Semantics-enabled Policies for Information Sharing and Protection in the Cloud

Yuh-Jong Hu Win-Nan Wu Jiun-Jan Yang
{hu, d9905, 98753036}@cs.nccu.edu.tw

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

Oct-7th-2011

International Conference on Social Informatics
(SocInfo'11)


Part I

Research Goals

Motivations

- A new spectacular phenomenon of information sharing and service integration on the social web 2.0 using semantic web techniques
- Investigating the inter-disciplinary area of information technology and law for information sharing and protection
- Exploring the emerging challenges of legalizing semantics-enabled policies for laws in the cloud computing
- Exploiting the legitimate law enforcement processes to allow legal authorities to collect and use shareable personal information without fear of privacy violation


Motivations

- A new spectacular phenomenon of information sharing and service integration on the social web 2.0 using semantic web techniques
- Investigating the inter-disciplinary area of information technology and law for information sharing and protection
- Exploring the emerging challenges of legalizing semantics-enabled policies for laws in the cloud computing
- Exploiting the legitimate law enforcement processes to allow legal authorities to collect and use shareable personal information without fear of privacy violation


Motivations

- A new spectacular phenomenon of information sharing and service integration on the social web 2.0 using semantic web techniques
- Investigating the inter-disciplinary area of information technology and law for information sharing and protection
- Exploring the emerging challenges of legalizing semantics-enabled policies for laws in the cloud computing
- Exploiting the legitimate law enforcement processes to allow legal authorities to collect and use shareable personal information without fear of privacy violation


Motivations

- A new spectacular phenomenon of information sharing and service integration on the social web 2.0 using semantic web techniques
- Investigating the inter-disciplinary area of information technology and law for information sharing and protection
- Exploring the emerging challenges of legalizing semantics-enabled policies for laws in the cloud computing
- Exploiting the legitimate law enforcement processes to allow legal authorities to collect and use shareable personal information without fear of privacy violation


Research Goals

1. How to use the semantics-enabled (formal) policies to represent and interpret of laws without causing any *ambiguity*?
2. How to ensure the semantics-enabled policies are *compliant* with the laws?
3. How to and *enforce* the semantics-enabled policies deployed in the formal policy platform?
4. How to *unify* the semantics-enabled policies when *conflicts* exist?
5. How to *automatically unify* semantics-enabled policies from multiple legal domains to achieve the flexible and optimal data operations in the cloud?


Research Goals

1. How to use the semantics-enabled (formal) policies to represent and interpret of laws without causing any *ambiguity*?
2. How to ensure the semantics-enabled policies are *compliant* with the laws?
3. How to and *enforce* the semantics-enabled policies deployed in the formal policy platform?
4. How to *unify* the semantics-enabled policies when *conflicts* exist?
5. How to *automatically unify* semantics-enabled policies from multiple legal domains to achieve the flexible and optimal data operations in the cloud?


Research Goals

1. How to use the semantics-enabled (formal) policies to represent and interpret of laws without causing any *ambiguity*?
2. How to ensure the semantics-enabled policies are *compliant* with the laws?
3. How to and *enforce* the semantics-enabled policies deployed in the formal policy platform?
4. How to *unify* the semantics-enabled policies when *conflicts* exist?
5. How to *automatically unify* semantics-enabled policies from multiple legal domains to achieve the flexible and optimal data operations in the cloud?


Research Goals

1. How to use the semantics-enabled (formal) policies to represent and interpret of laws without causing any *ambiguity*?
2. How to ensure the semantics-enabled policies are *compliant* with the laws?
3. How to and *enforce* the semantics-enabled policies deployed in the formal policy platform?
4. How to *unify* the semantics-enabled policies when *conflicts* exist?
5. How to *automatically unify* semantics-enabled policies from multiple legal domains to achieve the flexible and optimal data operations in the cloud?


Research Goals

1. How to use the semantics-enabled (formal) policies to represent and interpret of laws without causing any *ambiguity*?
2. How to ensure the semantics-enabled policies are *compliant* with the laws?
3. How to and *enforce* the semantics-enabled policies deployed in the formal policy platform?
4. How to *unify* the semantics-enabled policies when *conflicts* exist?
5. How to *automatically unify* semantics-enabled policies from multiple legal domains to achieve the flexible and optimal data operations in the cloud?


Part II

Semantics-enabled Formal Policy


Formal Protection Policy

1. A *formal policy* ($\mathcal{FP}$) is a declarative expression executed in a computer system for a human legal norm without semantic ambiguity.
2. An $\mathcal{FP}$ is created from a *policy language* ($\mathcal{PL}$), and $\mathcal{PL}$ is shown as a combination of ontology and rule languages.
3. An $\mathcal{FP}$ is composed of ontologies $\mathcal{O}$ and rules $\mathcal{R}$, where ontologies are created from an ontology language and rules are created from a rule language.
4. A *formal protection policy* ($\mathcal{FPP}$) is an $\mathcal{FP}$ that aims at representing and enforcing resource protection principles, where the structure of resources is modeled as ontologies $\mathcal{O}$ and the resources protection is shown as rules $\mathcal{R}$.

Formal Protection Policy

1. A *formal policy* ($\mathcal{FP}$) is a declarative expression executed in a computer system for a human legal norm without semantic ambiguity.
2. An $\mathcal{FP}$ is created from a *policy language* ($\mathcal{PL}$), and $\mathcal{PL}$ is shown as a combination of ontology and rule languages.
3. An $\mathcal{FP}$ is composed of ontologies $\mathcal{O}$ and rules $\mathcal{R}$, where ontologies are created from an ontology language and rules are created from a rule language.
4. A *formal protection policy* ($\mathcal{FPP}$) is an $\mathcal{FP}$ that aims at representing and enforcing resource protection principles, where the structure of resources is modeled as ontologies $\mathcal{O}$ and the resources protection is shown as rules $\mathcal{R}$.


Formal Protection Policy

1. A *formal policy* ($\mathcal{FP}$) is a declarative expression executed in a computer system for a human legal norm without semantic ambiguity.
2. An $\mathcal{FP}$ is created from a *policy language* ($\mathcal{PL}$), and $\mathcal{PL}$ is shown as a combination of ontology and rule languages.
3. An $\mathcal{FP}$ is composed of ontologies $\mathcal{O}$ and rules $\mathcal{R}$, where ontologies are created from an ontology language and rules are created from a rule language.
4. A *formal protection policy* ($\mathcal{FPP}$) is an $\mathcal{FP}$ that aims at representing and enforcing resource protection principles, where the structure of resources is modeled as ontologies $\mathcal{O}$ and the resources protection is shown as rules $\mathcal{R}$.


Formal Protection Policy

1. A *formal policy* ($\mathcal{FP}$) is a declarative expression executed in a computer system for a human legal norm without semantic ambiguity.
2. An $\mathcal{FP}$ is created from a *policy language* ($\mathcal{PL}$), and $\mathcal{PL}$ is shown as a combination of ontology and rule languages.
3. An $\mathcal{FP}$ is composed of ontologies $\mathcal{O}$ and rules $\mathcal{R}$, where ontologies are created from an ontology language and rules are created from a rule language.
4. A *formal protection policy* ($\mathcal{FPP}$) is an $\mathcal{FP}$ that aims at representing and enforcing resource protection principles, where the structure of resources is modeled as ontologies $\mathcal{O}$ and the resources protection is shown as rules $\mathcal{R}$.


Formal Privacy Protection Policy

1. A *privacy protection policy* shown as an $\mathcal{FPP}$ is a combination of ontologies and rules, where Description Logic (DL)-based ontologies provide data sharing, while Logic Program (LP)-based rules provide data query and protection.
2. A *formal policy combination* ($\mathcal{FPC}$) in a *global policy schema* ($\mathcal{GPS}$) allows data sharing as an integration of $\mathcal{FP}$ from a variety of structure data sources, where $\mathcal{GPS}$ includes integrated $\mathcal{O}$ and integrated $\mathcal{R}$.
3. A *formal protection policy combination* ($\mathcal{FPPC}$) allows data sharing and protection through using $\mathcal{FPC}$.


Formal Privacy Protection Policy

1. A *privacy protection policy* shown as an $\mathcal{FPP}$ is a combination of ontologies and rules, where Description Logic (DL)-based ontologies provide data sharing, while Logic Program (LP)-based rules provide data query and protection.
2. A *formal policy combination* ($\mathcal{FPC}$) in a *global policy schema* ($\mathcal{GPS}$) allows data sharing as an integration of $\mathcal{FP}$ from a variety of structure data sources, where $\mathcal{GPS}$ includes integrated $\mathcal{O}$ and integrated $\mathcal{R}$.
3. A *formal protection policy combination* ($\mathcal{FPPC}$) allows data sharing and protection through using $\mathcal{FPC}$.


Formal Privacy Protection Policy

1. A *privacy protection policy* shown as an $\mathcal{FPP}$ is a combination of ontologies and rules, where Description Logic (DL)-based ontologies provide data sharing, while Logic Program (LP)-based rules provide data query and protection.
2. A *formal policy combination* ($\mathcal{FPC}$) in a *global policy schema* ($\mathcal{GPS}$) allows data sharing as an integration of $\mathcal{FP}$ from a variety of structure data sources, where $\mathcal{GPS}$ includes integrated $\mathcal{O}$ and integrated $\mathcal{R}$.
3. A *formal protection policy combination* ($\mathcal{FPPC}$) allows data sharing and protection through using $\mathcal{FPC}$.


Part III

Semantics-enabled Policies in the Cloud


Formal Policy Compliance

1. Current data protection and national security laws are not up-to-date on handling the cross-border data sharing and protection in the cloud.
2. We need to address research issues, not only for a law refinement, but for a technology re-engineering when embark the law concepts in the cloud.
3. The ultimate objective is to empower the flexible and agile use of cloud resources without fear of violating the laws.


Formal Policy Compliance

1. Current data protection and national security laws are not up-to-date on handling the cross-border data sharing and protection in the cloud.
2. We need to address research issues, not only for a law refinement, but for a technology re-engineering when embark the law concepts in the cloud.
3. The ultimate objective is to empower the flexible and agile use of cloud resources without fear of violating the laws.


Formal Policy Compliance

1. Current data protection and national security laws are not up-to-date on handling the cross-border data sharing and protection in the cloud.
2. We need to address research issues, not only for a law refinement, but for a technology re-engineering when embark the law concepts in the cloud.
3. The ultimate objective is to empower the flexible and agile use of cloud resources without fear of violating the laws.

Formal Policy Compliance (conti.)

1. We propose a formal policy framework for flexible policy deployment, integration, and enforcement in the cloud.
2. A formal policy compliance of each data request is based on the idea of *data usage context* creation of a user.
3. The laws that will be applied to a specific data request in a trusted legal domain (TLD) and also the legal boundary of a TLD are all depend on the data usage context creation.


Formal Policy Compliance (conti.)

1. We propose a formal policy framework for flexible policy deployment, integration, and enforcement in the cloud.
2. A formal policy compliance of each data request is based on the idea of *data usage context* creation of a user.
3. The laws that will be applied to a specific data request in a trusted legal domain (TLD) and also the legal boundary of a TLD are all depend on the data usage context creation.


Formal Policy Compliance (conti.)

1. We propose a formal policy framework for flexible policy deployment, integration, and enforcement in the cloud.
2. A formal policy compliance of each data request is based on the idea of *data usage context* creation of a user.
3. The laws that will be applied to a specific data request in a trusted legal domain (TLD) and also the legal boundary of a TLD are all depend on the data usage context creation.


A Semantics-enabled Policy Framework

We propose a three-layer architecture of a semantics-enabled policy framework:

1. Cloud Legalized Domain (CLD) top layer:
   A *legal cages* model for a Trusted Legal Domain (TLD)
2. Cloud Virtual Domain (CVD) middle layer:
   A *logical cages* model for a Trusted Virtual Domain (TVD)
3. Cloud Machine Domain (CMD) bottom layer:
   A *physical cages* model for a Trusted Machine Domain (TMD)


A Semantics-enabled Policy Framework

We propose a three-layer architecture of a semantics-enabled policy framework:

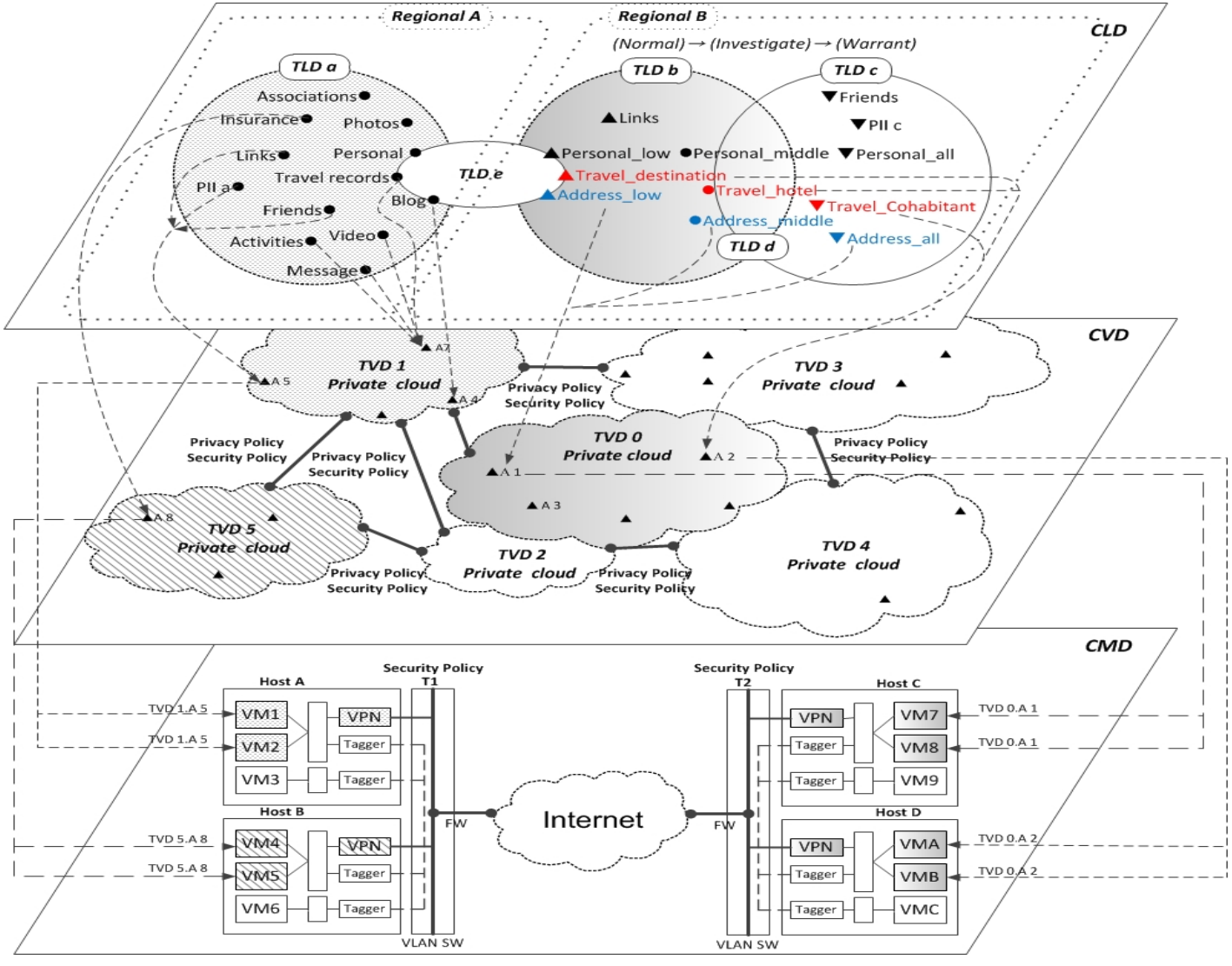
1. Cloud Legalized Domain (CLD) top layer:
   A *legal cages* model for a Trusted Legal Domain (TLD)
2. Cloud Virtual Domain (CVD) middle layer:
   A *logical cages* model for a Trusted Virtual Domain (TVD)
3. Cloud Machine Domain (CMD) bottom layer:
   A *physical cages* model for a Trusted Machine Domain (TMD)


A Semantics-enabled Policy Framework

We propose a three-layer architecture of a semantics-enabled policy framework:

1. Cloud Legalized Domain (CLD) top layer:
   A *legal cages* model for a Trusted Legal Domain (TLD)
2. Cloud Virtual Domain (CVD) middle layer:
   A *logical cages* model for a Trusted Virtual Domain (TVD)
3. Cloud Machine Domain (CMD) bottom layer:
   A *physical cages* model for a Trusted Machine Domain (TMD)


A Semantics-enabled Policy Framework (conti.)



Which Privacy Laws Should be Applied?

- When we enforce the legalized data sharing and protection policies, the relationships between adjacent layers' domains should be addressed .
- Before that, we have to decide which privacy laws should be applied (Peter Fleischer: Privacy...?):
  - Location of the organization using the data:
    Article 4(1)(a) of the EU Data Protection Directive.
  - Location of the people whose data is being used:
    USA Children's Online Privacy Protection Act (COPPA).
  - Place where the actual processing happens:
    Article 4(1)(c) of the EU Data Protection Directive.
- How about multi-national data management operations?


Which Privacy Laws Should be Applied?

- When we enforce the legalized data sharing and protection policies, the relationships between adjacent layers' domains should be addressed .
- Before that, we have to decide which privacy laws should be applied (Peter Fleischer: Privacy...?):
  - Location of the organization using the data:
    Article 4(1)(a) of the EU Data Protection Directive.
  - Location of the people whose data is being used:
    USA Children's Online Privacy Protection Act (COPPA).
  - Place where the actual processing happens:
    Article 4(1)(c) of the EU Data Protection Directive.
- How about multi-national data management operations?

Which Privacy Laws Should be Applied?

- When we enforce the legalized data sharing and protection policies, the relationships between adjacent layers' domains should be addressed .
- Before that, we have to decide which privacy laws should be applied (Peter Fleischer: Privacy...?):
  - Location of the organization using the data:
    Article 4(1)(a) of the EU Data Protection Directive.
  - Location of the people whose data is being used:
    USA Children's Online Privacy Protection Act (COPPA).
  - Place where the actual processing happens:
    Article 4(1)(c) of the EU Data Protection Directive.
- How about multi-national data management operations?

Which Privacy Laws Should be Applied?

- When we enforce the legalized data sharing and protection policies, the relationships between adjacent layers' domains should be addressed .
- Before that, we have to decide which privacy laws should be applied (Peter Fleischer: Privacy...?):
  - Location of the organization using the data:
    Article 4(1)(a) of the EU Data Protection Directive.
  - Location of the people whose data is being used:
    USA Children's Online Privacy Protection Act (COPPA).
  - Place where the actual processing happens:
    Article 4(1)(c) of the EU Data Protection Directive.
- How about multi-national data management operations?

Which Privacy Laws Should be Applied?

- When we enforce the legalized data sharing and protection policies, the relationships between adjacent layers' domains should be addressed .
- Before that, we have to decide which privacy laws should be applied (Peter Fleischer: Privacy...?):
  - Location of the organization using the data:
    Article 4(1)(a) of the EU Data Protection Directive.
  - Location of the people whose data is being used:
    USA Children's Online Privacy Protection Act (COPPA).
  - Place where the actual processing happens:
    Article 4(1)(c) of the EU Data Protection Directive.
- How about multi-national data management operations?

Which Privacy Laws Should be Applied?

- When we enforce the legalized data sharing and protection policies, the relationships between adjacent layers' domains should be addressed .
- Before that, we have to decide which privacy laws should be applied (Peter Fleischer: Privacy...?):
  - Location of the organization using the data:
    Article 4(1)(a) of the EU Data Protection Directive.
  - Location of the people whose data is being used:
    USA Children's Online Privacy Protection Act (COPPA).
  - Place where the actual processing happens:
    Article 4(1)(c) of the EU Data Protection Directive.
- How about multi-national data management operations?

Formal Policy Deployment

1. The TLD's legal virtual boundary is determined by a particular law that regulates the data disclosure range and level, where the semantics-enabled policies should be compliant with the TLD's laws.
2. When a data usage context is created for a data user to request information, the possible semantics-enabled policies related to the laws are identified and executed.
3. A data usage context possibly includes a purpose, a data user's role, a requester location, a data location, and action, etc.

Formal Policy Deployment

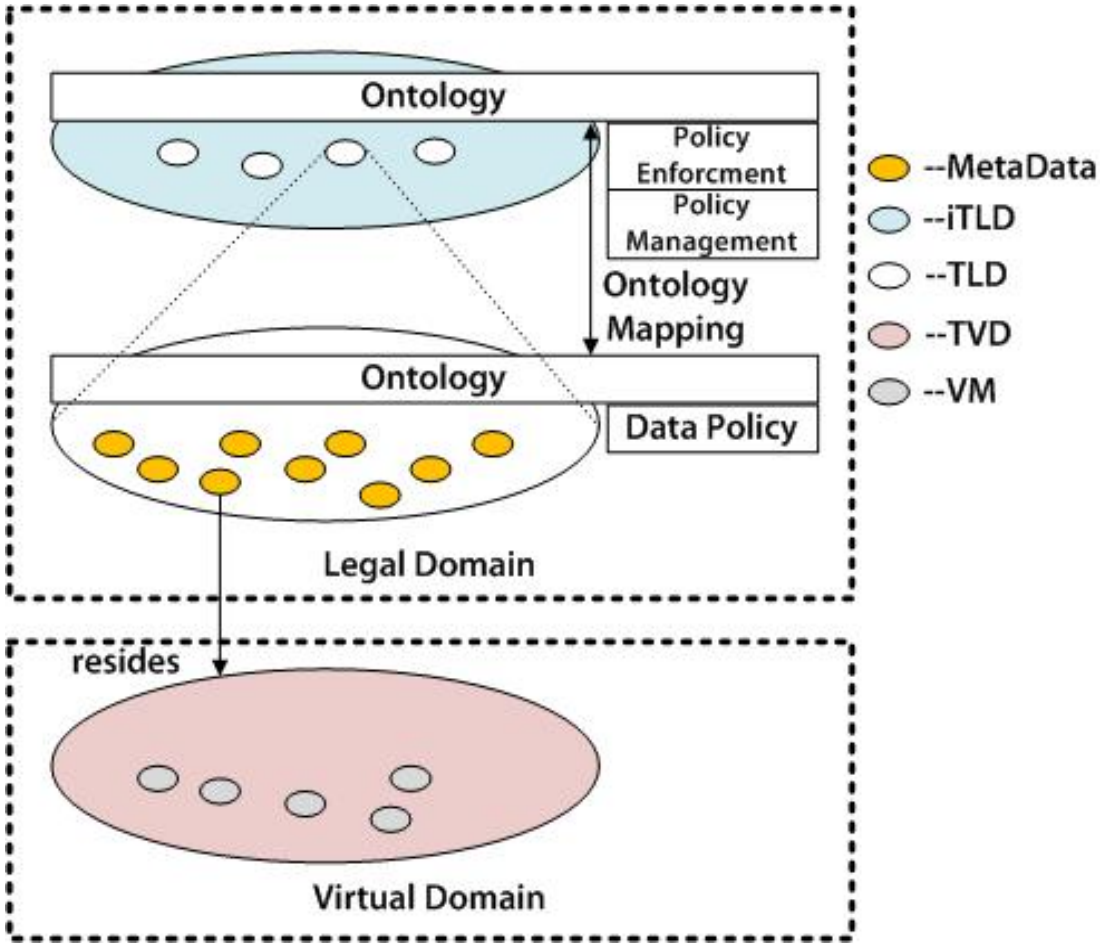
1. The TLD's legal virtual boundary is determined by a particular law that regulates the data disclosure range and level, where the semantics-enabled policies should be compliant with the TLD's laws.
2. When a data usage context is created for a data user to request information, the possible semantics-enabled policies related to the laws are identified and executed.
3. A data usage context possibly includes a purpose, a data user's role, a requester location, a data location, and action, etc.


Formal Policy Deployment

1. The TLD's legal virtual boundary is determined by a particular law that regulates the data disclosure range and level, where the semantics-enabled policies should be compliant with the TLD's laws.
2. When a data usage context is created for a data user to request information, the possible semantics-enabled policies related to the laws are identified and executed.
3. A data usage context possibly includes a purpose, a data user's role, a requester location, a data location, and action, etc.

From CLD to CVD

Legal Domain vs. Virtual Domain



Part IV

Unifying Formal Policies

Formal Policy Integration

1. The semantics-enabled policies for an intersection area of TLDs are compliant with applicable laws of multiple TLDs.
2. We face a law integration problem that turns into a semantics-enabled formal policies integration problem.
3. When unifying multiple formal policies, we *map* and *merge* local ontologies from different TLDs' policies and construct a global ontology for these unified formal policies.
4. Two types of formal policies, privacy protection and national security, are unified manually to enforce a national security purpose in the social network cloud.


Formal Policy Integration

1. The semantics-enabled policies for an intersection area of TLDs are compliant with applicable laws of multiple TLDs.
2. We face a law integration problem that turns into a semantics-enabled formal policies integration problem.
3. When unifying multiple formal policies, we *map* and *merge* local ontologies from different TLDs' policies and construct a global ontology for these unified formal policies.
4. Two types of formal policies, privacy protection and national security, are unified manually to enforce a national security purpose in the social network cloud.

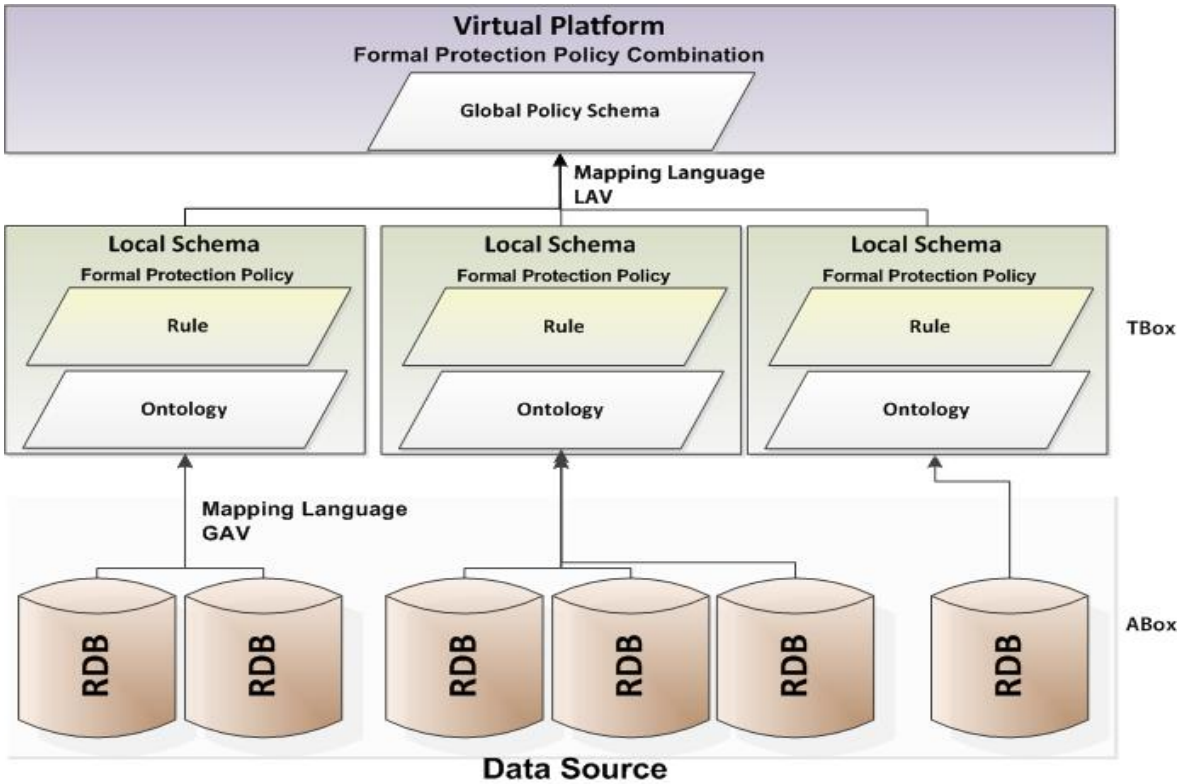

Formal Policy Integration

1. The semantics-enabled policies for an intersection area of TLDs are compliant with applicable laws of multiple TLDs.
2. We face a law integration problem that turns into a semantics-enabled formal policies integration problem.
3. When unifying multiple formal policies, we *map* and *merge* local ontologies from different TLDs' policies and construct a global ontology for these unified formal policies.
4. Two types of formal policies, privacy protection and national security, are unified manually to enforce a national security purpose in the social network cloud.


Formal Policy Integration

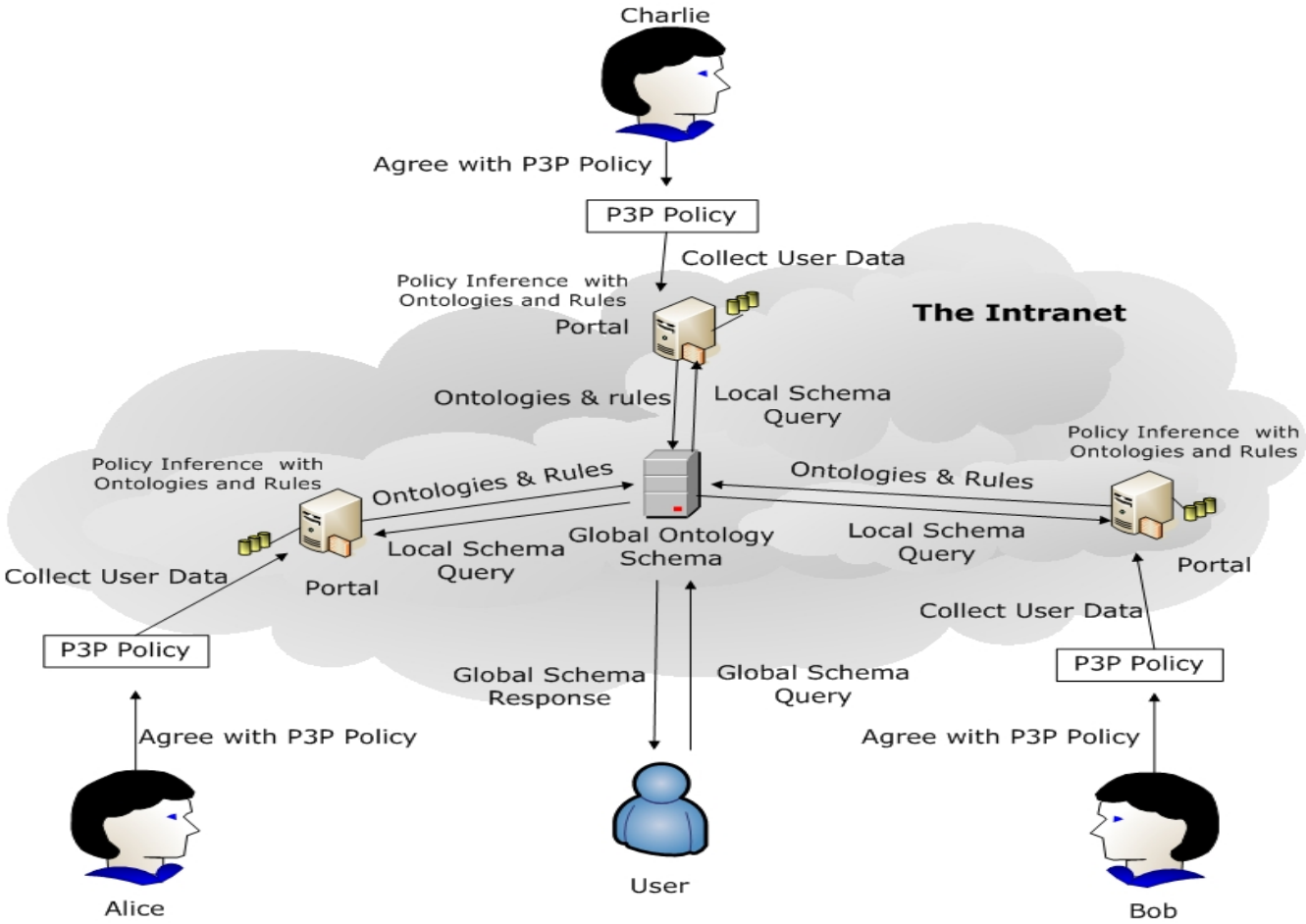
1. The semantics-enabled policies for an intersection area of TLDs are compliant with applicable laws of multiple TLDs.
2. We face a law integration problem that turns into a semantics-enabled formal policies integration problem.
3. When unifying multiple formal policies, we *map* and *merge* local ontologies from different TLDs' policies and construct a global ontology for these unified formal policies.
4. Two types of formal policies, privacy protection and national security, are unified manually to enforce a national security purpose in the social network cloud.


A Semantic Privacy-Preserving Model



–Hu, Y.J., Yang, J.J., A semantic privacy-preserving model for data sharing and integration. *WIMS'11*, Norway, ACM (2011)

A Semantic Privacy-Preserving Model (conti.)



–Hu, Y.J., Yang, J.J., A semantic privacy-preserving model for data sharing and integration. *WIMS'11*, Norway, ACM (2011)

Privacy Protection Policies

1. A privacy protection policy is a type of formal policy used for specifying a data usage constraint created by a data owner.
2. A data owner's Personal Identifiable Information (PII) is collected by a data controller, analyzed by a data processor, and accessed by a data user.
3. All of these operations are protected under the TLD privacy protection law's umbrella.
4. When a data request, including collection, analysis, and use, is asked for, we first consider the data usage context of this request.
5. This allows us to decide how many and at what level PII can be disclosed to comply with the privacy laws.


Privacy Protection Policies

1. A privacy protection policy is a type of formal policy used for specifying a data usage constraint created by a data owner.
2. A data owner's Personal Identifiable Information (PII) is collected by a data controller, analyzed by a data processor, and accessed by a data user.
3. All of these operations are protected under the TLD privacy protection law's umbrella.
4. When a data request, including collection, analysis, and use, is asked for, we first consider the data usage context of this request.
5. This allows us to decide how many and at what level PII can be disclosed to comply with the privacy laws.


Privacy Protection Policies

1. A privacy protection policy is a type of formal policy used for specifying a data usage constraint created by a data owner.
2. A data owner's Personal Identifiable Information (PII) is collected by a data controller, analyzed by a data processor, and accessed by a data user.
3. All of these operations are protected under the TLD privacy protection law's umbrella.
4. When a data request, including collection, analysis, and use, is asked for, we first consider the data usage context of this request.
5. This allows us to decide how many and at what level PII can be disclosed to comply with the privacy laws.


Privacy Protection Policies

1. A privacy protection policy is a type of formal policy used for specifying a data usage constraint created by a data owner.
2. A data owner's Personal Identifiable Information (PII) is collected by a data controller, analyzed by a data processor, and accessed by a data user.
3. All of these operations are protected under the TLD privacy protection law's umbrella.
4. When a data request, including collection, analysis, and use, is asked for, we first consider the data usage context of this request.
5. This allows us to decide how many and at what level PII can be disclosed to comply with the privacy laws.


Privacy Protection Policies

1. A privacy protection policy is a type of formal policy used for specifying a data usage constraint created by a data owner.
2. A data owner's Personal Identifiable Information (PII) is collected by a data controller, analyzed by a data processor, and accessed by a data user.
3. All of these operations are protected under the TLD privacy protection law's umbrella.
4. When a data request, including collection, analysis, and use, is asked for, we first consider the data usage context of this request.
5. This allows us to decide how many and at what level PII can be disclosed to comply with the privacy laws.


National Security Policies

1. When a national security officer intends to access a group of suspects' PII, a data usage context is also created for this request.
2. The data usage context of this information request is created, including a national security officer's user role, an investigation purpose, a data user's location,etc.
3. Formal policies, based on the national security laws, are fetched to circumscribe the TLD's virtual boundary of a data usage.
4. Once the laws are revised, the data usage context will be changed and the TLD's virtual boundary of a data usage will be updated.
5. The formal policy framework provides a flexible policy re-mapping mechanism while applying the new laws to redraw a TLD's virtual boundary.


National Security Policies

1. When a national security officer intends to access a group of suspects' PII, a data usage context is also created for this request.
2. The data usage context of this information request is created, including a national security officer's user role, an investigation purpose, a data user's location,etc.
3. Formal policies, based on the national security laws, are fetched to circumscribe the TLD's virtual boundary of a data usage.
4. Once the laws are revised, the data usage context will be changed and the TLD's virtual boundary of a data usage will be updated.
5. The formal policy framework provides a flexible policy re-mapping mechanism while applying the new laws to redraw a TLD's virtual boundary.


National Security Policies

1. When a national security officer intends to access a group of suspects' PII, a data usage context is also created for this request.
2. The data usage context of this information request is created, including a national security officer's user role, an investigation purpose, a data user's location,etc.
3. Formal policies, based on the national security laws, are fetched to circumscribe the TLD's virtual boundary of a data usage.
4. Once the laws are revised, the data usage context will be changed and the TLD's virtual boundary of a data usage will be updated.
5. The formal policy framework provides a flexible policy re-mapping mechanism while applying the new laws to redraw a TLD's virtual boundary.

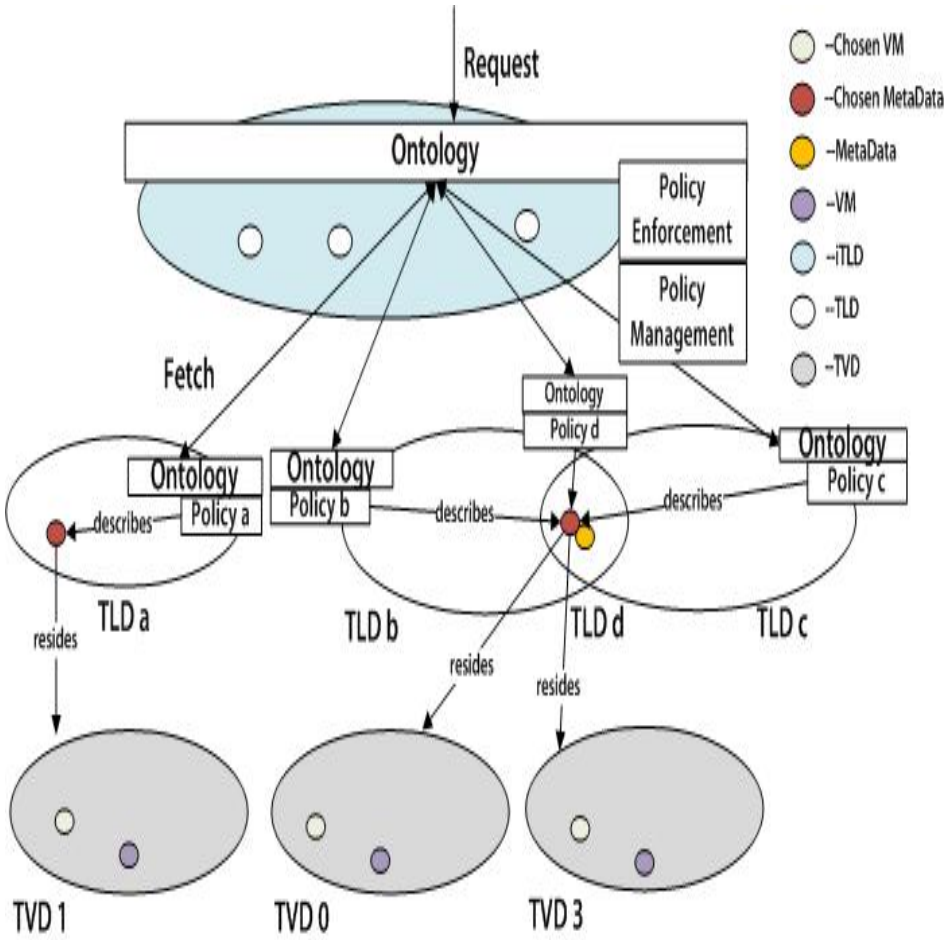

National Security Policies

1. When a national security officer intends to access a group of suspects' PII, a data usage context is also created for this request.
2. The data usage context of this information request is created, including a national security officer's user role, an investigation purpose, a data user's location,etc.
3. Formal policies, based on the national security laws, are fetched to circumscribe the TLD's virtual boundary of a data usage.
4. Once the laws are revised, the data usage context will be changed and the TLD's virtual boundary of a data usage will be updated.
5. The formal policy framework provides a flexible policy re-mapping mechanism while applying the new laws to redraw a TLD's virtual boundary.

National Security Policies

1. When a national security officer intends to access a group of suspects' PII, a data usage context is also created for this request.
2. The data usage context of this information request is created, including a national security officer's user role, an investigation purpose, a data user's location,etc.
3. Formal policies, based on the national security laws, are fetched to circumscribe the TLD's virtual boundary of a data usage.
4. Once the laws are revised, the data usage context will be changed and the TLD's virtual boundary of a data usage will be updated.
5. The formal policy framework provides a flexible policy re-mapping mechanism while applying the new laws to redraw a TLD's virtual boundary.


A Data Usage Request for Information Disclosure



Unifying Formal Policies

1. Whether the objectives of greater national security and greater personal privacy can be compromised?
2. Balancing the national security and privacy protection by using information technologies to counter terrorism and also to safeguard civil liberties.
3. When we identify the terrorist suspects to avoid privacy rights violation, we issue pattern-based data queries iteratively.
4. The semantics-enabled polices reasoning can provide additional evidence for updating the data usage context to enforce national security policies iteratively; however the information disclosure still respects the data protection policies.


Unifying Formal Policies

1. Whether the objectives of greater national security and greater personal privacy can be compromised?
2. Balancing the national security and privacy protection by using information technologies to counter terrorism and also to safeguard civil liberties.
3. When we identify the terrorist suspects to avoid privacy rights violation, we issue pattern-based data queries iteratively.
4. The semantics-enabled polices reasoning can provide additional evidence for updating the data usage context to enforce national security policies iteratively; however the information disclosure still respects the data protection policies.


Unifying Formal Policies

1. Whether the objectives of greater national security and greater personal privacy can be compromised?
2. Balancing the national security and privacy protection by using information technologies to counter terrorism and also to safeguard civil liberties.
3. When we identify the terrorist suspects to avoid privacy rights violation, we issue pattern-based data queries iteratively.
4. The semantics-enabled polices reasoning can provide additional evidence for updating the data usage context to enforce national security policies iteratively; however the information disclosure still respects the data protection policies.


Unifying Formal Policies

1. Whether the objectives of greater national security and greater personal privacy can be compromised?
2. Balancing the national security and privacy protection by using information technologies to counter terrorism and also to safeguard civil liberties.
3. When we identify the terrorist suspects to avoid privacy rights violation, we issue pattern-based data queries iteratively.
4. The semantics-enabled polices reasoning can provide additional evidence for updating the data usage context to enforce national security policies iteratively; however the information disclosure still respects the data protection policies.


Unifying Formal Policies (conti.)

1. When a data usage context is moved into the intersection of TLDs, this implies the privacy protection and national security policy are unified.
2. The ontologies of these policies will be mapped and merged and rules will be further integrated to enforce the data usage within the TLDs' intersection.
3. When applying pattern-based data usage in the TLDs' intersection, we follow the PII stepwise anonymous disclosure principles if supporting evidence is not strong enough to allow a full information disclosure.
4. Handling anonymous information requires multiple stages of human-driven analysis with reasoning of unified policies, where a third-party legal authority establishes sufficient probable cause to trigger the event.


Unifying Formal Policies (conti.)

1. When a data usage context is moved into the intersection of TLDs, this implies the privacy protection and national security policy are unified.
2. The ontologies of these policies will be mapped and merged and rules will be further integrated to enforce the data usage within the TLDs' intersection.
3. When applying pattern-based data usage in the TLDs' intersection, we follow the PII stepwise anonymous disclosure principles if supporting evidence is not strong enough to allow a full information disclosure.
4. Handling anonymous information requires multiple stages of human-driven analysis with reasoning of unified policies, where a third-party legal authority establishes sufficient probable cause to trigger the event.

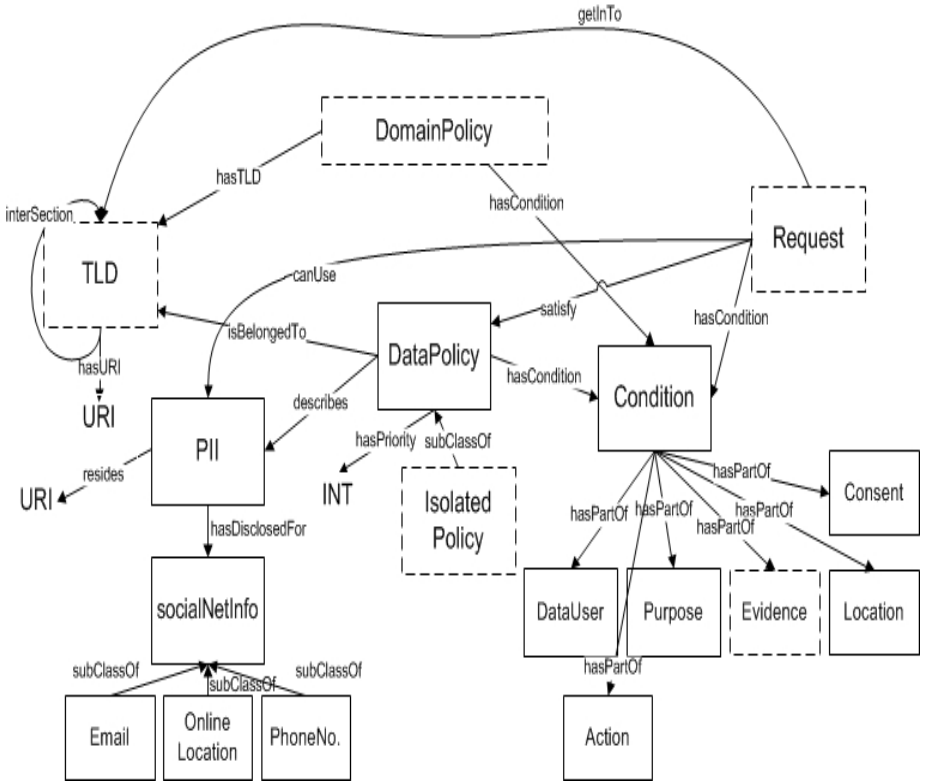

Unifying Formal Policies (conti.)

1. When a data usage context is moved into the intersection of TLDs, this implies the privacy protection and national security policy are unified.
2. The ontologies of these policies will be mapped and merged and rules will be further integrated to enforce the data usage within the TLDs' intersection.
3. When applying pattern-based data usage in the TLDs' intersection, we follow the PII stepwise anonymous disclosure principles if supporting evidence is not strong enough to allow a full information disclosure.
4. Handling anonymous information requires multiple stages of human-driven analysis with reasoning of unified policies, where a third-party legal authority establishes sufficient probable cause to trigger the event.


Unifying Formal Policies (conti.)

1. When a data usage context is moved into the intersection of TLDs, this implies the privacy protection and national security policy are unified.
2. The ontologies of these policies will be mapped and merged and rules will be further integrated to enforce the data usage within the TLDs' intersection.
3. When applying pattern-based data usage in the TLDs' intersection, we follow the PII stepwise anonymous disclosure principles if supporting evidence is not strong enough to allow a full information disclosure.
4. Handling anonymous information requires multiple stages of human-driven analysis with reasoning of unified policies, where a third-party legal authority establishes sufficient probable cause to trigger the event.


An Ontology for a Formal Policy of a TLD



A Formal Domain Policy of a TLD

A partial ontology for a domain policy:

- $\texttt{hasTLD.DomainPolicy(d)}$, $\texttt{hasTLD}^{-}\texttt{.TLD(d)}$
- $\texttt{hasCondition.DomainPolicy(d)}$, $\texttt{hasCondition}^{-}\texttt{.Condition(d)}$
- $\texttt{hasPartOf.Condition(d)}$, $\texttt{hasPartOf}^{-}\texttt{.Purpose(investigation)}$
- $\texttt{hasPartOf}^{-}\texttt{.DataUser(securityPersonnel)}$
- $\texttt{hasPartOf}^{-}\texttt{.Location(TW)}$, $\texttt{hasPartOf}^{-}\texttt{.Evidence(things)}$
- $\texttt{hasPartOf}^{-}\texttt{.Consent(nill)}$

A rule for a domain policy enforcement

- $\texttt{Request(?x)} \wedge \texttt{hasCondition(?x, ?c)} \wedge \texttt{Condition(?c)}$
  $\wedge\ \texttt{hasCondition(?d, ?dc)} \wedge \texttt{Condition(?dc)}$
  $\wedge\ \texttt{DomainPolicy(?d)} \wedge \texttt{hasTLD(?d, ?tld)}$

  $\longrightarrow \texttt{getInTo(?x, ?tld)} \leftarrow (1)$


A Formal Domain Policy of a TLD

A partial ontology for a domain policy:

- $\texttt{hasTLD.DomainPolicy(d)}$, $\texttt{hasTLD}^{-}\texttt{.TLD(d)}$
- $\texttt{hasCondition.DomainPolicy(d)}$, $\texttt{hasCondition}^{-}\texttt{.Condition(d)}$
- $\texttt{hasPartOf.Condition(d)}$, $\texttt{hasPartOf}^{-}\texttt{.Purpose(investigation)}$
- $\texttt{hasPartOf}^{-}\texttt{.DataUser(securityPersonnel)}$
- $\texttt{hasPartOf}^{-}\texttt{.Location(TW)}$, $\texttt{hasPartOf}^{-}\texttt{.Evidence(things)}$
- $\texttt{hasPartOf}^{-}\texttt{.Consent(nill)}$

A rule for a domain policy enforcement

- $\texttt{Request(?x)} \wedge \texttt{hasCondition(?x, ?c)} \wedge \texttt{Condition(?c)}$
  $\wedge\ \texttt{hasCondition(?d, ?dc)} \wedge \texttt{Condition(?dc)}$
  $\wedge\ \texttt{DomainPolicy(?d)} \wedge \texttt{hasTLD(?d, ?tld)}$

  $\longrightarrow \texttt{getInTo(?x, ?tld)} \leftarrow (1)$


A Formal Data Policy of a TLD

A partial ontology for a data policy

- $\texttt{isBelongedTo.DataPolicy(d)}$, $\texttt{isBelongedTo}^{-}\texttt{.TLD(d)}$
- $\texttt{describes.DataPolicy(d)}$, $\texttt{describes}^{-}\texttt{.PII(d)}$
- $\texttt{hasDisclosedFor.PII(d)}$, $\texttt{hasDisclosedFor}^{-}\texttt{.socialNetInfo(d)}$
- $\texttt{socialNetInfo(d)} \equiv \texttt{Email(d)} \sqcup \texttt{OnlineLocation(d)} \sqcup \texttt{phoneNo.(d)}.$

A rule for a data policy enforcement

- $\texttt{Request(?r)} \wedge \texttt{satisfy(?r, ?x)} \wedge \texttt{DataPolicy(?d)} \wedge \texttt{describes(?d, ?pii)} \wedge \texttt{hasDisclosedFor(?pii, ?sInfo)} \wedge \texttt{Evidence(things)}$

  $\longrightarrow \texttt{canUse(?r, ?pii)} \wedge \texttt{socialNetInfo(?sInfo)} \leftarrow (2)$


A Formal Data Policy of a TLD

A partial ontology for a data policy

- $\texttt{isBelongedTo.DataPolicy(d)}$, $\texttt{isBelongedTo}^{-}\texttt{.TLD(d)}$
- $\texttt{describes.DataPolicy(d)}$, $\texttt{describes}^{-}\texttt{.PII(d)}$
- $\texttt{hasDisclosedFor.PII(d)}$, $\texttt{hasDisclosedFor}^{-}\texttt{.socialNetInfo(d)}$
- $\texttt{socialNetInfo(d)} \equiv \texttt{Email(d)} \sqcup \texttt{OnlineLocation(d)} \sqcup \texttt{phoneNo.(d)}.$

A rule for a data policy enforcement

- $\texttt{Request(?r)} \wedge \texttt{satisfy(?r, ?x)} \wedge \texttt{DataPolicy(?d)} \wedge \texttt{describes(?d, ?pii)} \wedge \texttt{hasDisclosedFor(?pii, ?sInfo)} \wedge \texttt{Evidence(things)}$

  $\longrightarrow \texttt{canUse(?r, ?pii)} \wedge \texttt{socialNetInfo(?sInfo)} \leftarrow (2)$

Related Work

References

- Cloud computing, privacy and security: [2] [4] [6] [18]
- A privacy policy model: [2] [1] [15]
- data sharing and protection: [5] [7] [8] [13]
- Policy and meta-policy: [3] [11] [12] [14] [19] [20]
- National security policy: [9] [16] [17]


Part V

Conclusion and Future Work

Conclusion

1. Semantics-enabled policies are presented as a combination of ontologies and rules.
2. Unifying privacy protection policies with national security policies in the social network cloud.
3. Formal policy integration is indicated as ontologies merging and rules integration from multiple judicial domains.
4. A data request for a counter-crime example is demonstrated to simultaneously enforce privacy protection and national security policies.
5. We intend to provide legal information sharing services for national security without violating the data protection law in the cloud.


Conclusion

1. Semantics-enabled policies are presented as a combination of ontologies and rules.
2. Unifying privacy protection policies with national security policies in the social network cloud.
3. Formal policy integration is indicated as ontologies merging and rules integration from multiple judicial domains.
4. A data request for a counter-crime example is demonstrated to simultaneously enforce privacy protection and national security policies.
5. We intend to provide legal information sharing services for national security without violating the data protection law in the cloud.

Conclusion

1. Semantics-enabled policies are presented as a combination of ontologies and rules.
2. Unifying privacy protection policies with national security policies in the social network cloud.
3. Formal policy integration is indicated as ontologies merging and rules integration from multiple judicial domains.
4. A data request for a counter-crime example is demonstrated to simultaneously enforce privacy protection and national security policies.
5. We intend to provide legal information sharing services for national security without violating the data protection law in the cloud.


Conclusion

1. Semantics-enabled policies are presented as a combination of ontologies and rules.
2. Unifying privacy protection policies with national security policies in the social network cloud.
3. Formal policy integration is indicated as ontologies merging and rules integration from multiple judicial domains.
4. A data request for a counter-crime example is demonstrated to simultaneously enforce privacy protection and national security policies.
5. We intend to provide legal information sharing services for national security without violating the data protection law in the cloud.


Conclusion

1. Semantics-enabled policies are presented as a combination of ontologies and rules.
2. Unifying privacy protection policies with national security policies in the social network cloud.
3. Formal policy integration is indicated as ontologies merging and rules integration from multiple judicial domains.
4. A data request for a counter-crime example is demonstrated to simultaneously enforce privacy protection and national security policies.
5. We intend to provide legal information sharing services for national security without violating the data protection law in the cloud.


Future Work

- Consider a multi-national operations across different jurisdictions through unifying the applicable privacy and data protection policies in the cloud.
- Automatically unify semantics-enabled policies from multiple judicial domains to achieve the flexible and optimal data operations in the cloud?
- A full scale of cloud system implementation for information sharing and protection in the social network.

Future Work

- Consider a multi-national operations across different jurisdictions through unifying the applicable privacy and data protection policies in the cloud.
- Automatically unify semantics-enabled policies from multiple judicial domains to achieve the flexible and optimal data operations in the cloud?
- A full scale of cloud system implementation for information sharing and protection in the social network.

Future Work

- Consider a multi-national operations across different jurisdictions through unifying the applicable privacy and data protection policies in the cloud.
- Automatically unify semantics-enabled policies from multiple judicial domains to achieve the flexible and optimal data operations in the cloud?
- A full scale of cloud system implementation for information sharing and protection in the social network.

Part VI

References


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


Ardagna, A.C., et al.:
A privacy-aware access control system.
Journal of Computer Security **16** (2008) 369–397


Berger, S., et al.:
Security for the cloud infrastructure: Trusted virtual data center implementation.
IBM Journal of Research and Development (2009) 6:1–6:12


Bonatti, P., Olmedilla, D.:
Policy language specification, enforcement, and integration. project deliverable D2, working group I2.
Technical report, REWERSE (2005)


Bruening, J.P., Treacy, B.C.:
Cloud computing: privacy, security challenges.
Privacy & Security Law Report (2009)


Buchanan, W., et al.:
Interagency data exchange protocols as computational data protection law.
In: Legal Knowledge and Information Systems - JURIX, IOS Press (2010) 143–146



Cabuk, S., et al.:
Towards automated security policy enforcement in multi-tenant virtual data centers.
Journal of Computer Security **18** (2010) 89–121


Calvanese, D., Giacomo, G.D.:
Data integration: A logic-based perspective.
AI Magazine **26** (2005) 59–70


Clifton, C., et al.:
Privacy-preserving data integration and sharing.
In: Data Mining and Knowledge Discovery, ACM (2004) 19–26


Deyrup, I., et al.:
Cloud Computing & National Security Law.
Tech. Report from The Harvard Law National Security Research Group (Oct. 2010).


Gruber, T.R.:
A translation approach to portable ontology specifications.
Knowledge Acquisition **5** (1993)


Hosmer, H.H.:
Metapolicies I.
ACM SIGSAC Review **10** (1992) 18–43


Hu, Y.J., Boley, H.:
SemPIF: A semantic meta-policy interchange format for multiple web policies.
In: 2010 IEEE/WIC/ACM Int. Conference on Web Intelligence and Intelligent Agent Technology, IEEE (2010) 302–307


Hu, Y.J., Yang, J.J.:
A semantic privacy-preserving model for data sharing and integration.
In: International Conference on Web Intelligence, Mining and Semantics (WIMS'11), Norway, ACM (2011)


Kagal, L., et al.:
Using semantic web technologies for policy management on the web.
In: 21st National Conference on Artificial Intelligence (AAAI), AAAI (2006)


Karjoth, G., et al.:
Translating privacy practices into privacy promises - how to promise what you can keep.
In: POLICY'03, IEEE (2003)


Kettler, B., et al.:
Facilitating information sharing across intelligence community boundaries using knowledge management and semantic web technologies.
In Popp, L.R., Yen, J., eds.: Emergent Information Technologies and Enabling Policies for Counter-Terrorism.
Wiley (2005) 175–195


Popp, R., Poindexter, J.:
Countering terrorism through information and privacy protection technologies.
IEEE Seurity & Privacy **4** (2006) 24–33


Takabi, H., et al.:
Security and privacy challenges in cloud computing environments.
IEEE Seurity & Privacy **8** (2010) 24–31

Tonti, G., et al.:
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 (2003) 419–437

Vimercati, S.D.C.d., et al.:
Second research report on next generation policies, project deliverable D5.2.2.
Technical report, PrimeLife (2010)