# Unifying Semantic Privacy Protection Web Policies for the Digital Rights Management (DRM) System

Yuh-Jong Hu
*Dept. of Computer Science,*
*National Chengchi University, Taipei, Taiwan*
*hu@cs.nccu.edu.tw*

**Abstract**

There are several right expression languages (RELs) for the information model of data or content protection representation on the Web. For example, P3P/EPAL exists for privacy data protection and ODRL/XrML is used for digital rights control in the digital rights management (DRM) system. However, these XML-based RELs lack the ability to express the semantics of the web protection policies unambiguously enough for as a software program to process them automatically. We need declarative semantics-enabled policies formulated as knowledge bases, i.e., ontologies and/or rules to solve this problem. Here, we consider employing a combination of ontologies and rules as a semantic model of the REL so that the power of Description Logic (DL) for ontologies and Logic Program (LP) for rules can be leveraged simultaneously. In fact, using different ontology and rule $\mathcal{O} + \mathcal{R}$ combinations, such as DLP, SWRL, and OWL 2 RL for the RELs implies variant semantic expressions that can be derived from DL and LP. Certainly, a semantic model of the REL based on $\mathcal{O} + \mathcal{R}$ will affect the robustness of semantics fulfillment for a protection policy. We propose a semantics-enabled policy framework, where privacy protection policies are unified with the digital rights policies in the DRM system. The customizable privacy protection of the DRM system satisfies a server's privacy protection promise to its users.

## 1 Introduction

We envision a promising future for the use of standardized rights expression languages (RELs) for privacy protection policy's representations in the digital rights management (DRM) system. The objective of a DRM system is to allow the legal sharing of digital content with a content owner's consent. In addition, we expect that this DRM system should also protect each content user's privacy rights. It will be a grand challenge to use RELs, such as XACML, for access control policies with an additional protection of a user's privacy in the DRM system . Moreover, we can enforce the web protection policies in a machine for digital content and personal information access control without too much human intervention. Several RELs, such as ODRL and P3P already have the capacity to represent digital content control policies in a digital rights license agreement for a server and privacy protection policies for a client. More specifically, ODRL and XrML have been proposed as RELs to express the digital content usage contracts in the DRM system [ContentGuard, 2002] [Guth & Iannella, 2005b]. P3P and EPAL are other RELs used to express privacy statements in protection policies, in order for a server to fulfil its privacy protection promises to its users regarding information disclosure [Antón et al., 2007].

However, the progress of modeling semantics for RELs has either gone unnoticed or exists at a very primitive stage [ContentGuard, 2002] [Guth & Iannella, 2007]. In general, the semantics of REL was previously shown as English descriptions or as computer algorithms that grant the access right permissions based on a set of license agreements. These approaches are quite inflexible and inextensible as are the semantics-enabled web policies. Therefore, the building of a formal semantic model from a variety of RELs for web protection policies has recently become a highly significant research area, such as research into XrML and ODRL for digital rights [Halpern, 2008] [Pucella & Weissman, 2006], and APPEL/P3P for privacy rights [Yu et al., 2004] [Li et al., 2006].

Theoretically, any XML-based RELs, such as ODRL and XrML do not have unambiguous expressive power to declare and enforce the semantics of the web policies in their information models unless we have a corresponding ontology language, such as the model theory found in RDF(S), OWL [Patel-Schneider & Siméon, 2002]. Another option for REL's formal semantics is a logic program (LP)-based datalog rule. The formal semantics of the ODRL and XrML RELs were recently modeled as a First-Order Logic (FOL) [Pucella & Weissman, 2006] [Halpern, 2008]. In these studies, authors showed how to express a decidable fragment of the FOL as the semantics of REL for a license agreement. XACML and EPAL are other XML-based RELs proposed to address the issue of information disclosure control in privacy protection systems [Anderson, 2006]. In fact, XACML is also a general access control language for usage control of digital content in the DRM system.

EPAL [Karjoth & Schunter, 2002], which was derived from the FAF model [Jajodia et al., 2001] was proposed for use in the enterprise's privacy protection policies on the web. When the information usage control for the privacy protection is similar to the content usage access control for the DRM, sensitive personal information may possibly be disseminated over the entire web without a user's consent. The semantic representation model of EPAL is far from satisfactory, because EPAL is only based on a logic program, so it lacks a well-defined semantics for its structure data model to specify the data access control policies.

In this chapter, we introduce the current status of numerous RELs for privacy protection and digital rights management. Then, we survey a taxonomy of existing semantics or not-semantics-enabled policy languages. Third, we demonstrate how semantic web policy language can be constructed from the REL by using a combination of ontologies and rules. After that, we propose a semantics-enabled policy framework for unifying the semantic privacy protection policies and the digital rights management policies in the DRM system. Finally, we provide a scenario of digital content subscription services to demonstrate how to apply our semantics-enable policies in the framework to unify privacy protection policies with digital rights policies in the DRM system .

## 2 Goal

The major criteria we need to consider when designing a formal semantic model for a privacy protection system are not the same as when designing a DRM system. Therefore, we propose a unifying semantic model to resolve the criteria discrepancy between privacy protection and content usage control in the DRM system. For instance, when a data user submits an information disclosure request, EPAL-based policy uses a purpose criterion of data usage from the data user. But in a DRM content usage control policy, when we apply ODRL and XrML RELs we do not consider a data user's purpose criterion. The truth is most DRM systems, do not consider using a purpose criterion unless a fair use or personal privacy protection rights are requested by the DRM's users. But these are statutory rights granted by the Copyright Act and privacy protection law. Therefore, the DRM system eventually has to enforce the fair use and privacy protection rights for their content users [Arnab & Hutchison, 2005] [Erickson, 2003].

The goal of this chapter is to resolve the lack of the formal semantics problem in RELs in web policies' representation and enforcement as we design privacy protection policies in the DRM system. Current *de facto* RELs, such as P3P, ODRL, XACML, etc usually exist semantic ambiguity in the representation of license agreements and access control policies. Instead of using hard-coded computer algorithms or natural language descriptions, we propose a unifying formal semantic model that can be overlaid on the existing RELs to express and enforce the access control web policies. Under this unifying formal semantic model, the semantics-enabled REL can be used to express license agreements based on associated web policies to achieve rights protection when enforced by software programs without causing ambiguity.

## 3 Taxonomy of policy languages

The term "policy" encompasses different notions and usages, including security policies, trust management policies, business rules, etc. Computer policy is an executable and declarative rule that is created from a specific policy language to regulate the behavior of entities on the web [Vimercati et al., 2007]. Requirements for designing policies from a policy language are declarative, and have well-defined semantics, ontology support, rule support, and after-disclosure control, etc [Bonatti et al., 2006]. We select several well-known declarative RELs and policy languages and categorize them as follows:

- XML-based RELs (not semantics-enabled): P3P [Cranor et al., 2002], ODRL, XrML
- XML-based policy language (not semantics-enabled): XACML [Anderson, 2006], WS-Policy
- Logic Program (LP)-based policy language (semantics-enabled): EPAL [Antoniou et al., 2007]
- Description Logic (DL)-based policy language (semantics-enabled): KAoS, Rei [Tonti et al., 2003]
- $\mathcal{O} + \mathcal{R}$-based policy language (semantics-enabled): Protune [Bonatti et al., 2006], AIR[1]

We will argue why we need a formal semantic model based on a combination of ontologies and rules $\mathcal{O} + \mathcal{R}$ but not on an ontology $\mathcal{O}$ or a rule $\mathcal{R}$ alone. Moreover, the important criteria that people use to select a $\mathcal{O} + \mathcal{R}$ for web policy's semantics representation will also also be shown. We propose a unifying formal semantic model based on a particular $\mathcal{O} + \mathcal{R}$ with DL-based ontologies and LP-based datalog rules. This semantics-enabled web policy provides clear and decidable semantic enforcement of access control policies to ensure a user's privacy rights or a server's content digital rights.

## 4 REL, license agreement, policy, and rights protection

The $UCON_{ABC}$ model provides a solution for the content usage right control in the DRM and other similar problems, such as privacy protection, etc [Park & Sandhu, 2004]. This $UCON_{ABC}$ access control model uses *Authorization(A), oBligations(B), and Conditions(C)* as specifications for its access control policy. In fact, usage control is a generalization of a regular access control that covers authorization, obligations, conditions, continuity (ongoing controls), and mutability attributes. The $UCON_{ABC}$ model improves the original server-based access control approach, which cannot be used for usage and rights protection on the web. The $UCON_{ABC}$ model still cannot provide after-disclosure control because the original data owner is hard-pressed to enforce its protection policies once the digital content or personal information is disseminated on the web.

[1] **A**MORD **I**n **R**DF (**AIR**), `http://dig.csail.mit.edu/TAMI/2007/AIR/`

### 4.1 REL for a license agreement

A rights expression language (REL) provides an information modelling format for representing the digital rights usage and delegation on the web. The RELs are used for digital license agreements, access control policies, and rights protection systems. A license agreement is an instance of a digital contract for participants under which a principal, $\texttt{Prin}_o$ allows another principal, $\texttt{Prin}_u$ to use an asset, `r`, presumably owned (or controlled) by $\texttt{Prin}_o$. $\texttt{Prin}_o$ is an asset owner and $\texttt{Prin}_u$ is an asset user. We might also allow a license agreement specifically for a single asset owner to have multiple asset users, but to formalize the expressions and to enforce a license agreement without any ambiguous semantics is more challenging in this case.

A license agreement supports the expression of rights that are formal digital contracts, but there is no guarantee of clear semantics to stipulate the content, terms and conditions of rights usage for all the parties involved in this agreement. Formally speaking, a license agreement must contain at least one `asset` entity, at least one `permission` and `prohibition` entity, at least one `party` entity with an `assigner` role, and at least one `party` with `assignee(s)`(or `consumer(s)`) role(s) [Guth & Iannella, 2007].

### 4.2 REL for an access control policy

Most existing XML-based standard RELs, such as XACML and EPAL, only have vocabularies consisting of terms and conditions for protected resources. As a standard REL for privacy protection, XACML was compared with EPAL on the privacy policy enforcement and decisions [Anderson, 2006]. On the other hand, ODRL and XrML are intended to provide models for an access control policy on content publishing, distribution and consuming in the DRM system [ContentGuard, 2002] [Guth & Iannella, 2005b].

Although these RELs have a formal information model to express assets usage rights, obligations of conditions and requirements, the semantics used by these RELs to represent and enforce access control policies are sometimes ambiguous. ODRL specifications simply contain expression language, data dictionary elements, and XML syntax to encode the DRM's expressions and elements. However, ODRL does not enforce or mandate any rights protection policies for the DRM system. It only provides expressions of the policies for digital rights [Guth & Iannella, 2005b].

### 4.3 A rights protection system

Even REL contains enough necessary vocabularies to specify a license agreement with a formal information model to express the access control web policies. But we still need a run time engine to derive a permission (or not permission) in the rights protection system when we use these web policies for each service request. The information usage and delegation rights are shown as web policies to achieve after-disclosure control when enforced in a rights protection system. It processes a license agreement by execution the respective protection policies, which semantics are described as an algorithm or logic-based declarative ontologies and rules.

## 5 A formal semantic model

We propose a unifying formal semantic model of REL based on ODRL for DRM and P3P/EPAL for privacy protection. A semantics-enabled license agreement is a digital contract created from this model to describe the concepts of protection for content usage rights and user privacy rights. Furthermore, the semantics-enabled access control policies are also represented in the same model to enforce the privacy protection in the DRM system (see Figure 1).

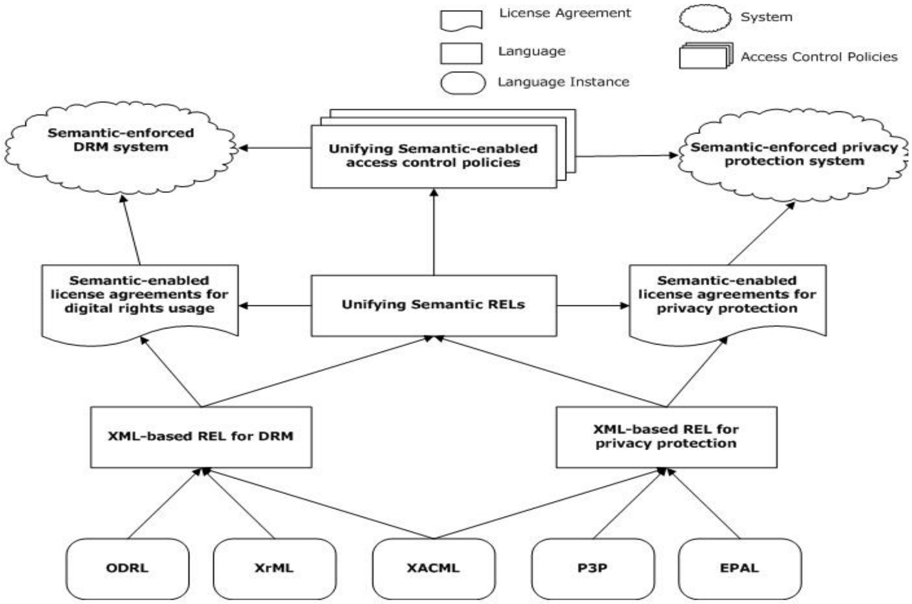
License Agreement
System
Language
Access Control Policies
Language Instance
Semantic-enforced DRM system
Unifying Semantic-enabled access control policies
Semantic-enforced privacy protection system
Semantic-enabled license agreements for digital rights usage
Unifying Semantic RELs
Semantic-enabled license agreements for privacy protection
XML-based REL for DRM
XML-based REL for privacy protection
ODRL
XrML
XACML
P3P
EPAL

**Figure 1:** A unifying semantic model of REL for describing license agreements and associated access control policies for privacy protection in the DRM system

### 5.1 FOL as a formal semantic model

In [Halpern, 2008] [Pucella & Weissman, 2006], a formal FOL foundation was elaborated to find out what are the tractable fragments for ODRL and XrML that provide the verification of access control permission implied by a set of licenses and policies. This result has a strong impact on the revised new version of ODRL and XrML information models [Guth & Iannella, 2005a] [Guth & Iannella, 2007].

However, the FOL-based formal semantic model is far from perfect because the tractable fragments of FOL for REL do not allow the updating of a license agreement conditions with its policies. Moreover, communication mechanisms between protection systems cannot be defined as a simple FOL-based REL. Therefore, it is impossible to deploy a generic FOL-based formal semantic model on the web unless we have web-enabled supporting markup languages, similar to RDF(S) and OWL ontology languages to express its semantics.

### 5.2 DL as a formal semantic model

A DL-based formal semantic model of REL provides the taxonomy of digital asset and usage rights as an ontology `TBox` for a DL-based reasoning engine, such as Racer or Pellet to decide the hierarchy implicit relationships [Garcia et al., 2005]. We can further use the standardized ontology languages, such as RDF(S) and OWL, to enforce the rights protection policies deployed on the web. Since DL is a subset of FOL, the limitations of expressive power in DL is similar to that in FOL for the updating of a license agreement and on the enabling of a message passing between the rights protection systems. This prevents us from building a full scale rights protection system on the web [Hu, 2007].

### 5.3 LP as a formal semantic model

The representations of LP-based FAF semantics and relational semantics were shown previously in the formal semantic models of EPAL and P3P [Antoniou et al., 2007] [Yu et al., 2004]. In order to have a decidable computational complexity for a rule language, the fragment of LP-based expressions are usually restricted to datalog rules with no function parameter within the predicates of each rule. However, a LP-based formal semantic model for REL has limitations on the representation of the concept and relationship hierarchy that prevent us from easily modeling the rights protection policies and their underlying REL's terms for rights, obligations, and usage conditions of protected resources.

### 5.4 $\mathcal{O} + \mathcal{R}$ as a formal semantic model

We exploited one of the homogeneous $\mathcal{O} + \mathcal{R}$ combinations, i.e., SWRL for the semantic representation and reasoning of a license agreement with its policies in the semantic DRM [Hu, 2007]. SWRL combines OWL-DL's ontology language with an additional datalog rule language, where a datalog rule language is shown as an axiom of ontology, a little extension of the OWL-DL language that overcomes the limitations of property chaining in the OWL-DL language [Horrocks et al., 2005]. The computation complexity of answering SWRL-based policies might be undecidable regarding the verification of rights access permission unless these policies satisfy the $\mathtt{DL} - \mathtt{Safe}$ conditions [Motik et al., 2004]. Moreover, SWRL did not include reactive rules, such as an event-condition-action (ECA) rule or production rule in its language design. Therefore, it is also impossible to provide the function of message passing by using SWRL-based policies alone in the protection systems.

## 6 Semantic REL for license agreements and protection policies

Ontology specifies the unambiguous concepts in a well-defined format for agents to process and understand. We have ontology languages, such as RDF(S) and OWL, to provide a well-defined standardized vocabulary to specify the concept and relationship of an ontology. Rule languages based on a (declarative) datalog rule, such as RuleML and RIF, can further enhance the expressive power of the ontology language to enforce information querying, updating, and communication related actions [Boley et al., 2007].

### 6.1 Semantic REL as an $\mathcal{O} + \mathcal{R}$ combination

Ontologies and rules based on logic foundations, i.e. description logic (DL) and logic program (LP) are primary knowledge representations. Ontologies based on DL are a subset of FOL that represents the shared knowledge domain of concepts and roles. On the other hand, rules based on datalog of LP are also a subset of FOL with the expressive power to overcome the limitations of ontology. Furthermore, reactive rules provide additional power, such as event acceptance and action trigger to enable data communication and updating operations [Berstel et al., 2007].

We propose a unifying semantic model of REL in license agreement and web protection policies for the verification of access rights permission in the DRM system (see Figure 2)

The benefits of using $\mathcal{O} + \mathcal{R}$ combination as the semantic model of REL are shown as follows:

- More expressive power for the semantics representations from ontologies and rules.
- Standardized web-enabled ontology language and rule language are possibly available for agents to automatically process license agreements and policies without facing semantics ambiguity.
- A flexible and scalable reasoning engine are available from DL and LP for executing the privacy protection policies in the DRM system.

The important criteria for using an $\mathcal{O} + \mathcal{R}$ combination as a semantic model of REL are shown as follows:

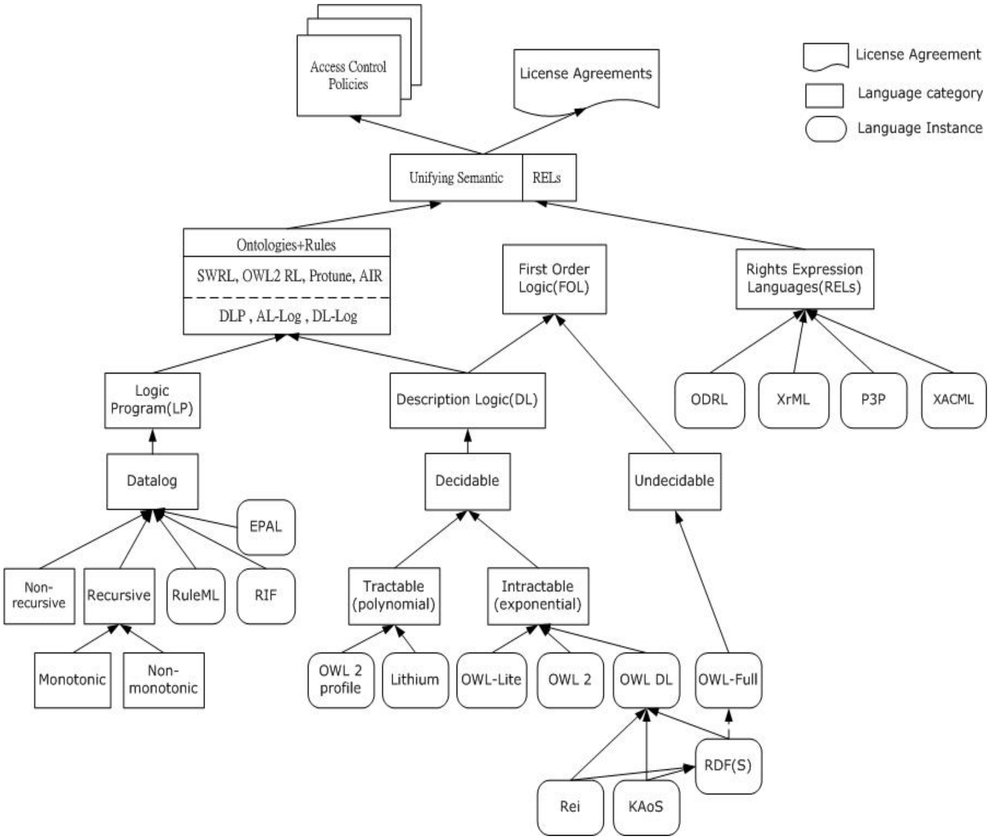

**Figure 2:** A unifying semantic model of REL from FOL, LP, RELs for license agreements and access control policies

- To use an $\mathcal{O} + \mathcal{R}$ combination which has a decidable computation fragment. Otherwise, we might not be able to obtain an answer for every rights permission query.
- To decide what semantic expressions of REL are from ontologies and rules.
- To resolve the semantic assumption of difference between ontologies and rules. DL-based ontology is an open world assumption (OWA) but an LP-based rule is a closed world assumption (CWA). This difference has side effects on the decision of protection policy when enforced.
- To have a bi-directional or a uni-directional information flow from ontologies to rules. In a uni-directional case, concepts and properties in the ontology are used to specify unary and binary predicates in the rules. In a bi-directional case, reaction rules provide the updating of the facts, e.g. $\mathcal{AB}\wr\S$ for the ontology.

There are two types of $\mathcal{O} + \mathcal{R}$ combinations [Eiter & Ianni, 2008]: homogeneous (tight) integration and heterogeneous (loose) integration. *DLP* [Grosof et al., 2003], *SWRL* [Horrocks et al., 2005], and *OWL 2 RL* [Grau et al., 2008] are a type of tight $\mathcal{O} + \mathcal{R}$ integration. *DLP* is too restricted to use for ontology and in the license agreements and web policies. On the other hand, *SWRL* might have a fragment of undecidable computation on the decision of rights permission unless we request that all of the rules satisfy the $\mathtt{DL-Safe}$ condition[2]. Another *OWL 2 RL* [Hitzler et al., 2010] is an emerging $\mathcal{O}+\mathcal{R}$ combination, and thus needs further study.

*AL-log* [Donini et al., 1998] and *DL-log* are $\mathcal{O}+\mathcal{R}$ heterogeneous combinations. *AL-log* has decidable computation to answer a request of license or privacy rights. *AL-log* is based on *A*ttribute *L*anguage with *C*omplements (*ALC*) of the DL-based ontology for monotonic (positive) recursive $\mathtt{DL-Safe}$ datalog rules. The other is *DL-log*, which has a decidable computation from the decidable DL-based ontologies and non-monotonic, recursive $\mathtt{DL-Safe}$ datalog rules [Rosati, 2006]. In this study, we use a SWRL-based $\mathcal{O}+\mathcal{R}$ combination with the satisfaction of $\mathtt{DL-Safe}$ conditions to avoid the undecidable computation of decisions for each request for license or privacy rights.

### 6.2 A unifying semantic model of REL

The future of online privacy will be closely linked to copyright enforcement in the DRM system [Feigenbaum et al., 2002]. In the past, personal information and digital traces could be easily collected and a dossier of the user's preferences could be built by the DRM system. In order to avoid information disclosure without a user's awareness and agreement, we propose a unifying semantic model of REL based on a SWRL-based $\mathcal{O}+\mathcal{R}$ combination, where the features of privacy protection can be incorporated into the DRM system (see [Cohen, 2003]). This unifying semantic model of REL is used to resolve the rights protection dilemma between privacy protection and content usage control in the DRM system (Figure 3). In this unifying semantic model, the abstract concepts for describing the enforcement of content usage rights under certain conditions with corresponding obligations are modeled as ontologies. Furthermore, the criteria for privacy rights protection, such as $\mathtt{purpose}, \mathtt{action}, \mathtt{data}, \mathtt{datauser}$, and $\mathtt{obligation}$ are also considered and incorporated into the rule module of the DRM system. The access control web policies to enforce the digital usage rights and the protection web policies for a DRM user's privacy rights are integrated together to avoid the possible right protection conflicts between these two systems.

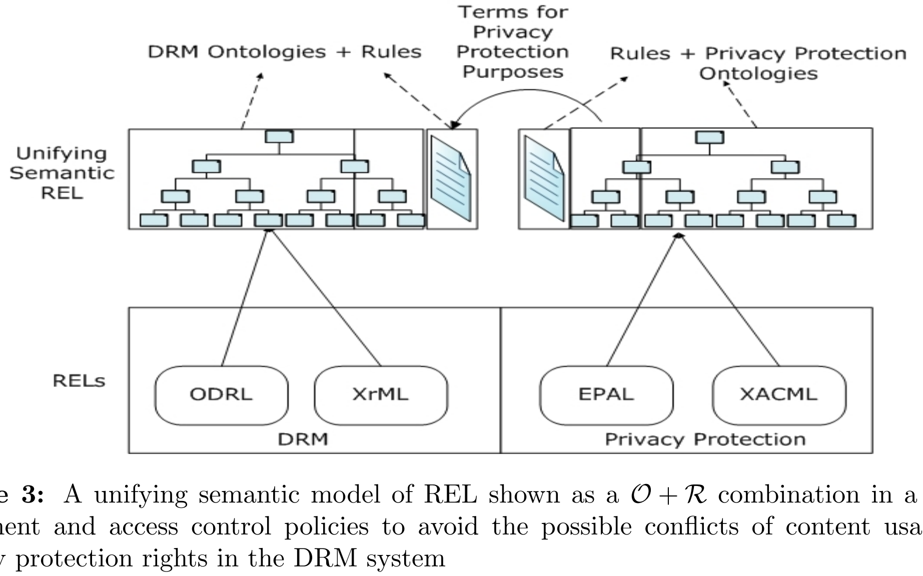

**Figure 3:** A unifying semantic model of REL shown as a $\mathcal{O}+\mathcal{R}$ combination in a license agreement and access control policies to avoid the possible conflicts of content usage and privacy protection rights in the DRM system

[2] All variables in each rule must appear in at least one of the datalog predicates, i.e., not predicates directly adopted from ontology for the rule's pre-conditions (or body).

### 6.3 The compromise of rights protection

In the EPAL data model a 5-tuple, i.e., (user, data, purpose, right, obligation) is used as the set of attributes for privacy protection policies [Karjoth & Schunter, 2002]. The use of a 5-tuple indicates that a particular type of users ask for data achieving a purpose with a certain right(s) and obligation(s). In a standalone semantics-enabled privacy protection system, web protection policies for privacy are enforced as verifying the satisfaction of constraints for data user, data type, purpose, rights, and obligation in the ontologies and rules. When we consider enforcing privacy protection rights and content usage rights in the DRM system, we do not directly combine the privacy protection system and the DRM system because this would entail more research on the merging and aligning of ontologies and rules in the heterogeneous systems.

The easiest way to resolve a rights protection dilemma for privacy and content usage is to incorporate a user's privacy rights in the DRM system (see Figure 3). In our unifying semantic model of REL, we allow a content user to specify privacy protection rights unambiguously in the semantics-enabled privacy protection web policies. A user's privacy rights are ensured when the user asks for usage rights to digital content because a user's profile and digital trace usage permission are modeled as a pre-condition of the rules, acting as an extra constraint of execution access control policies in the DRM system.

We extend our previous SWRL-based semantics-enabled DRM system to grant a content user privacy and fair use rights in the DRM system [Hu, 2007] [Hu et al., 2008]. We first request that the content distributor fulfill fair use statutory rights of the copyright law, i.e., allowing a content user to reuse his or her copyrighted digital contents in certain unrestricted ways for the purposes of teaching and research. Then, we require the content distributor to abide by a content user's opt-in and opt-out privacy rights. The data usage policy forces the distributor to comply with privacy protection laws on collecting, using, and disclosing of each user's profile and digital trace.

## 7 A scenario of rights protection

A scenario of the rights protection use case is extended from [Hu, 2007], and shown as Figure 4, where a license agreement for content usage is signed between a DRM server Charlie and two DRM clients, Alice and Bob to facilitate the content usage rights for a server and privacy and fair use rights for each client.

A license agreement in different expressions are shown as follows:

1. **Natural Language (NL)**:

   A DRM content distributor server, Charlie, makes a license agreement with two content consumer clients, Alice and Bob. After each paying thirty dollars and receiving acknowledgement from Charlie, Alice and Bob are each given personal usage rights and may display an *eBook*, , TheSemanticWebPrimer, up to five times in each client's side DRM controller box. They may each print it only once. The total number of actions, either displays or prints, done by Alice and Bob together, may be at most ten. The usage rights validity period is from 2008/05/07/00 : 00 to 2008/06/06/24 : 00.

   However, if either Alice or Bob uses this eBook for teaching and research, then the usage rights constraint may be relaxed for fair use to comply with the Copyright law. In this case, a maximum of 25 consecutive pages of each eBook can be printed and an unrestricted number of pages can be displayed for an unlimited number of times with unlimited validity period. Fair use is not allowed if the usage purposes are not successfully verified. Furthermore, to protect the privacy rights of Alice and Bob, we allow each one to specify usage options for respective profiles and digital traces

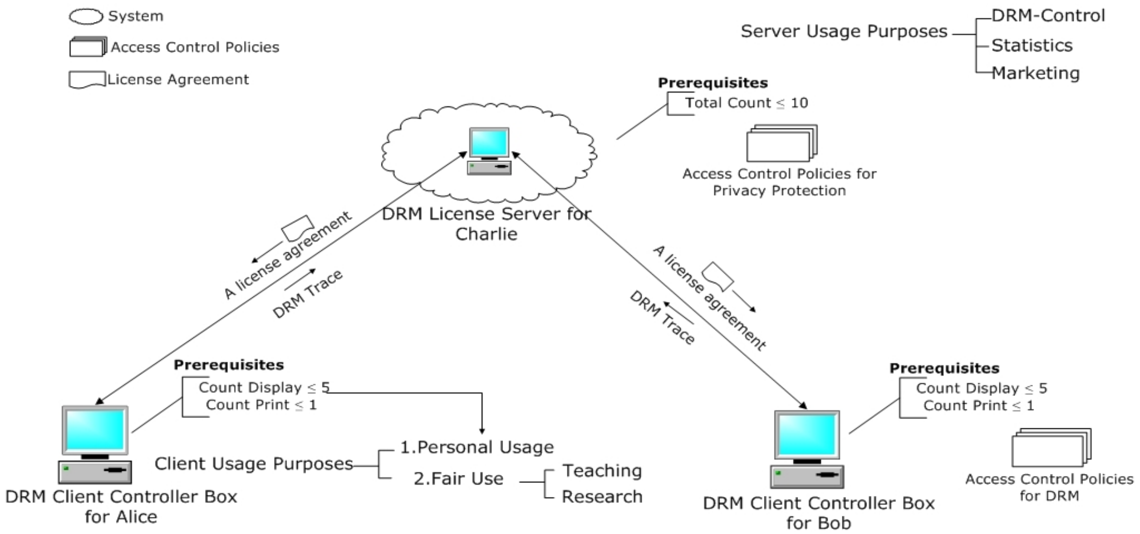

**Figure 4:** A scenario of rights protection as a license agreement between a license server, `Charlie`, and two clients `Alice`, and `Bob`, to enforce the respective semantics-enabled rights protection web policies

before the DRM server can collect them. In this case, `Alice` only allows her DRM client's controller to disclose her personal profile and online digital trace to a server for DRM control purposes but for no other purposes. On the other hand, `Bob` allows his DRM client's controller to disclose his personal profile and online digital trace to a server, for DRM control as well as non-DRM control purposes, such as marketing and statistics.

2. **Human readable abstract syntax**:

```
agreement
between Charlie and {Alice,Bob}
about The Semantic Web Primer
with inSequence[prePay[30.00],
attribution[Charlie]]

Access control applied to a client for DRM in a client:

clientUsagePurpose:

case Non-FairUse{personal}:
|==> not[and[Time < 2008/05/07/00:00,
Time > 2008/06/06/24:00]]
|==> with usageCount[10] ==>
and[forEachMember[{Alice,Bob};displayCount[5]]
    ==> display,
    forEachMember[{Alice,Bob};printCount[1]]
    ==> print]
```

```
case FairUse{teaching,research}:
|==> forEachMember[{Alice,Bob}] ==> display
|==> forEachMember[{Alice,Bob};
not [and [printPage# > endPage#,
     printPage# < startPage#]]
|==> forEachMember[{Alice,Bob};
     printPageCount[25]]
|==> forEachMember[{Alice,Bob}] ==> print

Access control applied to a server for privacy protection in a client:

serverUsagePurpose:

case DRMControl{DRMControl}:
|==> forEachMember[{Alice, Bob},
clientAllowPurpose[DRMControl]]
|==> forEachMember[{Alice,Bob},
profileDiscloseAllowed[personalProfile]==> disclose]
|==> forEachMember[{Alice,Bob},
traceDiscloseAllowed[digitalTrace]==> disclose]

case Non-DRMControl{Marketing,Statistics}:
|==> forEachMember[{Bob},
clientAllowPurpose[Non-DRMControl]]
|==> forEachMember[{Bob},
profileDiscloseAllowed[personalProfile]==> disclose]
|==> forEachMember[{Bob},
traceDiscloseAllowed[digitalTrace]==> disclose]
```

3. **First Order Logic (FOL)**:

   - Access control applied to a client for DRM in a client:

     $\forall x((x = Alice \vee x = Bob) \Rightarrow$
     $(\exists t_1 \exists t_2 (t_1 < t_2 \wedge Paid(30, t_1) \wedge Attributed(Charlie, t_2))$
     $\Rightarrow \exists y((y = teaching \vee y = research) \wedge HasClientUsagePurpose(x, y))$
     $\Rightarrow \mathbf{Permitted}(x, display, eBook))$

     $\Rightarrow \forall p \exists sp \exists ep$
     $((hasPrintPage\#(eBook, pg) \geq startPage\#(eBook, sp)$
     $\wedge hasPrintPage\#(eBook, pg) \leq endPage\#(eBook, ep)$
     $\Rightarrow hasPrintPageCount(eBook, sub(ep, sp)) \leq 25$
     $\Rightarrow \mathbf{Permitted}(x, display, eBook))$

     $\Rightarrow \exists y((y = personal) \wedge hasClientUsagePurpose(x, y))$
     $\Rightarrow \forall t(hasUsageDateTime(t) \geq 2008/05/07/00:00$
     $\wedge\ hasUsageDateTime(t) \leq 2008/06/06/24:00)$

$$\begin{aligned}
&\Rightarrow hasDisplayCount(Alice, id_1) + hasDisplayCount(Alice, id_2)\\
&+ hasPrintCount(Bob, id_1) + hasPrintCount(Bob, id_2) < 10\\
&\Rightarrow (hasDisplayCount(Alice, id_1) < 5\ \wedge hasDisplayCount(Bob, id_1) < 5\\
&\Rightarrow \textbf{Permitted}(x, display, eBook))
\end{aligned}$$

$$\begin{aligned}
&\Rightarrow hasPrintCount(Alice, id_2) < 1 \wedge hasPrintCount(Bob, id_2) < 1\\
&\Rightarrow \textbf{Permitted}(x, print, eBook))))
\end{aligned}$$

- Access control applied to a server for privacy protection in a client:

$$\begin{aligned}
&\forall x((x = Alice) \Rightarrow\\
&\Rightarrow \exists p \exists y \exists f \exists d((p = DRM - control) \wedge y = Charlie)\\
&\Rightarrow serverUsagePurpose(p) \wedge personalProfile(f)\\
&\Rightarrow clientAllowPurpose(x, p) \wedge serverRequestPurpose(y, p)\\
&\Rightarrow ProfileDiscloseAllowed(f, p)\\
&\Rightarrow \textbf{Permitted}(y, disclose, f)\\
&\Rightarrow TraceDiscloseAllowed(d, p)\\
&\Rightarrow \textbf{Permitted}(y, disclose, d))
\end{aligned}$$

$$\begin{aligned}
&\forall x((x = Bob) \Rightarrow\\
&\Rightarrow \exists p \exists y \exists f \exists d((p = DRM - control \vee p = Marketing \vee p = Statistics) \wedge y = Charlie)\\
&\Rightarrow serverUsagePurpose(p) \wedge personalProfile(f)\\
&\Rightarrow clientAllowPurpose(x, p) \wedge serverRequestPurpose(y, p)\\
&\Rightarrow ProfileDiscloseAllowed(f, p)\\
&\Rightarrow \textbf{Permitted}(y, disclose, f)\\
&\Rightarrow TraceDiscloseAllowed(d, p)\\
&\Rightarrow \textbf{Permitted}(y, disclose, d))
\end{aligned}$$

### 7.1 Semantic web policies as $\mathcal{O} + \mathcal{R}$ for a license

Three types of ontology are proposed to describe the concepts of data user, data type, and data usage purpose. In the data user ontology (see Figure 5), $\texttt{DRM} - \texttt{Client}$ class is the set of content users for a client $\texttt{c} \in \texttt{DRM} - \texttt{Client}$ class asks for content usage rights and a server $\texttt{s} \in \texttt{DRM} - \texttt{server}$ class through enforcing DRM web policies in a client side's DRM controller box to make its decision. On the other hand, a server $\texttt{s} \in \texttt{DRM} - \texttt{Server}$ class who asks for customer data usage rights and the permission granting is also enforced by privacy protection web policies in a DRM controller box.

The data usage purpose ontology (see Figure 6) provides the classification concepts of data usage purpose for a DRM client and a DRM server. The $\texttt{Client} - \texttt{Usage} - \texttt{Purpose}$ class provides data usage purposes for a DRM client to indicate whether it asks for a fair use or a not-fair use (such as a personal use) data usage. The $\texttt{Server} - \texttt{Usage} - \texttt{Purpose}$ class constrains a DRM server so that it can only disclose data satisfied previous client's opt-in purposes, such as DRM control or marketing,.

In the data type ontology (see Figure 7), the $\texttt{Digital} - \texttt{Content}$ class provides the classification concepts of digital media content for users and $\texttt{Customer} - \texttt{Data}$ class provides the classification concepts of client data for a selected server to access. In a client's DRM controller box, most of the vocabularies used for describing the concepts of data user and data type ontologies for semantic DRM web policies are imported directly from the DRM server's access control ontologies. The data usage purpose ontology

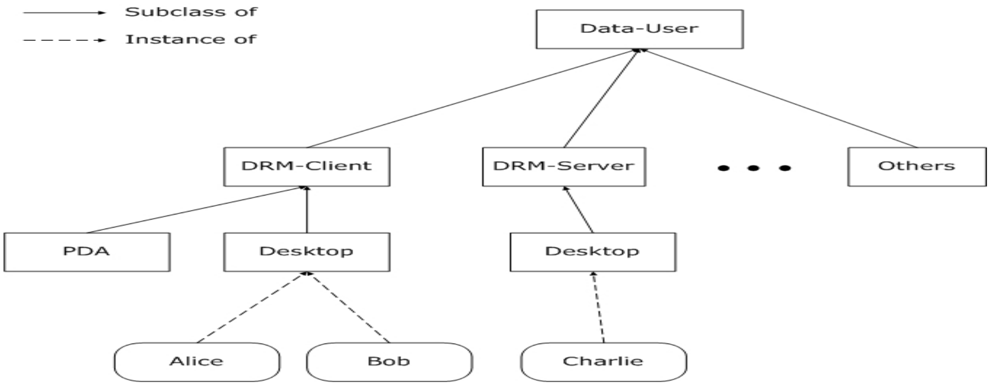

**Figure 5:** The data user ontology for the concepts of DRM client and DRM server taxonomy

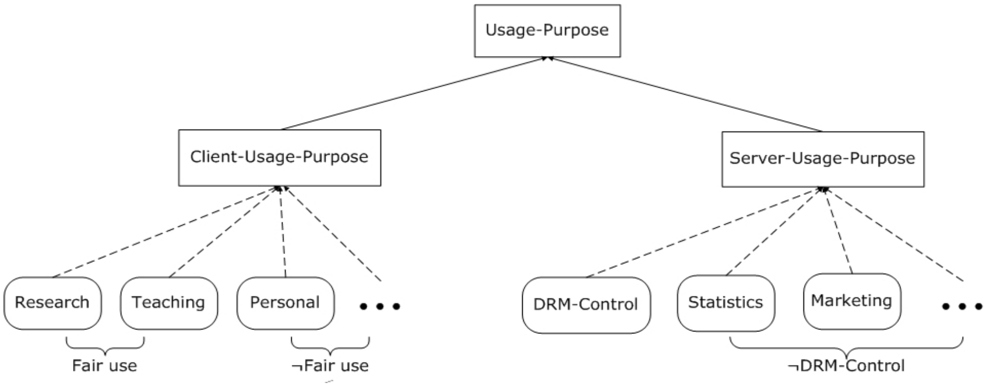

**Figure 6:** The data usage purpose ontology for the concepts of client's usage purposes and server's usage purposes taxonomy

(see Figure 6) is the exception, where the concepts for describing data usage to achieve the fair use and privacy protection purposes are outside the DRM's $\mathcal{O} + \mathcal{R}$ representations (see Figure 3) [3].

### 7.2 Properties for data usage purposes

Properties in the data usage purpose ontology in Figure 6 for a DRM client's to constraint the fair use and privacy protection purposes are shown as follows:

- $\texttt{HasClientUsagePurpose} \sqsubseteq \texttt{HasUsagePurpose}$
- $\texttt{HasServerUsagePurpose} \sqsubseteq \texttt{HasUsagePurpose}$

- $\texttt{T} \sqsubseteq \forall\ \texttt{HasUsagePurpose.Data} - \texttt{User}$ [4]
- $\texttt{T} \sqsubseteq \forall\ \texttt{HasUsagePurpose}^{-}\texttt{.Usage} - \texttt{Purpose}$ [5]
- $\texttt{T} \sqsubseteq \forall\ \texttt{HasClientUsagePurpose.DRM} - \texttt{Client}$

[3] The first capital character in the predicates is a marker to indicate that they are directly created in the datalog rule.

[4] The $\texttt{Data} - \texttt{User}$ class is defined as the domain of property $\texttt{HasUsagePurpose}$, as are as the following specifications.

[5] The $\texttt{Usage} - \texttt{Purpose}$ class is defined as the range of property $\texttt{HasUsagePurpose}$, as are the following specifications.

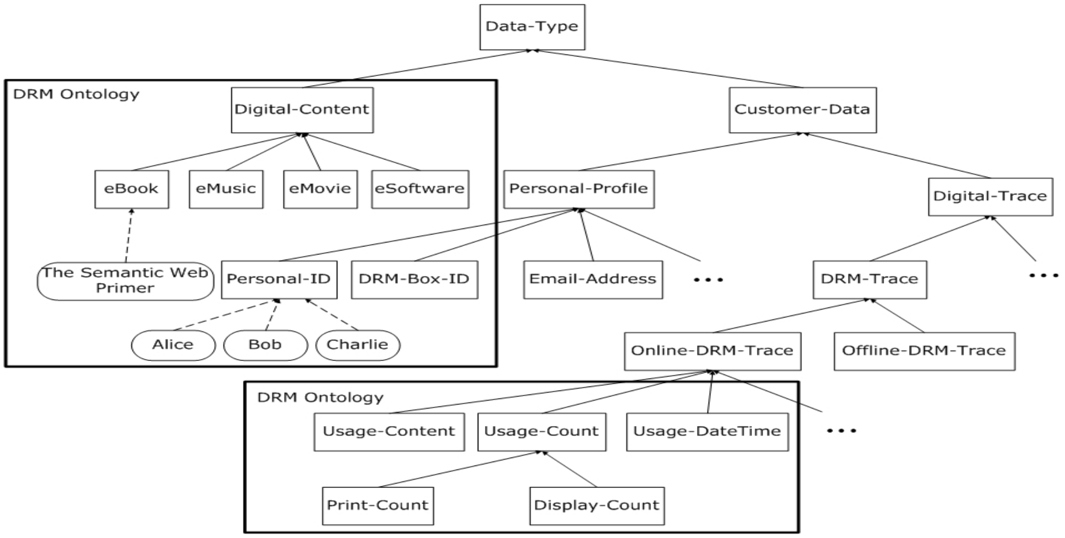

**Figure 7:** The data type ontology for the concepts of digital content and customer data taxonomy

- $\mathtt{T} \sqsubseteq \forall$ $\mathtt{HasClientUsagePurpose}^{-}.\mathtt{Client}-\mathtt{Usage}-\mathtt{Purpose}$
- $\mathtt{T} \sqsubseteq \forall$ $\mathtt{HasServerUsagePurpose.DRM}-\mathtt{Server}$
- $\mathtt{T} \sqsubseteq \forall$ $\mathtt{HasServerUsagePurpose}^{-}.\mathtt{Server}-\mathtt{Usage}-\mathtt{Purpose}$
- $\mathtt{T} \sqsubseteq \forall$ $\mathtt{HasResourceFairUse.Digital}-\mathtt{Content}$
- $\mathtt{T} \sqsubseteq \forall$ $\mathtt{HasResourceFairUse}^{-}.\mathtt{Client}-\mathtt{Usage}-\mathtt{Purpose}$

The domain class and range class of a property HasUsagePurpose and its sub-properties, such as HasClientUsagePurpose and HasServerUsagePurpose are imported from the data user and the data usage purpose ontologies. The datalog rules specified for the DRM control and privacy protection policies reuse these imported predicates to ensure all of the permission for information disclosure are satisfied.

### 7.3 O+R Representations

The $\mathcal{O}+\mathcal{R}$ representations for a DRM server, Charlie, and a DRM client, Alice are shown as the following sections. The given ontology modules are shown as TBox axioms, ABox instances; the rule modules are shown as rules and facts. The enforcement of unifying semantic privacy protection web policies for the DRM system are explicitly demonstrated:

Let $\Pi = (\Gamma, \Delta)$ are the $\mathcal{O}+\mathcal{R}$ knowledge representations of semantics-enabled web policies for privacy protection in the DRM system, where $\Gamma = \mathcal{O} = (\mathtt{axioms}, \mathtt{instances})$, $\Delta = \mathcal{R} = (\mathtt{rules}, \mathtt{facts})$.

- At the DRM license server Charlie's site:

  - $\Gamma = \mathcal{O}$, ontology module at the Charlie site:

*Axioms in the ontology module for DRM:

$$\begin{array}{l}
\mathtt{hasDisplayRights} \sqsubseteq \mathtt{hasUsageRights}\\
\mathtt{hasPrintRights} \sqsubseteq \mathtt{hasUsageRights}\\
\mathtt{eBook} \sqsubseteq \mathtt{Digital} - \mathtt{Content}\\
\mathtt{DRM} - \mathtt{Client} \sqsubseteq \mathtt{Data} - \mathtt{User}\\
\mathtt{DRM} - \mathtt{Server} \sqsubseteq \mathtt{Data} - \mathtt{User}\\
\mathtt{Print} - \mathtt{Count} \sqsubseteq \mathtt{Usage} - \mathtt{Count}\\
\mathtt{Display} - \mathtt{Count} \sqsubseteq \mathtt{Usage} - \mathtt{Count}\\
\mathtt{hasDisplayRights} \sqsubseteq \mathtt{hasUsageRights}\\
\mathtt{hasPrintRights} \sqsubseteq \mathtt{hasUsageRights}
\end{array}$$

$$\begin{array}{l}
\mathtt{T} \sqsubseteq \forall\ \mathtt{hasUsageCount.Data} - \mathtt{User}\ ^{6}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{hasUsageCount}^{-}.\mathtt{Digital} - \mathtt{Content}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{hasDisplayCount.Data} - \mathtt{User}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{hasDisplayCount}^{-}.\mathtt{Digital} - \mathtt{Content}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{hasPrintCount.Data} - \mathtt{User}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{hasPrintCount}^{-}.\mathtt{Digital} - \mathtt{Content}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{hasUsageDateTime.Data} - \mathtt{User}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{hasUsageDateTime}^{-}.\mathtt{Digital} - \mathtt{Content}
\end{array}$$

*Facts in the ontology module for DRM:

$$\begin{array}{l}
\mathtt{DRM} - \mathtt{Client(Alice)}\\
\mathtt{DRM} - \mathtt{Client(Bob)}\\
\mathtt{DRM} - \mathtt{Server(Charlie)},\\
\mathtt{Teacher(Alice)}\\
\mathtt{Researcher(Bob)}\\
\mathtt{eBook(TheSemanticWebPrimer)}\\
\mathtt{hasDisplayRights(Alice, TheSemanticWebPrimer)}
\end{array}$$

*Axioms in the ontology module for privacy protection:

$$\begin{array}{l}
\mathtt{Personal} - \mathtt{Profile} \sqsubseteq \mathtt{Customer} - \mathtt{Data}\\
\mathtt{Digital} - \mathtt{Trace} \sqsubseteq \mathtt{Customer} - \mathtt{Data}\\
\mathtt{DRM} - \mathtt{Trace} \sqsubseteq \mathtt{Digital} - \mathtt{Trace}\\
\mathtt{Online} - \mathtt{DRM} - \mathtt{Trace} \sqsubseteq \mathtt{DRM} - \mathtt{Trace}
\end{array}$$

$$\begin{array}{l}
\mathtt{T} \sqsubseteq \forall\ \mathtt{ClientAllowPurpose.DRM} - \mathtt{Client}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{ClientAllowPurpose}^{-}.\mathtt{Server} - \mathtt{Usage} - \mathtt{Purpose}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{ServerRequestPurpose.DRM} - \mathtt{Server}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{ServerRequestPurpose}^{-}.\mathtt{Server} - \mathtt{Usage} - \mathtt{Purpose}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{ProfileDiscloseAllowed.Personal} - \mathtt{Profile}\\
\mathtt{T} \sqsubseteq \forall\ \mathtt{ProfileDiscloseAllowed}^{-}.\mathtt{Server} - \mathtt{Usage} - \mathtt{Purpose}
\end{array}$$

[6] In $\mathtt{OWL} - \mathtt{DL}$, $\mathtt{maxCardinalityQ}$ is shown as $\leqslant_{\mathtt{n}} \mathtt{P.C}$, where $\mathtt{n}$ is an integer number, $\mathtt{P}$ is a property and $\mathtt{C}$ is a class. So $\leqslant_5 \mathtt{hasUsageCount.Usage} - \mathtt{Count}(?\mathtt{r}, ?\mathtt{uc})$ indicates that a particular resource $\mathtt{r}$, such as $\mathtt{eBook}$ is bound to a variable $?\mathtt{r}$, and the current usage count $\mathtt{uc}$ is bound to a variable $?\mathtt{uc}$ with maximum number 5.

$$\begin{array}{l}
\mathtt{T} \sqsubseteq \forall\ \mathtt{TraceDiscloseAllowed.Digital - Trace} \\
\mathtt{T} \sqsubseteq \forall\ \mathtt{TraceDiscloseAllowed^{-}.Server - Usage - Purpose}
\end{array}$$

*Facts in the ontology module for privacy protection:

$$\begin{array}{l}
\mathtt{Personal - Profile(AliceProfile)} \\
\mathtt{Personal - Profile(BobProfile)} \\
\mathtt{DRM - Trace(AliceDRMTrace)} \\
\mathtt{DRM - Trace(BobDRMTrace)} \\
\mathtt{Server - Usage - Purpose(DRM - Control)} \\
\mathtt{Server - Usage - Purpose(Marketing)} \\
\mathtt{ClientAllowPurpose(Alice, DRM - Control)} \\
\mathtt{ClientAllowPurpose(Bob, DRM - Control)} \\
\mathtt{ClientAllowPurpose(Bob, Marketing)} \\
\mathtt{ProfileDiscloseAllowed(AliceProfile, DRM - Control)} \\
\mathtt{TraceDiscloseAllowed(AliceDRMTrace, DRM - Control)} \\
\mathtt{ProfileDiscloseAllowed(BobProfile, Marketing)} \\
\mathtt{TraceDiscloseAllowed(BobDRMTrace, DRM - Control)} \\
\mathtt{ProfileDiscloseAllowed(BobProfile, DRM - Control)} \\
\mathtt{TraceDiscloseAllowed(BobDRMTrace, Marketing)}
\end{array}$$

- $\Delta = \mathcal{R}$ rule module at the $\mathtt{Charlie}$ site:

  *Rules in the rule module for DRM:

  $$\begin{array}{l}
  \mathtt{hasDisplayRights}(?x, ?r) \land \mathtt{hasSell_{d}Rights}(?x, ?r) \\
  \Longrightarrow \mathtt{hasDisplaySell_{d}Rights}(?x, ?r) \leftarrow (c1)
  \end{array}$$

  $$\begin{array}{l}
  \mathtt{hasDisplaySell_{d}Rights}(?x, ?r) \land \mathtt{delegate_{g}}(?x, ?y) \land \mathtt{hasPrepaid}(?y, ?a) \\
  \Longrightarrow \mathtt{hasDisplayRights}(?y, ?r) \leftarrow (c2) \\
  \cdots\cdots
  \end{array}$$

  *Rules in the rule module of privacy protection:

  $$\begin{array}{l}
  \mathtt{DRM - Client}(?x) \land \mathtt{DRM - Server}(?y) \land \mathtt{Server - Usage - Purpose}(?p) \\
  \land \mathtt{Personal - Profile}(?f) \land \mathtt{ClientAllowPurpose}(?x, ?p) \\
  \land \mathtt{ServerRequestPurpose}(?y, ?p) \land \mathtt{ProfileDiscloseAllowed}(?f, ?p) \\
  \Longrightarrow \mathtt{Permitted_{Charlie}}(\mathtt{Disclose}, ?f)) \leftarrow (c3)
  \end{array}$$

  $$\begin{array}{l}
  \mathtt{DRM - Client}(?x) \land \mathtt{DRM - Server}(?y) \land \mathtt{Server - Usage - Purpose}(?p) \\
  \land \mathtt{Digital - Trace}(?d) \land \mathtt{ClientAllowPurpose}(?x, ?p) \\
  \land \mathtt{ServerRequestPurpose}(?y, ?p) \land \mathtt{TraceDiscloseAllowed}(?d, ?p) \\
  \Longrightarrow \mathtt{Permitted_{Charlie}}(\mathtt{Disclose}, ?d) \leftarrow (c4)
  \end{array}$$

Rules $(\mathtt{c1})$ and $(\mathtt{c2})$ are $\mathtt{Datalog - Safe}$ DRM control rules, where all of the variables appearing in each rule's head also appear in the rule's body. Moreover, all of the predicates in these rules are imported from DRM ontologies. More detailed descriptions can refer to [Hu, 2007]. Rules (c3) and (c4) are privacy protection rules that satisfy the $\texttt{DL}-\texttt{Safe}$ conditions, where all of the rule variables occur at least in one of the datalog predicates in each rule's body. When server Charlie requests a DRM controller box in Alice's site to enforce privacy protection policies for disclosing Alice's profile or a digital trace under the purpose of DRM control, it will be permitted, i.e., the following facts will be derived by rules $(c3)$ and $(c4)$:

$\texttt{Permitted}_{\texttt{Charlie}}(\texttt{Disclose}, \texttt{AliceProfile})$
$\texttt{Permitted}_{\texttt{Charlie}}(\texttt{Disclose}, \texttt{AliceDRMTrace})$

Similarly, when server Charlie asks for disclosure of Bob's profile or digital trace for DRM control purpose, it is also permitted. However, when server Charlie asks for the disclosure of Alice's profile and digital trace for marketing purposes, it will not be permitted. In fact, we cannot explicitly obtain the following two facts from rules (c3) and (c4):

$\texttt{Permitted}_{\texttt{Charlie}}(\texttt{Disclose}, \texttt{AliceProfile})$
$\texttt{Permitted}_{\texttt{Charlie}}(\texttt{disclose}, \texttt{AliceDRMTrace})$

The fact is that Alice does not explicitly allow her profile and DRM digital trace to be shown as facts for marketing purposes in the ontologies module. Therefore server Charlie cannot obtain a positive permission from rules (c3) and (c4).

- At content consumer client Alice's site:

  - $\Gamma = \mathcal{O}$, the ontology module at the Alice site:

    Most of the axioms and facts for privacy protection in the ontology module in an Alice DRM controller box are the same as the results we have shown at server Charlie's site except for fair use access control policies shown as the following:

    *Facts in the ontology module for DRM:

    $\texttt{Teacher}(\texttt{Alice}), \texttt{Researcher}(\texttt{Alice})$
    $\texttt{HasClientUsagePurpose}(\texttt{Alice}, \texttt{Teaching})$
    $\texttt{HasClientUsagePurpose}(\texttt{Alice}, \texttt{Research})$
    $\texttt{HasResourceFairUse}(\texttt{TheSemanticWebPrimer})$
    $\geq_3 \texttt{HasStartPage}\#(\texttt{TheSemanticWebPrimer}, 20)$
    $\leq_{24} \texttt{HasEndPage}\#(\texttt{TheSemanticWebPrimer}, 20)$
    $\leq_{25} \texttt{HasPrintPageCount}(\texttt{TheSemanticWebPrimer}, 17)$

  - $\Delta = \mathcal{R}$, rules in the rule module for DRM to enforce fair use right:

    *Rules in the rule module for DRM to enforce fair use:

$$\mathtt{Teacher(?x) \wedge DRM - Client(?x) \wedge Client - Usage - Purpose(Teaching)}$$
$$\Longrightarrow \mathtt{HasFairUseAllowed(?x, Teaching)} \leftarrow \mathtt{(a1)}$$

$$\mathtt{Researcher(?x) \wedge DRM - Client(?x) \wedge Client - Usage - Purpose(Research)}$$
$$\Longrightarrow \mathtt{HasFairUseAllowed(?x, Research)} \leftarrow \mathtt{(a2)}$$

$$\mathtt{hasDisplayRights(?x, ?r) \wedge eBook(?r) \wedge HasFairUseAllowed(?x, ?p)}$$
$$\wedge \mathtt{HasClientUsagePurpose(?x, ?p) \wedge HasResourceFairUse(?r, ?p)}$$
$$\Longrightarrow \mathtt{Permitted_{Alice}(Display, ?r, ?p)} \leftarrow \mathtt{(a3)}$$

$$\mathtt{hasDisplayRights(?x, ?r) \wedge eBook(?r) \wedge HasFairUseAllowed(?x, ?p)}$$
$$\wedge \mathtt{HasClientUsagePurpose(?x, ?p)} \wedge \geq_{\mathsf{sp}} \mathtt{HasStartPage\#(?r, ?pg)}$$
$$\wedge \leq_{\mathsf{ep}} \mathtt{HasEndPage\#(?r, ?pg)} \wedge \leq_{25} \mathtt{HasPrintPageCount(?r, ?c)}$$
$$\wedge \mathtt{HasResourceFairUse(?r, ?p)} \Longrightarrow \mathtt{Permitted_{Alice}(Print, ?r, ?p)} \leftarrow \mathtt{(a4)}$$

$$\mathtt{hasDisplayRights(?x, ?r)} \wedge <_{10} \mathtt{hasUsageCount.Usage - Count(?r, ?uc)}$$
$$\wedge <_{5} \mathtt{hasDisplayCount.Display - Count(?r, ?dc)}$$
$$\wedge \geq_{\mathsf{2008/05/07/00:00}} \mathtt{hasUsageDateTime.Usage - DateTime(?r, ?ut)}$$
$$\wedge \leq_{\mathsf{2008/06/06:24:00}} \mathtt{hasUsageDateTime.Usage - DateTime(?r, ?ut)}$$
$$\Longrightarrow \mathtt{Permitted_{Alice}(Display, ?r)} \leftarrow \mathtt{(a5)}$$

$$\mathtt{hasPrintRights(?x, ?r)} \wedge <_{10} \mathtt{hasUsageCount.Usage - Count(?r, ?uc)}$$
$$\wedge <_{1} \mathtt{hasPrintCount.Print - Count(?r, ?pc)}$$
$$\wedge \geq_{\mathsf{2008/05/07/00:00}} \mathtt{hasUsageDateTime.Usage - DateTime(?r, ?ut)}$$
$$\wedge \leq_{\mathsf{2008/06/06:24:00}} \mathtt{hasUsageDateTime.Usage - DateTime(?r, ?ut)}$$
$$\Longrightarrow \mathtt{Permitted_{Alice}(Print, ?r)} \leftarrow \mathtt{(a6)}$$

*Facts in the rule module for DRM to enforce fair use right:

$\mathtt{HasFairUseAllowed(Alice, Teaching)} \leftarrow$ derived by $\mathtt{(a1)}$
$\mathtt{HasFairUseAllowed(Alice, Research)} \leftarrow$ derived by $\mathtt{(a2)}$

The DRM system derives fair use rights of teaching and research for Alice by using rules (a1) and (a2) if *Alice* can provide her teacher or researcher's digital certificate to the Charlie server and this certificate is verified successfully by a trusted third party (TTP) to endorse this fair use right. In this case, a maximum of 25 consecutive pages of TheSemanticWebPrimer eBook can be printed and an unrestricted number of pages can be displayed for an unlimited number of times when Alice asks for a request and is derived by $(a3)$ and $(a4)$ rules.

In another case, when Alice asks for content usage rights for TheSemanticWebPrimer of the eBook by using her personal digital certificate, a non-fair use right of this eBook for Alice is derived by the rules $(a5)$ and $(a6)$. All of the rules in $(a1)$-$(a6)$ are $\mathtt{DL - Safe}$ because they satisfy the conditions that all of the variables occurred within the datalog predicate, i.e., the non-DL predicate of the rule's body. The $\mathtt{DL - Safe}$ conditions ensure a decidable computation time for each permission decision of a request.

## 8 Conclusions

RELs, such as ODRL and P3P, provide an information model and vocabularies for designing a license agreement through the integration of web protection policies from both client and server. However, we sometimes face a semantic ambiguity problem when we use REL-based web protection policies to represent and enforce the access rights of data use. In this chapter, we proposed a unifying semantic model of REL to unambiguously express and enforce fair use and privacy protection rights for digital content users. This formal semantic model of REL is based on the homogeneous (or tight) integration of ontologies and rules, i.e., SWRL-based $\mathcal{O}+\mathcal{R}$ from the semantic web. A real-life scenario was given to demonstrate how to ensure the DRM server's content usage rights and a DRM client's fair use and privacy protection rights. This rights protection scenario, we believe, cannot be easily achieved by other semantic models, such as FOL, DL, and LP.

## Appendix

This research was partially supported by the NSC of Taiwan under Grant No. NSC 98-2221-E-004-009.

## References

[Anderson, 2006] Anderson, A. H. (2006). A comparison of two privacy policy languages: EPAL and XACML. In *Proceedings of the 3rd ACM Workshop on Secure Web Services (SWS'06)* (pp. 53–60).: ACM.

[Antón et al., 2007] Antón, I. A. et al. (2007). A roadmap for comprehensive online for privacy policy management. *Comm. of the ACM*, 50(7), 109–116.

[Antoniou et al., 2007] Antoniou, G. et al. (2007). Rule-based policy specification. In T. Yu & S. Jajodia (Eds.), *Secure Data Management in Decentralized Systems* (pp. 169–216). Springer.

[Arnab & Hutchison, 2005] Arnab, A. & Hutchison, A. (2005). Fair usage contracts for DRM. In *DRM '05: Proceedings of the 5th ACM workshop on Digital rights management* (pp. 1–7).: ACM.

[Berstel et al., 2007] Berstel, B. et al. (2007). Reactive rules on the web. In *Reasoning Web 2007, Third International Summer School*, LNCS4636 Dresden, Germany: Springer.

[Boley et al., 2007] Boley, H. et al. (2007). Rule interchange on the web. In *Reasoning Web 2007, Third International Summer School*, LNCS 4636 Dresden, Germany: Springer.

[Bonatti et al., 2006] Bonatti, A. P. et al. (2006). Semantic web policies - a discussion of requirements and research issues. In *3rd Eurpoean Semantic Web Conference (ESWC 2006)* Budva, Montenergro.

[Cohen, 2003] Cohen, E. J. (2003). DRM and privacy. *Commun. ACM*, 46(4), 47–49.

[ContentGuard, 2002] ContentGuard, I. (2002). *XrML: The digital rights language for trusted content and services*. Technical report, ContentGuard Inc. `http://www.xrml.org/index.asp`.

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

[Donini et al., 1998] Donini, M. F. et al. (1998). $\mathcal{AL}$-log: Integrating datalog and description logics. *Journal of Intelligent Information Systems*, 10(3), 227–252.

[Eiter & Ianni, 2008] Eiter, T. & Ianni, G. (2008). Rules and ontologies for the semantics web. In *Reasoning Web 2008*, LNCS 5224 (pp. 1–53).: Springer.

[Erickson, 2003] Erickson, S. J. (2003). Fair use, DRM, and trusted computing. *Commun. ACM*, 46(4), 34–39.

[Feigenbaum et al., 2002] Feigenbaum, J. et al. (2002). Privacy engineering for digital rights management systems. In *Digital Rights Management (DRM) Workshop 2002*, volume 2320 of *LNCS 2320* (pp. 76–105).: Springer.

[Garcia et al., 2005] Garcia, R., Gallego, I., & Delgado, J. (2005). Formalising ODRL semantics using web ontologies. In *2nd International ODRL Workshop* Lisbon, Portugal. `http://odrl.net/workshop2005/`.

[Grau et al., 2008] Grau, C. B. et al. (2008). OWL 2: The next step for OWL. *Web Semantics: Science, Services and Agents on the World Wide Web 3*, (pp. 309–322).

[Grosof et al., 2003] Grosof, N. B. et al. (2003). Description logic programs: Combining logic programs with description logic. In *World Wide Web 2003* (pp. 48–65). Budapest, Hungary.

[Guth & Iannella, 2005a] Guth, S. & Iannella, R. (2005a). *ODRL V2.0 - Requirements*. Working draft, The ODRL Initiative. `http://odrl.net/2.0/v2req.html`.

[Guth & Iannella, 2005b] Guth, S. & Iannella, R. (2005b). *Open Digital Rights Language (ODRL) Version 2*. Odrl initiative working draft, The ODRL Initiative. `http://odrl.net/2.0/v2req.html`.

[Guth & Iannella, 2007] Guth, S. & Iannella, R. (2007). *ODRL V2.0 - Model Semantics*. Working draft, The ODRL Initiative. `http://odrl.net/2.0/v2req.html`.

[Halpern, 2008] Halpern, Y. J. V. W. (2008). A formal foundation for XrML. *Journal of the ACM*, 55(1), 1–42.

[Hitzler et al., 2010] Hitzler, P. et al. (2010). *Foundations of Semantic Web Technologies*. CRC Press.

[Horrocks et al., 2005] Horrocks, I. et al. (2005). OWL rules: A proposal and prototype implementation. *Web Semantics: Science, Services and Agents on the World Wide Web 3*, (1), 23–40.

[Hu, 2007] Hu, Y. J. (2007). Semantic-driven enforcement of rights delegation policies via the combination of rules and ontologies. In *Workshop on Privacy Enforcement and Accountability with Semantics in conjunction with ISWC+ASWC'07*.

[Hu et al., 2008] Hu, Y. J., Guo, H. Y., & Lin, G. D. (2008). Semantic enforcement of privacy protection policies via the combination of ontologies and rules. In *IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing (SUTC 2008)* Taichung, Taiwan.

[Jajodia et al., 2001] Jajodia, S. et al. (2001). Flexible support for multiple access control policies. *ACM Trans. on Database Systems*, 26(2), 214–260.

[Karjoth & Schunter, 2002] Karjoth, G. & Schunter, M. (2002). A privacy policy model for enterprises. In *15th IEEE Computer Security Foundations Workshop (CSFW)*: IEEE.

[Li et al., 2006] Li, N., Yu, T., & Antón, A. I. (2006). A semantics-approach to privacy languages. *Computer Systems and Engineering (CSSE)*, 21(5).

[Motik et al., 2004] Motik, B., Sattler, U., & Studer, R. (2004). Query answering for OWL-DL with rules. In *3rd International Semantic Web Conference (ISWC) 2004*, LNCS 3298 (pp. 549–563).: Springer.

[Park & Sandhu, 2004] Park, J. & Sandhu, R. T. (2004). The UCON$_{ABC}$ usage control model. *ACM Trans. on Information and System Security*, 7(1), 128–174.

[Patel-Schneider & Siméon, 2002] Patel-Schneider, F. P. & Siméon, J. (2002). Building the semantic web on XML. In *ISWC 2002*, LNCS2342 (pp. 147–161).: Springer.

[Pucella & Weissman, 2006] Pucella, R. & Weissman, V. (2006). *A Formal Foundation for ODRL*. arXiv:cs/0601085v1, Cornell University. `http://arxiv.org/abs/cs/0601085`.

[Rosati, 2006] Rosati, R. (2006). Integrating ontologies and rules: Semantic and computional issues. In *Reasoning Web 2006*, LNCS 4126 (pp. 128–151).

[Tonti et al., 2003] Tonti, G. et al. (2003). Semantic web languages for policy representation and reasoning: A comparison of KAoS, Rei, and Ponder. In *2nd International Semantic Web Conference (ISWC) 2003*, LNCS 2870 (pp. 419–437).: Springer.

[Vimercati et al., 2007] Vimercati, S. D. C. d. et al. (2007). Access control policies and languages in open environments. In T. Yu & S. Jajodia (Eds.), *Secure Data Management in Decentralized Systems* (pp. 21–58). Springer.

[Yu et al., 2004] Yu, T., N. Li, A., & Antón, I. (2004). A formal semantics for P3P. In *ACM Workshop on Secure Web Services* Fairfax, VA, USA. `http://citeseer.ist.psu.edu/750176.html`.