
Policy Authoring



Matthew Dunlop

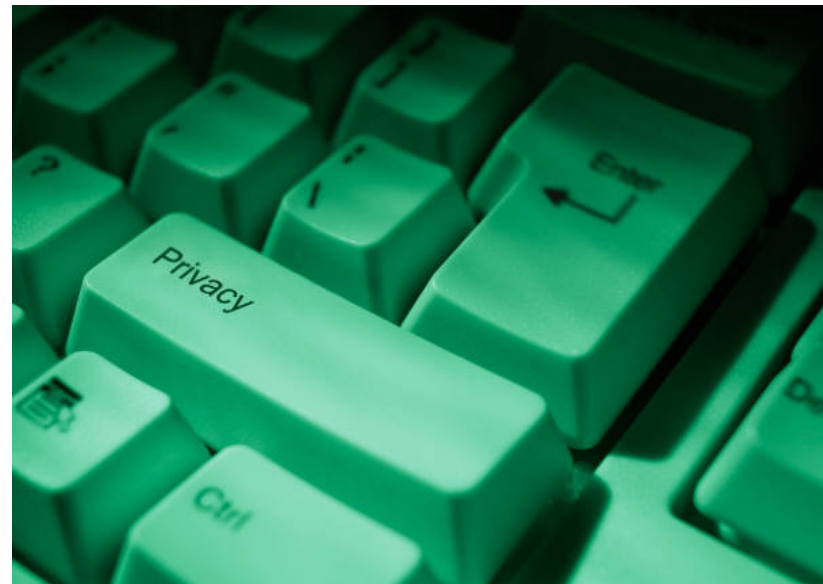
Policy Authoring

- 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

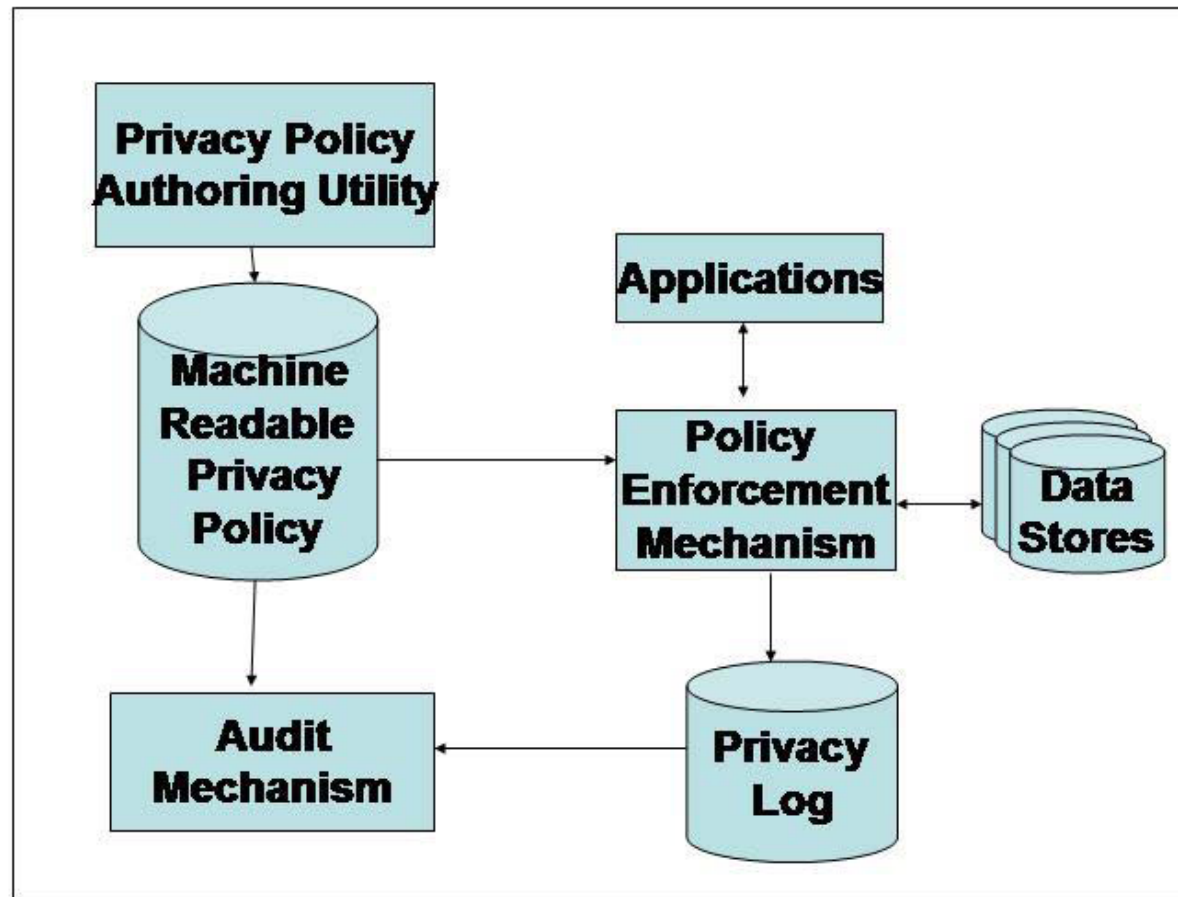
Objectives

- 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

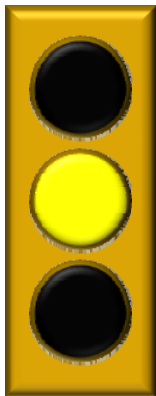
1. One integrated solution for an organization
2. Privacy functionality separated from application code
3. Support an appropriate level of granularity
4. Work with both structured and unstructured information
5. Simple and flexible privacy functionality

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

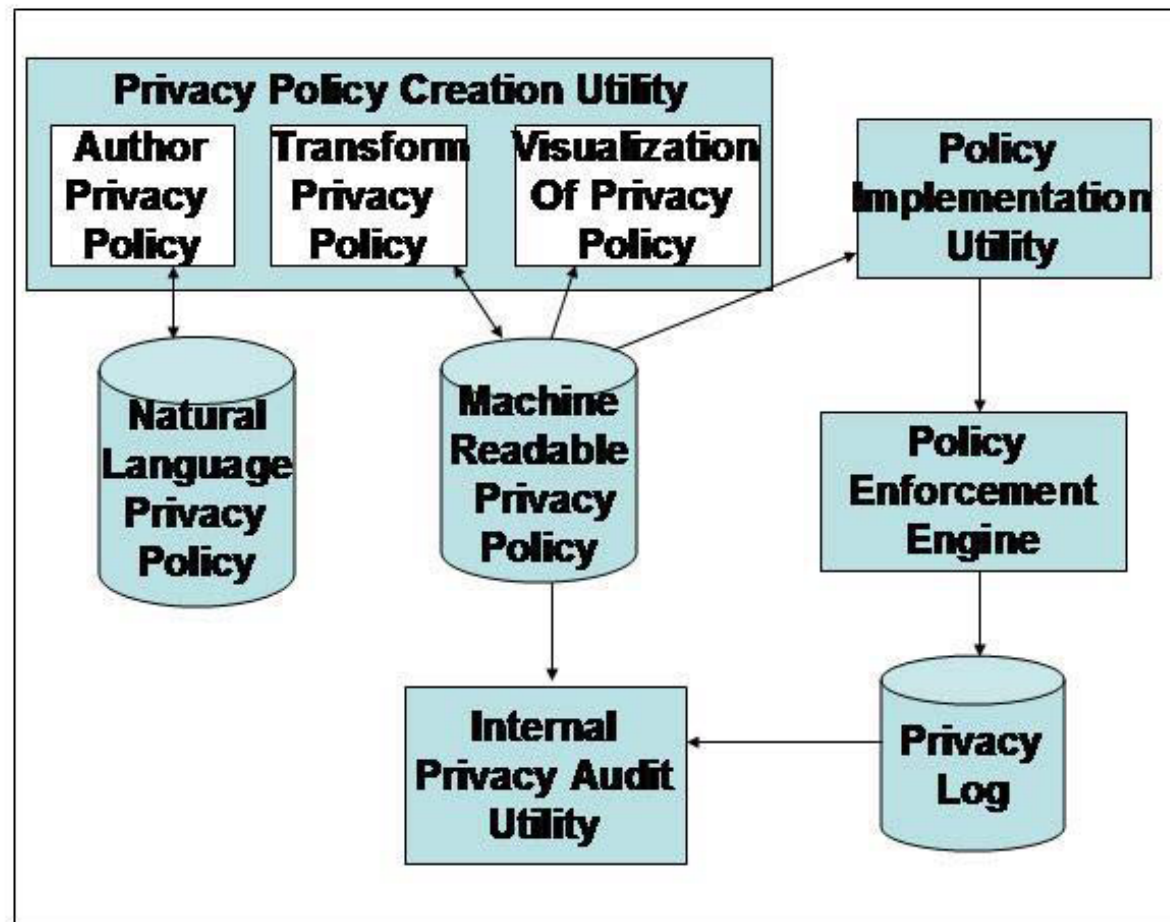
Structured/unstructured info handling & simple and flexible functionality

- 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

SPARCLE Privacy Policy Workbench - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Home Search Favorites Media Bluetooth

Links Search the Web with Lycos Address http://localhost:9080/SPARCLES/author.jsp Go

Policy Information

Policy Name : Customer Template - Finance Domain : Finance Created Date: 2005-08-23
Policy Description : Template for policy used in customer studies Last Modified Date :2005-10-08

Rule Guide

Example Rule Guide:

[User Category(ies)] can [Action(s)] [Data Category(ies)] for the purpose(s) of [Purpose(s)] if [(optional) Condition(s)] with [(optional) Obligation(s)].

1. Financial consultants can collect and use customer name for the purpose of confirming identity.

2. Financial analysts can use customer accounts to make loan decisions.

3. Management can report customer transactions if required by law.

Policy Text Editing Area

Invoke Parser

Save and Continue Help

Done Local Intranet

Structured policy creation

The screenshot displays the SPARCLE Privacy Policy Workbench in a Microsoft Internet Explorer browser window. The interface is divided into several sections:

- Navigation Panel (Left):** Includes links for "Map Obligations", "Verify Policy", "Administration", "Change password", and "Logout".
- Original Rule Text:** Shows the "Original Rule:" as "Financial consultants can collect and use customer name for the purpose of confirming identity." and the "Parsed Rule:" as a list of three items:
 1. Financial consultants can collect or use customer name for the purpose of confirming identity.
 2. Financial analysts can use customer accounts for the purpose of make loan decisions.
 3. Management can report customer transactions for the purpose of None Selecte if required by law.
- Policy Rules Reconstructed From Elements Identified by Parser:** A list of instructions for managing rules:
 - Create Rule:** To create a new rule, click the *Create Rule* button, select the elements of the rule from the categories as desired, and then click *Save Rule* button.
 - Modify Rule:** To modify a rule, select the rule to be modified, then select or deselect elements in the appropriate category and when the rule elements appear as desired, click *Modify Rule* button.
 - Delete Rule:** To delete a rule, select a rule and click the *Delete Rule* button.
- Policy Elements For Selected Rule:** A grid of selection boxes for rule components:
 - User Categories:** Includes "Financial consultants" (checked).
 - Actions:** Includes "collect" and "use" (checked).
 - Data Categories:** Includes "customer name" (checked).
 - Purposes:** Includes "confirming identity" (checked).
 - Conditions:** Includes "None Selected" (checked).

Viewing privacy policy rules

The screenshot shows the SPARCLE Privacy Policy Workbench interface. The main content is a table with columns for User Categories and rows for Data Categories. The table is filtered to show 'Financial analysts', 'Financial consultants', and 'Management' for columns, and 'customer accounts', 'customer name', and 'customer transactions' for rows. The table cells contain access rules and permissions.

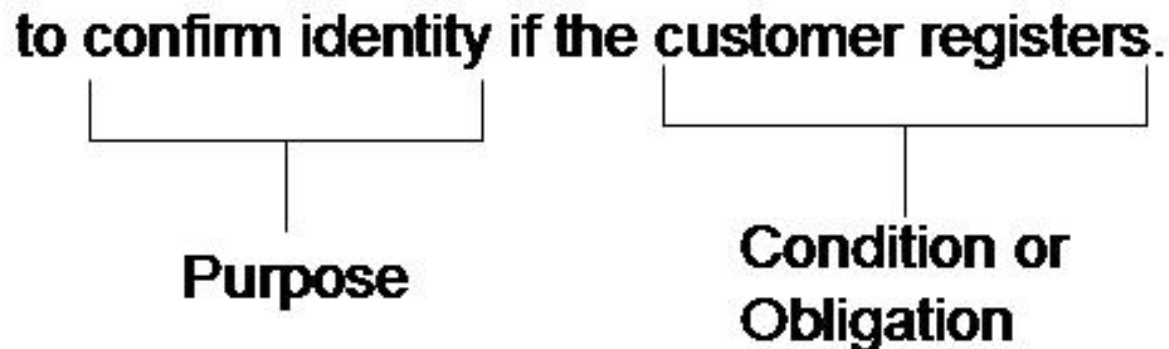
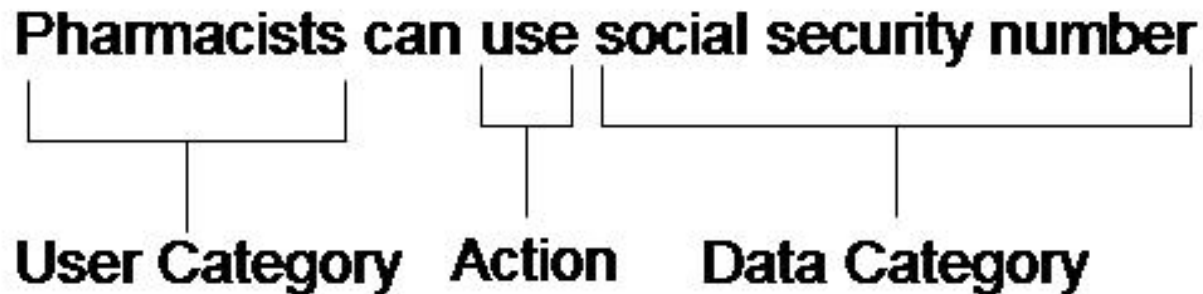
Choose Elements To be Shown On Rows and Columns

	Financial analysts	Financial consultants	Management
customer accounts	<ul style="list-style-type: none">2. Can use for the purpose of make loan decisions	No Access Allowed	No Access Allowed
customer name	No Access Allowed	<ul style="list-style-type: none">1. Can collect or use for the purpose of confirming identity	No Access Allowed
customer transactions	No Access Allowed	No Access Allowed	<ul style="list-style-type: none">3. Can report for the purpose of None Selected if required by law

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

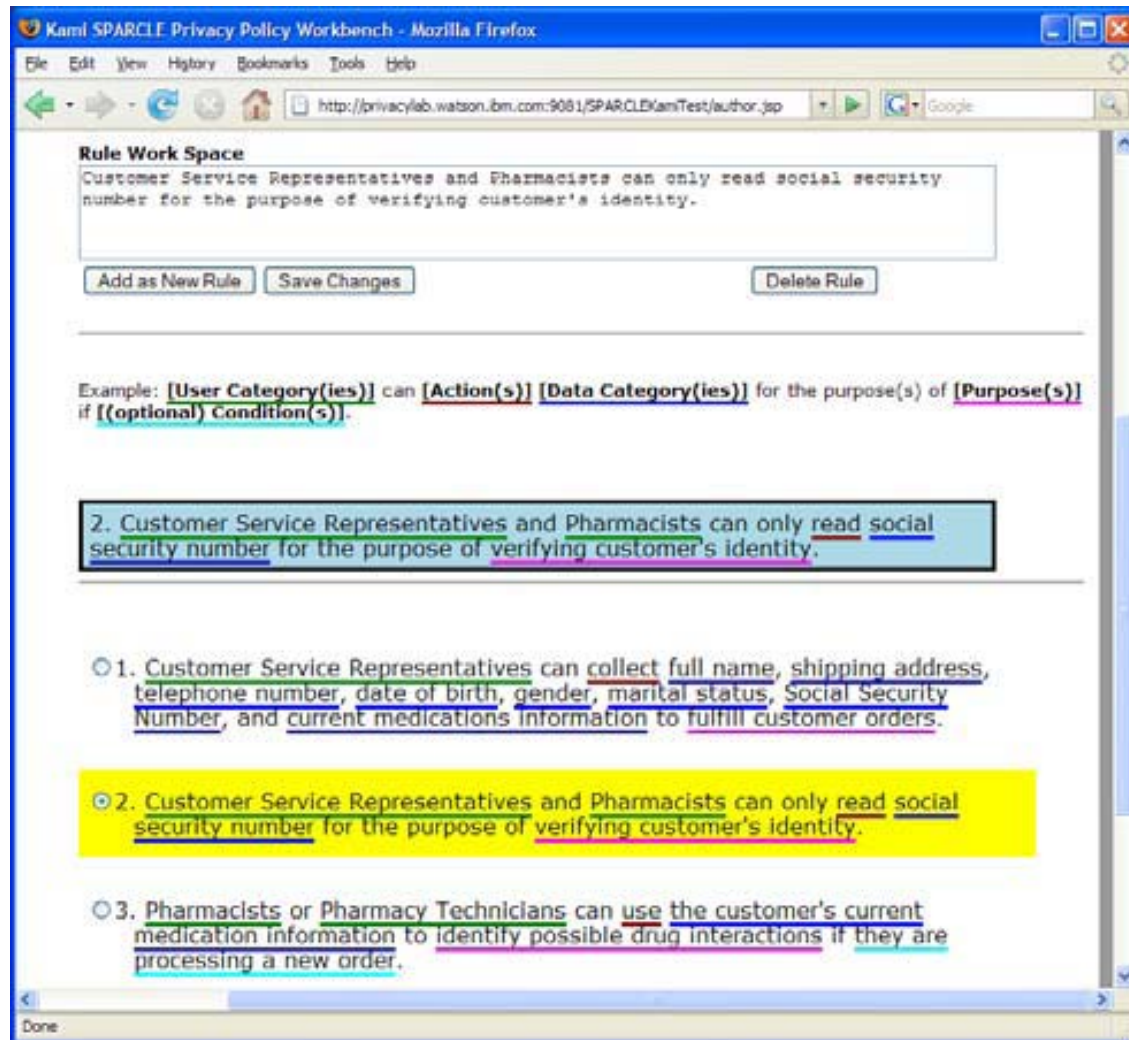
Implementation testing

- 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

- Improves on P3P by guaranteeing policy enforcement
- Provides interface usable by both IT and non-IT professionals
- Good policy visualization

Improve

- 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?