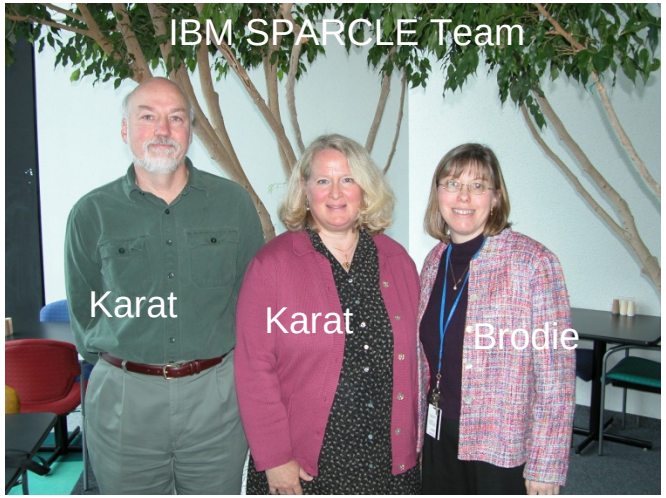
Policy Authoring

Matthew Dunlop

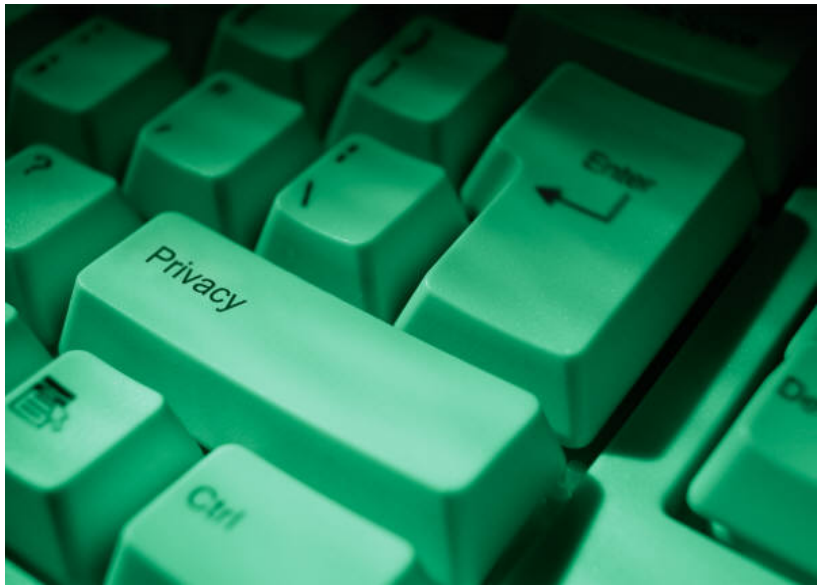
Policy Authoring

- Usable Security and Privacy: A Case Study of Developing Privacy Management Tools (2005)
- An Empirical Study of Natural Language Parsing of Privacy Policy Using the SPARCLE Policy Workbench (2006)



What is privacy?

- The right of an individual to control information about themselves



Do people care about privacy?

- In 1999, 78% of people surveyed refused to provide personal information due to concern of misuse
- In 2000, 50% of people surveyed routinely provide false personal information
- In 2004, 94% of people surveyed believe the benefit gained does not outweigh the cost of sharing personal information

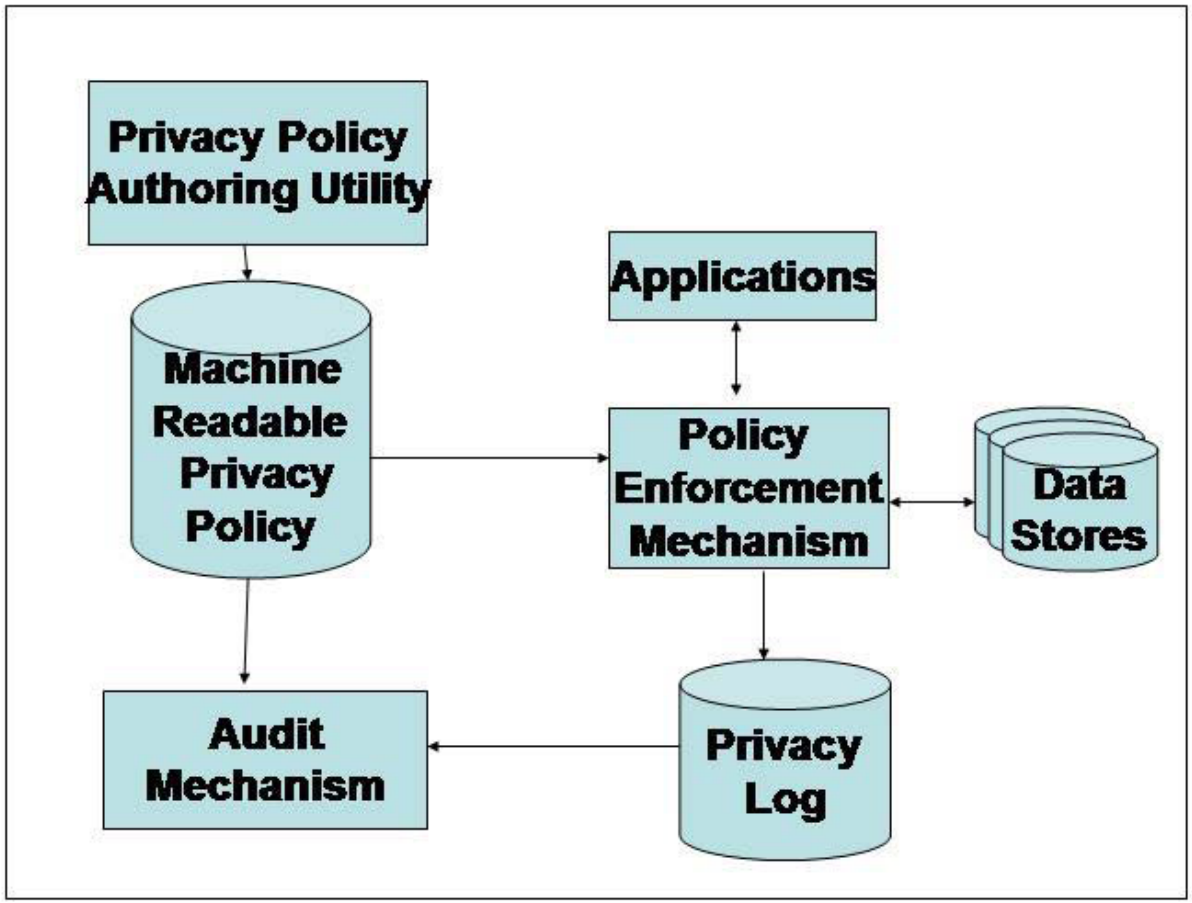
Objectives

- Identify organizational privacy requirements
- Identify approaches that address privacy requirements
- **Design and validate a prototype for flexible and simple privacy policy creation**

Key privacy design concepts

1. One integrated solution for an organization
2. Privacy functionality separated from application code
3. Support an appropriate level of granularity
4. Work with both structured and unstructured information
5. Simple and flexible privacy functionality

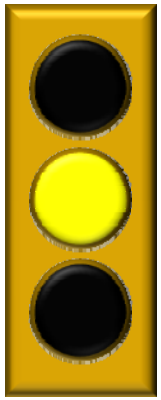
Abstract privacy architecture



Integrated solution techniques

- Creation of a common set of privacy utilities

- Creation of a single system that acts as a personal information “vault”



Not Met Yet

Separated functionality techniques & techniques for maintaining granularity

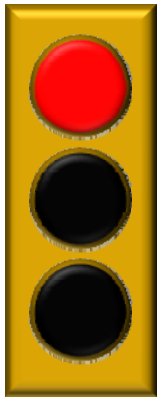
- Hippocratic database

- Tivoli Privacy Manager

Met

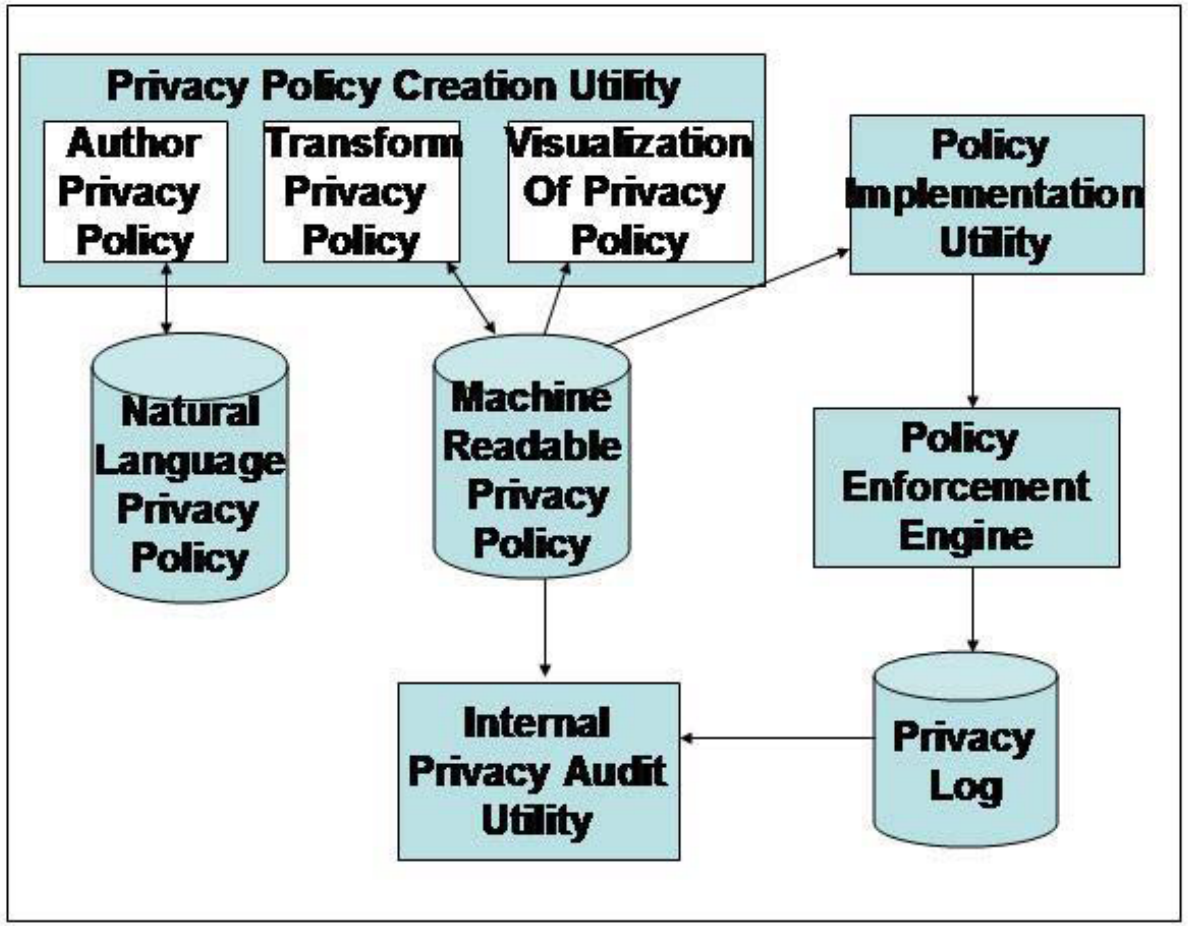
Structured/unstructured info handling & simple and flexible functionality

- No approaches exist



Not Met

Expanded abstract privacy architecture

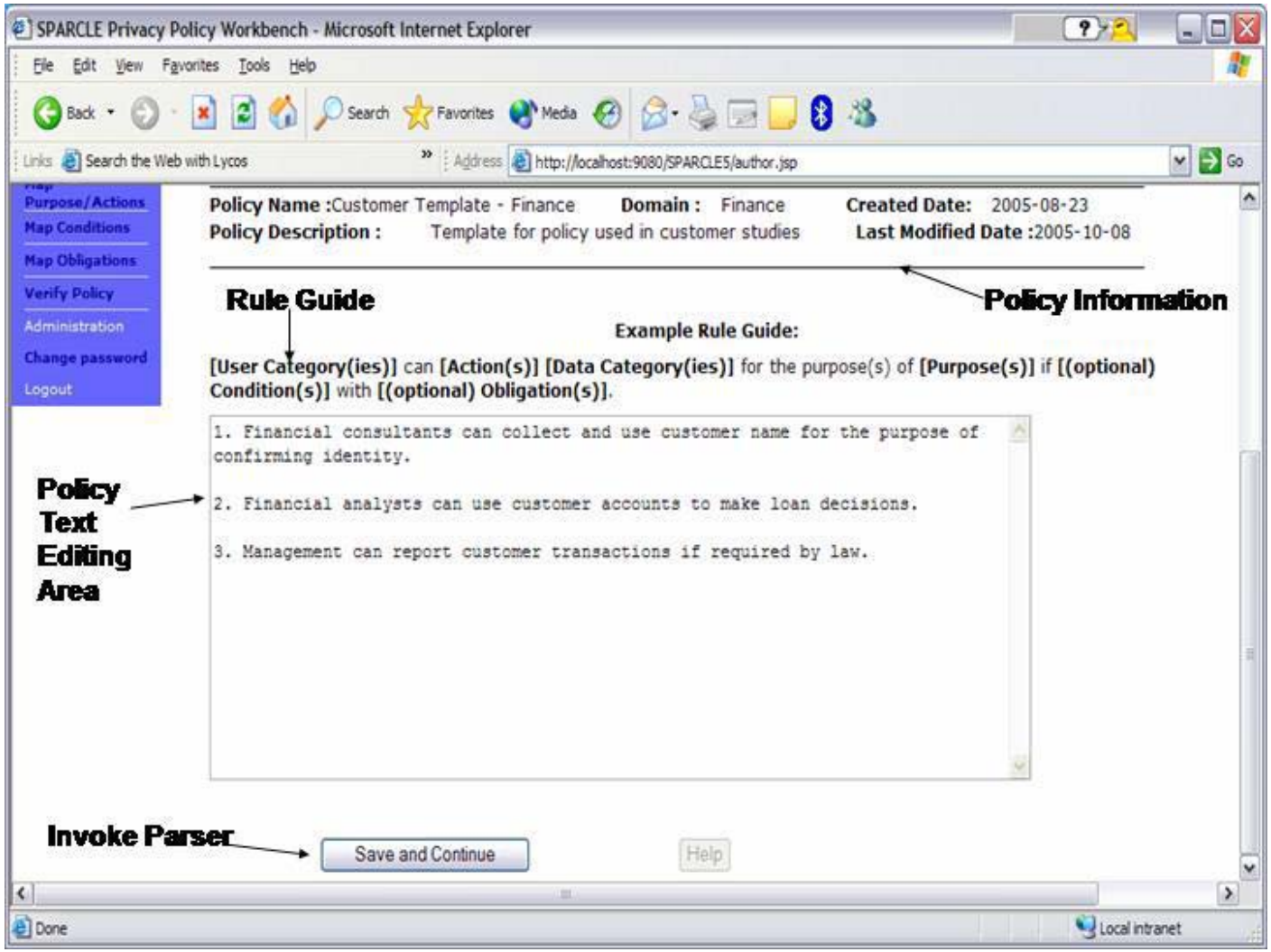


SPARCLE

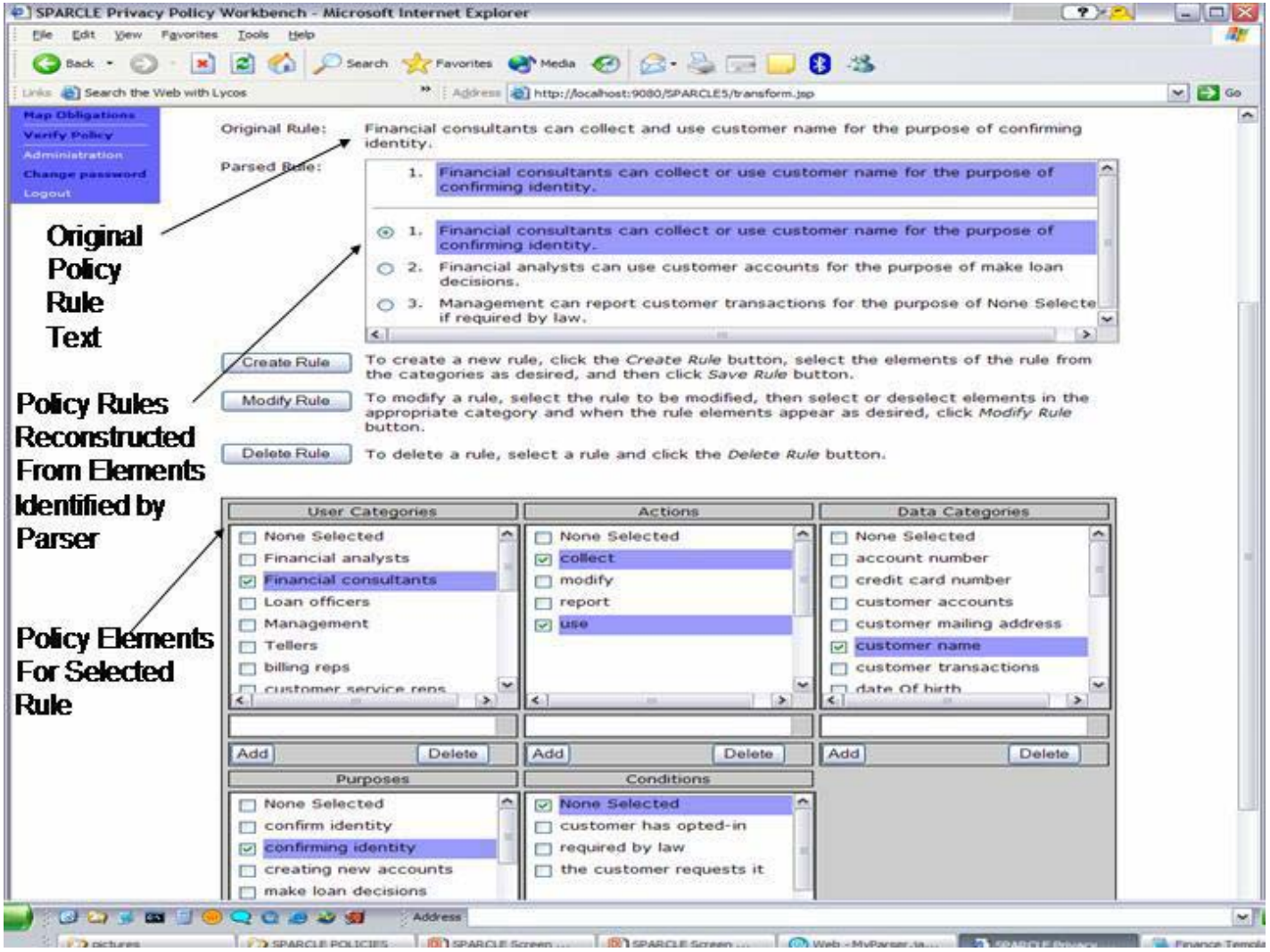
- **S**erver **P**rivacy **AR**chitecture and **C**apabi**L**ity **E**nablement

- Goals
  - Create understandable privacy policies
  - Link written privacy policies with their implementation
  - Monitor enforcement of policies

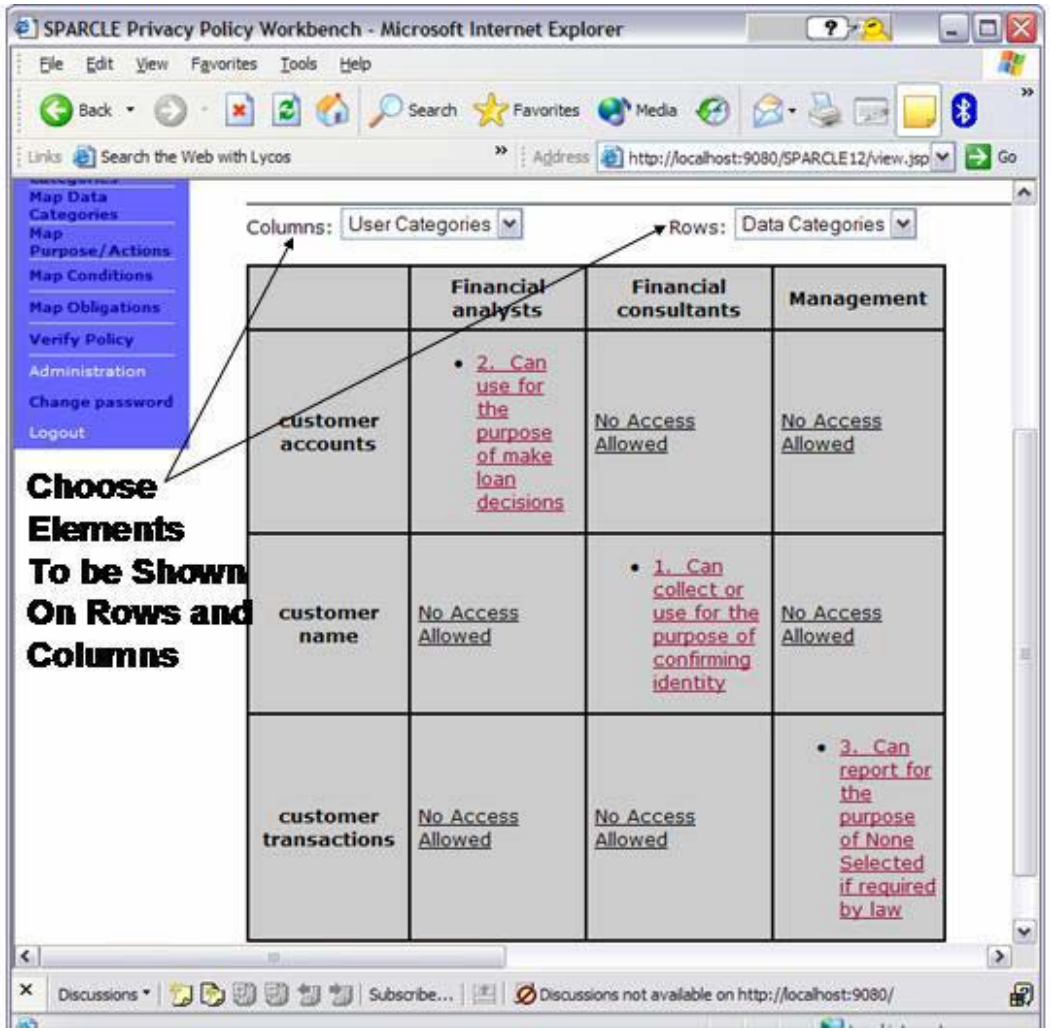
Natural language policy creation



Structured policy creation



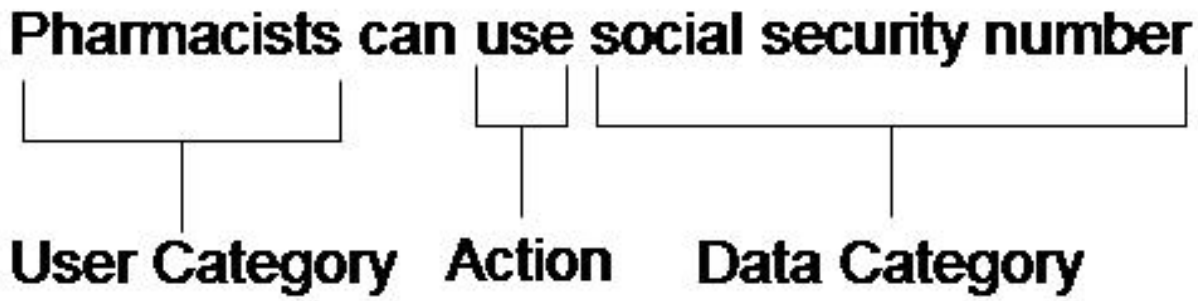
Viewing privacy policy rules

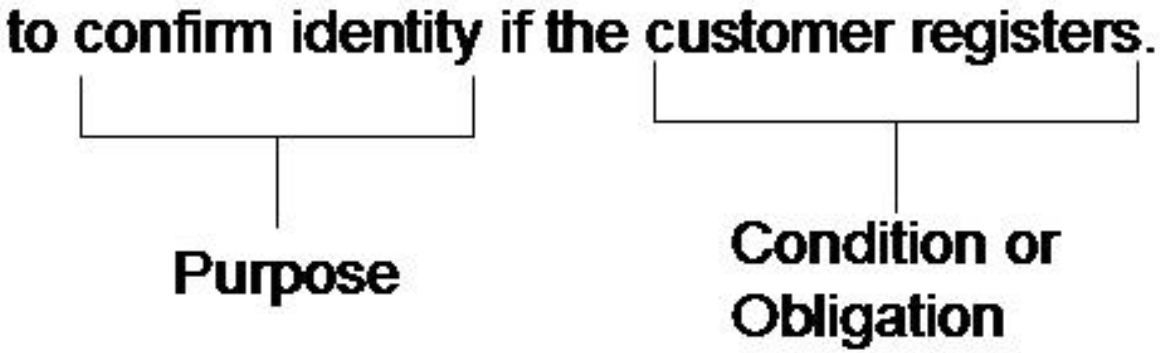


Natural language parsing

- Uses a shallow parser
  - Identify syntactic structures (e.g. nouns, verbs)
  - Use grammars to choose desired text based on speech patterns
- SPARCLE defines five grammars
  - User categories
  - Actions
  - data categories
  - Purposes
  - Conditions/obligations

Natural language parsing example





Parsing Accuracy

- Conservative
  - 86% precision
  - 88% recall
- Liberal
  - 95% precision
  - 97% recall

Prototype testing

- Initial 2004 tests of SPARCLE were favorable
  - High to very high on their seven point scale

- Improvements after testing:
  - Import pre-existing privacy policies
  - Use privacy policy templates as a starting point
  - Improved readability of the table view

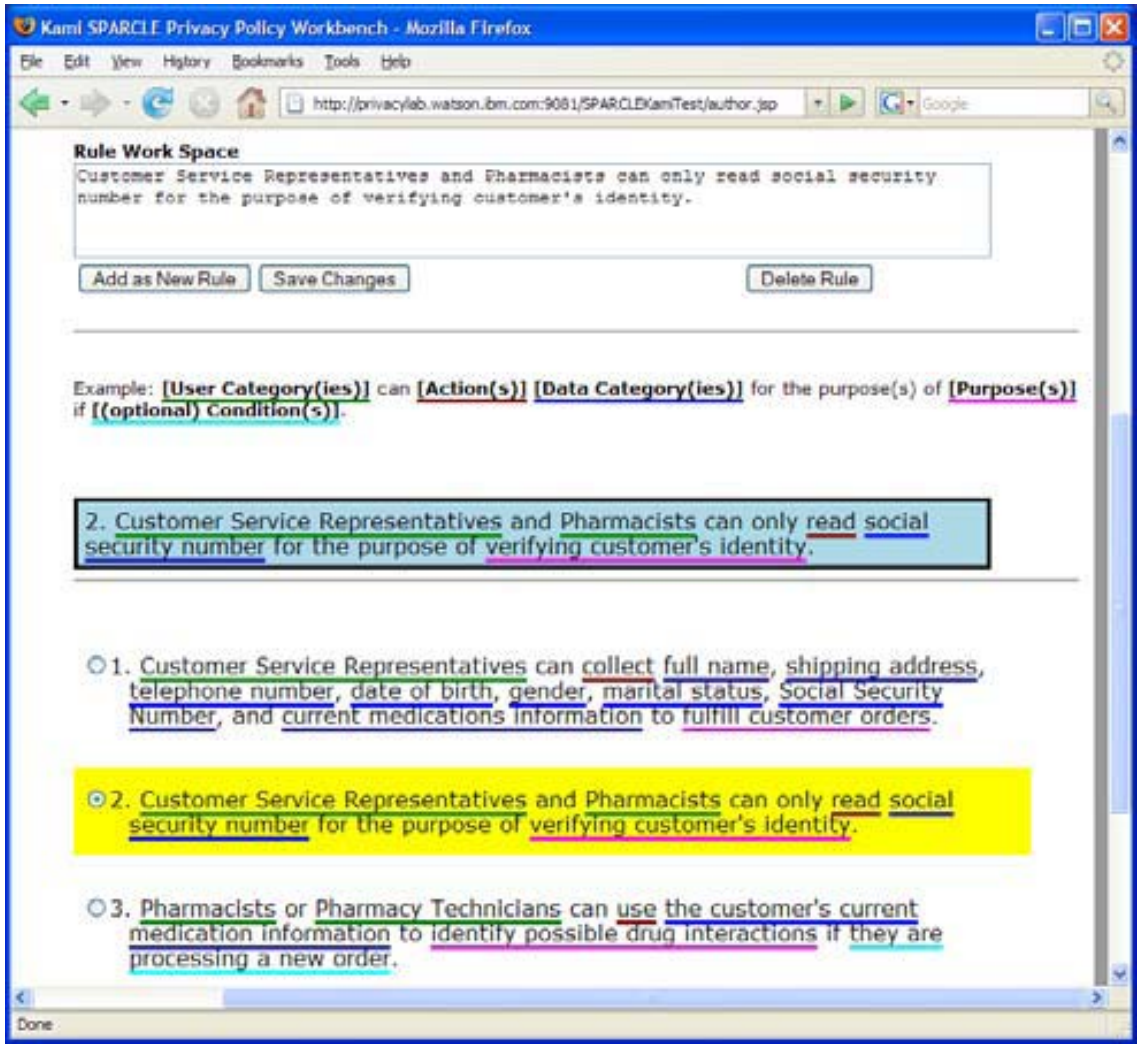
Implementation testing

- 2005 implementation tests were mostly favorable
  - High to very high on their seven point scale
- Participants were less favorable about pre-processing time
  - Desire for “no additional work” before inputting rules
  - Need better language parser

Subsequent Improvements

- In 2008, the authors looked at assisting policy authors in writing policies
  - "Evaluating assistance of natural language policy authoring" (SOUPS 2008)
- No improvement was made to the language parser
- Hypothesized that syntax highlighting would improve authoring

New Authoring Page



Why syntax highlighting failed

- Immediate feedback caused users to stop mid-process to correct mistakes
  - Interrupted verbalization
  - Interrupted recording of ideas
- Recommended fix
  - Move syntax highlighting to the translation page

Summary

Good	Improve
Improves on P3P by guaranteeing policy enforcement Provides interface usable by both IT and non-IT professionals Good policy visualization	Accuracy of policy parsing Preprocessing time No results on accuracy of machine-translated policies and preventing or granting access

Discussion

- Will the overhead of designing policies using SPARCLE discourage its adoption?
- Will organizations want privacy policies with guaranteed enforcement?
- Is 86-88% policy translation accuracy okay?
- What about policies that can't be defined within the context of SPARCLE?