

# The Role of Law in Software Requirements Engineering

Paul Otto

Advisor: Annie Antón  
CSC 890 Written Qualifier Exam

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

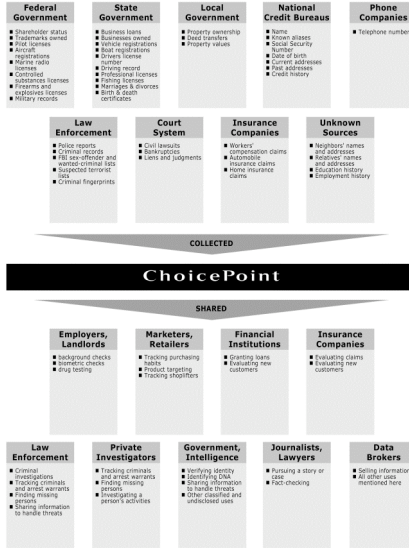
## Why should computer scientists study the law?

- Regulatory compliance is the primary driver of information security policy<sup>1</sup>
- The cost of non-compliance is high
  - HIPAA: civil money penalty up to \$25K per violation<sup>2</sup>
  - FCRA: ChoicePoint fined a civil penalty of \$10M and \$5M consumer redress fund<sup>3</sup>
- Regulations dictate many aspects of software and system requirements

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

# ChoicePoint Data Flows<sup>3</sup>

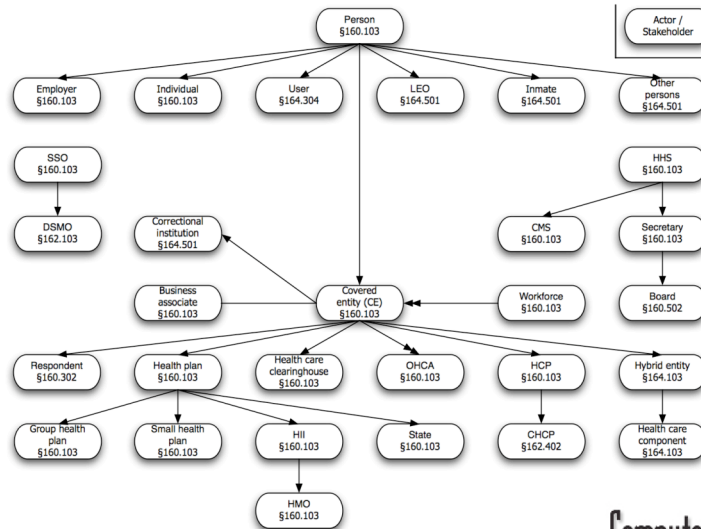


©2007 Paul Otto et al.



3

# HIPAA stakeholder hierarchy



©2007 Paul Otto et al.



4

## How regulations impact requirements engineering

- Elicitation: determining the stakeholders and requirements
  - Regulatory texts specify requirements that need to be incorporated into system development
  - Stakeholders require answers to specific queries about what is allowed or not allowed<sup>4,5</sup>
- Analysis: resolving ambiguities, contradictions, omissions
- Traceability: documenting and tracking requirements
  - Monitoring software systems for compliance with requirements and policies identified as a challenging and important problem<sup>6</sup>

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

5

## What is required for legal compliance?

- Traditional software engineering activities:
  - Analysis
  - Modeling
  - Development
- Traditional security activities:
  - Policy enforcement
  - Auditing

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

6

## Overview

- Why regulations are relevant to computer scientists
- **The nature of regulations**
- Survey of past work with regulations
- Requirements for handling regulations
- Discussion and future work

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

7

## Key characteristics of regulatory texts

- Factors that make regulations difficult to model and use in development:
  - Overlapping, contradictory hierarchies
  - Frequent amendments and revisions
  - Cross-references: internal and external
  - Definitions and acronyms
  - Case law and supplemental documents
  - Ambiguities: intentional and unintentional

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

8

## The influence of supplemental documents

- HIPAA: 90 pages in the Code of Federal Regulations
  - Privacy Rule: 55 pages
  - Security Standards: 16 pages
- U.S. Department of Health and Human Services publishes supplemental documents
  - Summary of the HIPAA Privacy Rule: 25 pages
  - Guidance for HIPAA Security Standards: 7 pages
- Numerous unofficial guides available online - third parties providing HIPAA interpretations
- **Software engineers currently rely on these texts and may never reference original regulations!**

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

9

## Examples of legal ambiguity

- Intentional ambiguity: HIPAA §164.306(a)(2)  
“Protect against any **reasonably** anticipated threats or hazards to the security or integrity of such information”
- Language ambiguity: HIPAA §164.530(i)(3)  
“...the covered entity must **promptly** document **and** implement the revised policy or procedure”

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

10

## Overview

- Why regulations are relevant to computer scientists
- The nature of regulations
- **Survey of past work with regulations**
- Requirements for handling regulations
- Discussion and future work

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

11

## Survey methodology

- Searched literature for papers involving some combination of compliance, modeling regulations, privacy, security, requirements
  - Discovered and read over 150 relevant papers
  - Cited 41 papers in CSC 890 written examination
- My methodology:
  1. Identified main contributions in papers
  2. Consolidated criticisms and observations regarding the difficulty of working with legal texts
  3. Extracted common themes in handling regulatory texts and supporting compliance efforts
  4. Classified each approach based on primary implementation
  5. Analyzed the pros and cons of each approach

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

12

## Previous work in modeling and using regulations

- Logic Based Approaches
  - Symbolic logic
  - Logic Programming (Expert Systems)
  - Deontic Logic
  - Defeasible Logic
  - First-Order Temporal Logic
- Software Engineering Approaches
  - Access Control
  - Markup-based Representations
  - Goal Modeling
  - Reusable Requirements Catalog

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

13

## Symbolic Logic

Elicitation	<b>Analysis</b>	Traceability	Enforcement	Auditing
-------------	-----------------	--------------	-------------	----------

- One of the first efforts in modeling regulations
- Main idea: translate natural language into logical statements<sup>7</sup>
- Pros:
  - Eliminates unintended ambiguities
  - Provides machine-readable representations
- Cons:
  - Does not leverage computers for data processing
  - Requires manually encoding N.L. to logic
  - Not designed to aid software engineers

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

14

# Logic Programming

Elicitation

Analysis

Traceability

Enforcement

Auditing

- Main idea: represent and utilize legal knowledge through an expert system
- Many research efforts undertaken (e.g. representing the U.S. Internal Revenue Code in Prolog<sup>8</sup>)
- Pros:
  - Identifies unintended ambiguities
  - Supports queries on the regulatory text
- Cons:
  - Many projects, yet no fully working systems
  - Requires manually encoding natural language to logic

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

15

# Deontic Logic

Elicitation

Analysis

Traceability

Enforcement

Auditing

- Main idea: capture the rights and obligations present in legal texts
- Pros:
  - Answers specific queries
  - Supports development and requirement monitoring<sup>9</sup>
  - Maintains traceability<sup>9</sup>
- Cons:
  - Limited implementation efforts to date
  - Requires manually encoding rights and obligations
  - Only capturing subset of legal requirements

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

16

## Defeasible Logic

Elicitation

**Analysis**

Traceability

Enforcement

**Auditing**

- Main idea: strict rules, defeasible rules, and defeaters used to represent legal texts
- Rights and obligations are just two of the eight fundamental legal conceptions<sup>10</sup>
- Pros:
  - Accommodates hierarchical, conflicting nature of regulations
  - Supports legal reasoning and queries
- Cons:
  - High computational complexity
  - Requires numerous enhancements to represent various aspects of legal texts (e.g. arithmetic and temporal operators)

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

17

## First-Order Temporal Logic

Elicitation

**Analysis**

Traceability

Enforcement

**Auditing**

- Main idea: extract and represent certain key concepts (e.g. context, roles, type of info)<sup>11</sup>
- Based on contextual integrity framework, which is a narrow conceptualization of privacy<sup>12</sup>
- Pros:
  - Captures most privacy elements of the law
  - Supports compliance checks between specific regulations and organizational privacy policies
- Cons:
  - Limited applicability - only privacy regulations

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

18

# Access Control

Elicitation	Analysis	Traceability	Enforcement	Auditing
-------------	----------	--------------	-------------	----------

- Main idea: derive privacy-focused access control rules directly from regulatory text
- Provides an auditable privacy system<sup>13</sup>
- Pros:
  - Enables formal model checking
  - Supports queries
  - Traceability support
- Cons:
  - Abstracts away many key details of legal texts (e.g. assuming external and ambiguous references satisfied by default)
  - Omits many low-level system requirements specified by law
  - Largely focused on rights and obligations

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

19

# Markup-Based Representations

Elicitation	Analysis	Traceability	Enforcement	Auditing
-------------	----------	--------------	-------------	----------

- Main idea: mimic nature of regulations by encoding in semi-structured markup languages (e.g. XML)
- REGNET: major research effort to support compliance efforts through an XML framework<sup>14</sup>
- Pros:
  - Supports locating and analyzing regulatory texts
  - Automatically converts legal texts to XML
  - Provides semi-automatic generation of metadata
  - Traceability support
- Cons:
  - Only applied to limited domain areas
  - No working systems available

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

20

# Goal Modeling

Elicitation

Analysis

Traceability

Enforcement

Auditing

- Main idea: extract goals, soft goals, tasks, resources, and social relationships from regulatory text
- SecureTropos used to model the relationships between actors, trust, delegation<sup>15</sup>
- Italian Data Protection Act used as proof of concept
- Pros:
  - Supports requirements engineering activities
  - Identifies relationships between stakeholders
- Cons:
  - Requires manually extracting elements from law
  - No support for queries

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

21

# Reusable Requirements Catalog

Elicitation

Analysis

Traceability

Enforcement

Auditing

- Main idea: analysts extract legal requirements once, then reuse in future projects<sup>16</sup>
- Spanish Personal Data Protection Act is legal testbed
- Pros:
  - Identifies unintended ambiguities through process of mining for requirements
  - Quality of the catalog improves with each usage
- Cons:
  - Requires manually extracting requirements from law
  - No evaluation of time spent or requirements coverage
  - Would require manual updates each time the law changed

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

22

# Overview

- Why regulations are relevant to computer scientists
- The nature of regulations
- Survey of past work with regulations
- **Requirements for handling regulations**
- **Discussion and future work**

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

23

# Requirements for systems handling regulations

- Requirements Elicitation
  1. **Identification of Relevant Regulations**
  2. **Classification of Regulations with Metadata**
  3. Management of Evolving Regulations and Law
    - Antón extensively evaluated requirements evolution<sup>17</sup>
- Supporting Traceability
  4. Traceability between References and Requirements
    - Active RE research topic for 15 years - still an unsolved problem!
  5. Data Dictionary and Glossary to Ensure Consistency
    - Active RE research area, but not applied to regulatory domain
- Requirements Analysis
  6. Prioritization of Regulations and Exceptions
    - Breaux and Antón looked at handling exceptions<sup>9</sup>
  7. **Disambiguation of Regulatory Statements**

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

24

## Limitations and future work

- Only surveyed research within computer science and artificial intelligence domains - compliance is a broader engineering problem
- Did not consider research into natural language processing in general
- Need to consider how system developers currently handle legal texts
- Study how regulations are structured and how requirements can be extracted

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

25

## Upcoming research to evaluate legal compliance

- iTrust: existing system with fully documented requirements specification, use cases, and source code
  - Develop tests for HIPAA compliance
  - Establish traceability between requirements specification and regulatory text
  - Evaluate preliminary ideas for a legal compliance system
- Discussions with health care organizations
  - Determine current processes for HIPAA compliance
  - Evaluate user requirements for working with regulations and organizational policies

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

26

## References

1. Ernst & Young. "2006 Global Information Security Survey," November 2006.
2. Code for Federal Regulations, "Amount of a civil money penalty," Title 45, Subtitle A, §160.404, last updated October 2006.
3. P.N. Otto, A.I. Antón, D.L. Baumer. "The ChoicePoint Dilemma: How Data Brokers Should Handle the Privacy of Personal Information," Technical Report TR-2006-18, July 2006.
4. G. Antoniou, D. Billington, M.J. Maher. "On the Analysis of Regulations using Defeasible Rules," Proc. of the 32nd Hawaii Int'l Conf. on Sys. Sci., pp. 1-7, January 1999.
5. M.-F. Moens. "Combining Structured and Unstructured Information in a Retrieval Model for Accessing Legislation," Proc. of the 10th Int'l Conf. on AI and Law, pp. 141-145, June 2005.
6. W.N. Robinson. "Implementing Rule-Based Monitors within a Framework for Continuous Requirements Monitoring," Proc. of the 38th Hawaii Int'l Conf. on Sys Sci., January 2005.
7. L.E. Allen. "Symbolic Logic: A Razor-Edged Tool for Drafting and Interpreting Legal Documents," Yale Law Journal 66(6), pp. 833-879, May 1957.
8. L.T. McCarty. "The TAXMAN Project: Towards a Cognitive Theory of Legal Argument," *Computer Science and Law*, B. Niblett Ed., Cambridge Press: New York, pp. 23-43, June 1980.
9. T.D. Breaux, M.W. Vail, A.I. Antón. "Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations," Proc. of the 13th IEEE Int'l Conf. on Req'ts Eng., September 2006.
10. W.N. Hohfeld. "Some Fundamental Legal Conceptions as Applied in Judicial Reasoning," Yale Law Journal 23(1), pp. 16-59, November 1913.
11. A. Barth et al. "Privacy and Contextual Integrity: Framework and Applications," Proc. of the 2006 IEEE Symp. on Security and Privacy, May 2006.
12. H. Nissenbaum. "Privacy as Contextual Integrity," Washington Law Review 79(1), pp. 119-157, February 2004.
13. M.J. May, C.A. Gunter, I. Lee. "Privacy APIs: Access Control Techniques to Analyze and Verify Legal Privacy Policies," Proc. of the 19th Computer Security Foundations Workshop, July 2006.
14. S. Kerrigan, K.H. Law. "Logic-Based Regulation Compliance-Assistance," Proc. of the 9th Int'l Conf. on AI and Law, pp. 126-135, June 2003.
15. F. Massacci, M. Prest, N. Zannone. "Using a Security Requirements Engineering Methodology in Practice: The compliance with the Italian Data Protection Legislation," Technical Report DIT-04-103, 2004.
16. A. Toval, A. Olmos, M. Piattini. "Legal Requirements Reuse: A Critical Success Factor for Requirements Quality and Personal Data Protection," Proc. Of the IEEE Joint Int'l Conf. on Req'ts Eng., pp. 95-103, September 2002.
17. A.I. Antón, C. Potts. "Functional Paleontology: The Evolution of User-Visible System Services," IEEE Transactions on Software Engineering, 29(2), pp. 151-166, February 2003.

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

27

## Thank you!

- Thanks to Dr. Antón for her guidance
- Work supported by NSF Cyber Trust grant #0430166

©2007 Paul Otto et al.

Computer Science  
NC STATE UNIVERSITY

28