[hasPart} \rightarrow \?prfl]} \land \text{\texttt{?per[hasPart} \rightarrow \?trc]} \land \text{\texttt{?per[endowedWith} \rightarrow \?prrgt]} \\
\implies \?per[delegate} \rightarrow \texttt{IEEE]} \land \texttt{IEEE[temporarilyAssume} \rightarrow \?prrgt]} \\
\land \?prrgt[hasDuration} \rightarrow \texttt{month(2)}]\] \\
\land \texttt{?prrgt[appliedTo} \rightarrow \?prfl]} \land \texttt{?prrgt[appliedTo} \rightarrow \?trc]} \\
\land \texttt{?c#Collect} \land \texttt{?c[appliedTo} \rightarrow \?prfl]} \land \texttt{?c[appliedTo} \rightarrow \?trc]} \\
\land \texttt{?r#Retain} \land \texttt{?r[appliedTo} \rightarrow \?prfl]} \land \texttt{?r[appliedTo} \rightarrow \?trc]} \\
\land \texttt{?i#Disclose} \land \texttt{?i[appliedTo} \rightarrow \?prfl]} \land \texttt{?i[appliedTo} \rightarrow \?trc]}.\]
A Web User’s Privacy Policy
Natural (Controlled) Language

Policy ID: pp5-John

*If an EJournal Publisher other than IEEE has the purpose of enforcing DRM control of collecting, retaining, and disclosing on John’s data then it temporarily assumes privacy rights \{collect, retain\} on John’s digital Traces under the condition of a retention period less than seven days.*

Policy ID: pp6-John

*If the IEEE EJournal Publisher has the purpose of enforcing DRM control of collecting, retaining, and disclosing on John’s data then it temporarily assumes privacy rights \{collect, retain\} on John’s digital Traces under the condition of retention period less than fourteen days.*
Policy ID: pp5-John

If an EJournal Publisher other than IEEE has the purpose of enforcing DRM control of collecting, retaining, and disclosing on John’s data then it temporarily assumes privacy rights \{collect, retain\} on John’s digital Traces under the condition of a retention period less than seven days.

Policy ID: pp6-John

If the IEEE EJournal Publisher has the purpose of enforcing DRM control of collecting, retaining, and disclosing on John’s data then it temporarily assumes privacy rights \{collect, retain\} on John’s digital Traces under the condition of retention period less than fourteen days.
Discussion
Policy Representation and Enforcement

**Natural Language**
- **Pros:** human readable and understandable
- **Cons:** machine unfriendly but no formal semantics for the machine

**Pure FOL**
- **Pros:** formal and clear syntax and semantics
- **Cons:** machine unfriendly, possibly undecidable computation complexity, and policies writer (reader) needs to be a logician
**Natural Language**
- **Pros**: human readable and understandable
- **Cons**: machine unfriendly but no formal semantics for the machine

**Pure FOL**
- **Pros**: formal and clear syntax and semantics
- **Cons**: machine unfriendly, possibly undecidable computation complexity, and policies writer (reader) needs to be a logician
Discussion (conti.)
Policy Representation and Enforcement

**Rights Expression Languages**
- **Pros**: XML-based documents for machine processing
- **Cons**: no formal semantics for the machine

**Ontology+Rule with XML Presentation Syntax**
- **Pros**: formal semantics for automatic machine processing and understanding
- **Cons**: limited expressing power under certain conditions, such as negation-free, function-free, and with limited number of parameters in the Datalog
Discussion (conti.)
Policy Representation and Enforcement

**Rights Expression Languages**
- **Pros:** XML-based documents for machine processing
- **Cons:** no formal semantics for the machine

**Ontology+Rule with XML Presentation Syntax**
- **Pros:** formal semantics for automatic machine processing and understanding
- **Cons:** limited expressing power under certain conditions, such as negation-free, function-free, and with limited number of parameters in the Datalog
Policy Languages for Access Rights Permission

Access Control Policies

License Agreements

Unifying Semantic

RELs

Hybrid Ontologies + Rules Integration

Logic Program (LP)

Datalog

Non-recursive

Recursive

Monotonic

Non-monotonic

RuleML

RIF

First Order Logic (FOL)

Decidable

Undecidable

Tractable (polynomial)

Intractable (exponential)

ODRL

XRL

EPAL

XACML

RDF(S)

Rei

KQeS

AL-Log

DL-Log

OWL-Lite

OWL-DL

OWL-Full

Lithium
Conclusion and Future Work

- Semantics-enabled policies for DRM, privacy protection, and both
- Semantics-enabled DRM policies in terms of SWRL with ODRL.
- Semantics-enabled of privacy protection policies in terms of a combination of ontology+rule with P3P.
- SemPIF policy layered architecture is proposed for the following purposes:
  1. SemPIF extends W3C’s semantic web architecture.
  2. Policy in Policy Interchange Format (PIF) is available for facilitators (or agents) to provide regular policy interchange services.
  3. Meta-policy in meta-PIF is available for facilitators (or agents) to provide the management services for PIF-based policies and regular policies in the current and future policy languages.
  4. Three scenarios for each protection domain have been given to demonstrate our applicable approaches.
Conclusion and Future Work

- Semantics-enabled policies for DRM, privacy protection, and both
- Semantics-enabled DRM policies in terms of SWRL with ODRL.
- Semantics-enabled of privacy protection policies in terms of a combination of ontology+rule with P3P.
- SemPIF policy layered architecture is proposed for the following purposes:
  1. SemPIF extends W3C’s semantic web architecture.
  2. Policy in Policy Interchange Format (PIF) is available for facilitators (or agents) to provide regular policy interchange services.
  3. Meta-policy in meta-PIF is available for facilitators (or agents) to provide the management services for PIF-based policies and regular policies in the current and future policy languages.
  4. Three scenarios for each protection domain have been given to demonstrate our applicable approaches.
A. H. Anderson.
A comparison of two privacy policy languages: EPAL and XACML.

M. Blaze, J. Figenebaum, and M. Strauss.
Compliance checking in the policymaker trust management system.

Bonatti, P. and D. Olmedilla.
Policy language specification, enforcement, and integration
*Project Deliverable D2, Working Group I2, REWERSE, 2005*

A. Borgida.
On the relative expressiveness of description logic and predicate logics.

L. Cranor et al.
The platform for privacy preferences (p3p) 1.0 (p3p 1.0) specification, 2002.
http://www.w3.org/P3P/.

M. F. Donini et al.
AL-log: Integrating Datalog and description logics.

Formalising ODRL semantics using web ontologies.
http://odrl.net/workshop2005/.

N. B. Grosof et al.
Description logic programs: Combining logic programs with description logic.

S. Guth, G. Neumann, and M. Strembeck.
Experiences with the enforcement of access rights extracted from ODRL-based digital contracts.

Joseph Y. Halpern and Vicky Weissman.
A formal foundation for XrML.
Y. J. Halpern and V. Weissman.
Using first-order logic to reason about policies.

I. Horrocks et al.
http://www.w3.org/Submission/SWRL/.

Ian Horrocks et al.
OWL rules: A proposal and prototype implementation.

Y. J. Hu.
Semantic-driven enforcement of rights delegation policies via the combination of rules and ontologies.

Semantic enforcement of privacy protection policies via the combination of ontologies and rules.
R. Iannella.
Open digital rights language (ODRL), version 1.1.
http://www.w3.org/TR/odrl/.

ContentGuard Inc.
eXtensible rights Markup Language (XrML), ver. 2.0.
http://www.xrml.org/index.asp.

S. Jajodia et al.
Flexible support for multiple access control policies.

A. B. LaMacchia.
Key challenges in DRM: An industry perspective.
CARIN: A representation language combining horn rules and description logics.

N. Li, B. N. Grosof, and J. Feigenbaum.
Delegation logic: A logic-based approach to distributed authorization.

B. Motik et al.
Can OWL and logic programming live together happily ever after?

B. Motik, U. Sattler, and R. Studer.
Query answering for OWL-DL with rules.

J. Pan and I. Horrocks.
Web ontology reasoning with datatype groups.

The UCON\textsubscript{ABC} usage control model.


R. Pucella and V. Weissman.
A formal foundation for ODRL.

R. Rosati.
On the decidability and complexity of integrating ontologies and rules.

R. Rosati.
\textit{DL}+\textit{log}: Tight integration of description logics and disjunctive Datalog.

R. Rosati.
Integrating ontologies and rules: Semantic and computational issues.

M. Stefik.
Letting loose the light: Igniting commerce in electronic publication.

G. Tonti et al.

D. J. Weitzner et al.
Creating a policy-aware web: Discretionary, rule-based access for the world wide web.

T. Yu, A. N. Li, and I. Antón.
A formal semantics for p3p.
http://citeseer.ist.psu.edu/750176.html.