Legal Requirements: From Theory to Practice

Travis D. Breaux, PhD Candidate
North Carolina State University
tdbreaux@ncsu.edu

IFIP Working Group 2.9, February 29, 2008
IFIP WG2.9 Talk Outline

next: research setup

(1) Research Setup
- Problem and motivation
- Background
- Research methodology

(2) Acquisition
- Types of legal statements
- Identifying requirements
- Standard upper ontology
- Frame-based method

(3) Formalization
- Stakeholder/Goal hierarchies
- Catalogue of constraints
- Priority hierarchies

(4) Specification
- Requirement metrics
- Refinement patterns
Problem and Motivation

- Health Insurance Accountability and Portability Act (HIPAA) Privacy Rule governs access to medical information
- HIPAA is limited to electronic patient health information
- HIPAA Privacy Rule affects 545,000 establishments who employ 13.5M people
- Projected HIPAA compliance costs: $12-$42B

In software engineering, verification begins by understanding the software requirements
Background

laws, regulations and standards

U.S. Congress ratifies legislation (statutes)

Executive branch agencies (FAA, FDA, FTC, HHS) create regulations (rules)

Industry creates standards that support regulations
Industry and government perform regulatory audits

U.S. Federal courts decide:
(1) industry compliance with regulations
(2) regulatory compliance with statutes
(3) statutory compliance with the Constitution
Background

characteristics of legal requirements

- Legal requirements are never reworded – they may only be interpreted, refined or superseded
- The meaning of compliance and enforcement for each requirement is subject to change
- Legal requirements are reusable across industries
Background

*defining legal compliance*

- **Compliance** means to maintain a defensible position in a court of law.

- **Due diligence** refers to reasonable efforts that persons make to satisfy legal requirements or discharge their legal obligations.

- **Standard of care** means “under the law of negligence or of obligations, the conduct demanded of a person in a situation; typically, this involves a person giving attention both to possible dangers, mistakes and pitfalls and to ways of minimizing those risks.”

*Black’s Law Dictionary, 8th ed.*
Research Methodology

- Exploratory case studies [Yin 2003]
- Constructivist and pragmatist knowledge claims [Creswell 2003]
- Grounded theory [Glaser and Strauss 1967]
- Pattern-matching to formulate propositions [Campbell 1966]
Research Methodology

research questions

- **RQ1**: What types of legal requirements exist in policies and regulations?
- **RQ2**: What inferences must engineers make to account for these requirements?
- **RQ3**: How do practitioners manage conformance with legal requirements?
Research Methodology
domains and phenomena

- **(Privacy)** Use and disclosure of patient medical information
  - Health Insurance Portability and Accountability Act (HIPAA) of 1996
  - Gramm-Leach-Bliley Act (GLBA) of 1999
  - Stakeholder focus

- **(Accessibility)** Access by individuals with disabilities
  - Section 508, as amended in the Workforce Investment Act of 1998
  - Product focus
IFIP WG2.9 Talk Outline

next: acquisition

(1) Research Setup
- Problem and motivation
- Background
- Research methodology

(2) Acquisition
- Types of legal statements
- Identifying requirements
- Standard upper ontology
- Frame-based method

(3) Formalization
- Stakeholder/Goal hierarchies
- Catalogue of constraints
- Priority hierarchies

(4) Specification
- Requirement metrics
- Refinement patterns
Types of Legal Statements

Statements about actions that a stakeholder or product is...

- Permitted to perform (Permission)
- Required to perform (Obligation)
- Required to not perform (Refrainment)
- Not expressly permitted or required to perform (Exclusion)

**Definition** is a statement that restricts the meaning of a term by one or more constraints
Identifying Legal Requirements – 2

marking rights, obligations and constraints

1) The covered entity who has a direct treatment relationship with the individual **must**…
   
a) Provide notice **no later than the first service delivery**;

2) For the purposes of paragraph (1), a covered entity who delivers services electronically **must** provide electronic notice **unless** the individual requests to receive a paper notice.

Obligations are **red**;

Constraints are **underlined**; and

Modal/ condition keywords are **bold**.

*From HIPAA §160.520(c)(2)-(3).*
1) \([O_1]\) The covered entity \([C_1]\) who has a direct treatment relationship with the individual must…

   a) Provide notice \([C_2]\) no later than the first service delivery;

\[O_1:\] The covered entity **must** provide notice *to the individual*. 
   (1)(a); \([C_1 \land C_2]\)

\[C_1:\] The covered entity has a direct treatment relationship with the individual. \((1)\)

\[C_2:\] The notice is provided no later than the first service delivery. \((a)\)
Identifying Legal Requirements – 4

negating constraints for exceptions

2) For the purposes of paragraph (1), [\(O_2\)] a covered entity [\(C_3\)] who delivers services electronically must provide electronic notice unless [\(C_4\)] the individual requests to receive a paper notice.

\[
\begin{align*}
O_2: & \quad \text{The covered entity must provide electronic notice to the individual. (2)}; [C_3 \land \neg C_4] \\
C_3: & \quad \text{The covered entity delivers services electronically to the individual. (2)} \\
C_4: & \quad \text{The individual requests to receive a paper notice. (2)}
\end{align*}
\]
1) \([O_1]\) The covered entity \([C_1]\) who has a direct treatment relationship with the individual \textbf{must}…
   a) Provide notice \([C_2]\) no later than the first service delivery;
2) For the purposes of paragraph (1), \([O_1]\) a covered entity \([C_3]\) who delivers services electronically \textbf{must} provide electronic notice unless… \([C_4]\)

- From paragraph (1) we extracted \(O_1: [C_1 \land C_2]\)
- Now we carry down \(C_1\) and \(C_2\) from paragraph (1) to yield \(O_2: [C_1 \land C_2 \land C_3 \land \neg C_4]\)
Standard Upper Ontology
for legal requirements

Legend:
- Leads from part to whole
- Leads from sub-class to super-class
- Placeholder concept
- Phrase-level concept
- Statement-level concept

State

Rule

Permission
Obligation
Refrainment
Exclusion

Definition

Term
Kind
Description

Subject
Act
Object
Purpose
Instrument
Target

1
1
..*
0..*
0..*

State

Quality

Condition
Exception

Action

Transaction

Rule

Permission
Obligation
Refrainment
Exclusion
Definition

Term
Kind
Description

Subject
Act
Object
Purpose
Instrument
Target

1
1
..*
0..*
0..*

Legend:
## Identifying Legal Requirements – 1

**phrase heuristics**

<table>
<thead>
<tr>
<th>Phrase Pattern</th>
<th>Concept</th>
<th>Phrase Pattern</th>
<th>Concept</th>
</tr>
</thead>
<tbody>
<tr>
<td>if</td>
<td>Condition</td>
<td>must deny*</td>
<td>Obligation</td>
</tr>
<tr>
<td>when</td>
<td>Condition</td>
<td>must permit*</td>
<td>Obligation</td>
</tr>
<tr>
<td>except when</td>
<td>Exception</td>
<td>must request*</td>
<td>Obligation</td>
</tr>
<tr>
<td>is not required to</td>
<td>Exclusion</td>
<td>has a right to</td>
<td>Permission</td>
</tr>
<tr>
<td>may not</td>
<td>Obligation</td>
<td>may</td>
<td>Permission</td>
</tr>
<tr>
<td>may not require*</td>
<td>Obligation</td>
<td>may deny*</td>
<td>Permission</td>
</tr>
<tr>
<td>must</td>
<td>Obligation</td>
<td>may require*</td>
<td>Permission</td>
</tr>
</tbody>
</table>

*These patterns denote delegations.*
Frame-based Requirements
the tabular format

<table>
<thead>
<tr>
<th>Record Number: O-520.7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Property</td>
</tr>
<tr>
<td>Subject</td>
</tr>
<tr>
<td>Subject</td>
</tr>
<tr>
<td>Modality</td>
</tr>
<tr>
<td>Action</td>
</tr>
<tr>
<td>Object</td>
</tr>
<tr>
<td>Condition</td>
</tr>
</tbody>
</table>
Frame-based Markup

1) [#O [#s The covered entity & who has a direct treatment relationship with the individual] must…
   a) [#a Provide] [#o notice] [#c/1 no later than the first service delivery]];

2) For the purposes of paragraph (1), [#O [#c *1] [#s a covered entity & who delivers services electronically] must [#a provide] [#o electronic notice] [#e unless…]]

Markup provides...

- Improved traceability
- Operators for cut, copy and paste of legal phrases
IFIP WG2.9 Talk Outline

next: formalization

(1) Research Setup
- Problem and motivation
- Background
- Research design

(2) Acquisition
- Types of legal statements
- Identifying requirements
- Standard upper ontology
- Frame-based method

(3) Formalization
- Stakeholder/ Goal hierarchies
- Catalogue of constraints
- Priority hierarchies

(4) Specification
- Requirement metrics
- Refinement patterns
HIPAA §160.103: Covered entity means: a health plan, a health care clearinghouse and a health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.
Stakeholder Class Hierarchy – 2

multiple definitions and transitivity

- Stakeholders must satisfy all of the obligations in their classification hierarchy.

![Stakeholder Class Hierarchy Diagram]

- **Individual**
- **Personal Representative**
- **Covered Entity**
- **Correctional Institution**
- **Inmate**

- **Licensed Health Care Professional**
- **Health Plan**
- **Health Care Clearing House**
- **Health Care Provider**

- **Group Health Plan**
- **Health Insurance Issuer**
- **Health Maintenance Organization**
Goal Specialization Hierarchy – 1

- Show Description Logic formula
Under what constraints must a stakeholder provide what type of notice to whom?

- **O_{520.7}**
  - **(CE)**

- **O_{520.8}**
  - **(HP, to any person or individual)**

- **O_{520.13}**
  - **(CE, electronic notice)**

- **O_{520.14}**
  - **(CE, paper copy)**

- **O_{520.2}**
  - **(GHP, to any person)**

- **O_{520.15}**
  - **(CE, electronic notice, automatically)**

- **O_{520.4}**
  - **(GHP, to any person)**

(To Appear) 2009 ACM TOSEM
Catalogue of Constraints

- Identified over 300 information access requirements (legal uses and disclosures)

<table>
<thead>
<tr>
<th>Constraints on Information Access</th>
<th>Total</th>
</tr>
</thead>
<tbody>
<tr>
<td>Legal Determinations</td>
<td>231</td>
</tr>
<tr>
<td>Medical Determinations</td>
<td>184</td>
</tr>
<tr>
<td>Personal Beliefs</td>
<td>71</td>
</tr>
<tr>
<td>Contractual Statements</td>
<td>170</td>
</tr>
<tr>
<td>Data Subjects</td>
<td>42</td>
</tr>
<tr>
<td>Data Purposes</td>
<td>389</td>
</tr>
</tbody>
</table>
Beliefs, Determinations, Statements

constraints on use and disclosure

1. Constraints on the user, discloser or recipient
   a. (Beliefs) Who determines the consent of the individual is inferred from the circumstances.
   b. (Legal) Who has lawful custody of an inmate or individual.
   c. (Medical) Who determines the individual is incapacitated.

2. Constraints on data subjects
   a. About individuals who are Armed Forces personnel.

3. Constraints on data purposes
   a. (Explicit) For marketing.
   b. (Inferred) Which is compiled for use in a civil, criminal or administrative proceeding
HIPAA §164.512(f)(2): Except for disclosures required by law as permitted by paragraph 164.512(f)(1), a covered entity may disclose PHI in response to a law enforcement (LE) official's request for the purpose of identifying or locating a suspect.
Experimental Evaluation

- **Hypothesis**: The formal artifacts (stakeholder, priority hierarchies, etc.) improve requirements comprehension when deciding applicable jurisdiction.
IFIP WG2.9 Talk Outline

next: specification

(1) Research Setup
- Problem and motivation
- Background
- Research design

(2) Acquisition
- Types of legal statements
- Identifying requirements
- Standard upper ontology
- Frame-based method

(3) Formalization
- Stakeholder class hierarchies
- Goal specialization hierarchies
- Priority hierarchies

(4) Specification
- Requirement metrics
- Refinement patterns
Requirements Specification

identifying compliance gaps

- Compared 389 Cisco product requirements to 141 NCSU legal requirements

- In this study, a “gap” refers to both:
  - A mapping between a product requirement and a paragraph reference in a regulation
  - A difference in semantics between two requirements
Requirements Metrics

**statement metrics**

- **NCSU O-29**: PROVIDE textual information through operating system functions for displaying text.
- **Cisco SW-50.11 (M2)**: Draw text using the standard function calls
- **Cisco SW-50.11 (M3)**: Use standard functions to copy or erase text and graphics.

<table>
<thead>
<tr>
<th>Metric</th>
<th>A #</th>
<th>B #</th>
</tr>
</thead>
<tbody>
<tr>
<td>S-E (Equivalent)</td>
<td>NCSU O-29</td>
<td>Cisco-SW-50.11 (M2)</td>
</tr>
<tr>
<td>S-G (Goal)</td>
<td>NCSU O-29</td>
<td>Cisco SW-50.11 (M3)</td>
</tr>
</tbody>
</table>
Requirements Metrics

*phrase metrics*

- **NCSU O-29**: PROVIDE textual information through operating system functions for displaying text.

- **Cisco SW-50.11 (M2)**: Draw text using the standard function calls

<table>
<thead>
<tr>
<th>Metric</th>
<th><strong>NCSU O-29</strong></th>
<th><strong>Cisco SW-50.11 (M2)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>P-R</td>
<td>provide</td>
<td>draw</td>
</tr>
<tr>
<td>P-R</td>
<td>textual information</td>
<td>text</td>
</tr>
<tr>
<td>P-G</td>
<td>operating system functions for displaying text</td>
<td>standard function calls</td>
</tr>
</tbody>
</table>
Experimental Evaluation

- **Hypothesis**: What factors (domain knowledge, interests, etc.) influence agreement between analysts who apply the metrics?

- Are there strong correlations between applications of statement and phrase metrics?
Requirements Refinement Patterns

- A *refinement pattern* is a structure that an analyst applies to a legal requirement to yield a new legal, policy or product requirement.

Example patterns:
- Balancing rights and obligations
- Removing pre-conditions (simplification)
- Refine by refrainment (clarification)
- Broadly applying the regulatory goal (innovation)
Balancing Rights and Obligations

delegations, transactions, purposes

- The CE **requires** the individual to request an amendment in writing.
  - **(implied obligation)** The individual **must** request an amendment in writing.

- The individual **has a right to** receive notice.
  - **(implied obligation)** The CE **must** provide the notice.

- The CE **must** post the notice for the individual to read.
  - **(implied right)** The individual **has a right to** read the notice.

*Using formal models of rights and obligations, we can infer rights from obligations and vice versa.*
Removing Pre-conditions

simplifying compliance

- **NCSU O-73**: OPERATE telecommunications products, which have mechanically operated controls or keys, with one hand...

- **Cisco HW-10.11 (M1)**: All physical controls must be activated by one hand...
Refine by Refrainment
clarifying compliance

- **NCSU O-29**: PROVIDE textual information through operating system functions for displaying text
- **Cisco SW-50.11 (M4)**: Avoid directly manipulating bitmaps
- **Cisco SW-50.11 (M5)**: Avoid directly modifying the screen
Broadly Applying the Goal

innovating under the law

- **NCSU O-72**: Controls and keys shall be tactilely discernible without activating the controls or keys.

- **Legal Goal (implied by O-72)**: Provide methods for I/O that are discernable under limited sense and mobility.

- **Cisco SW-30.41 (O1)**: Design the default set of tones so that each tone is as distinct and intelligible as possible.

---

Diagram:

- Implied Goal
  - O-72
  - SW-30.41 (O1)
Related Work

- **Natural Language Requirements Analysis**
  [Goldin and Berry 1994; Overmyer et al. 2001; Cysneiros and Leite 2004; Wasson 2006]

- **Extracting Models from Regulations**
  [Kerrigan and Law 2003; May et al. 2005; Lee et al. 2006; Dinesh et al. 2006]

- **Goal-oriented Requirements Engineering**
  [Dardenne et al. 1993, Anton 1997; Potts et al. 2004, Breaux et al. 2005]

- **Frame-based representations**
  [Fillmore 1967; Misky 1975; Schank and Abelson 1977]
Feedback and Questions?

