

Privacy Impact and Risk Assessment at Design-Time



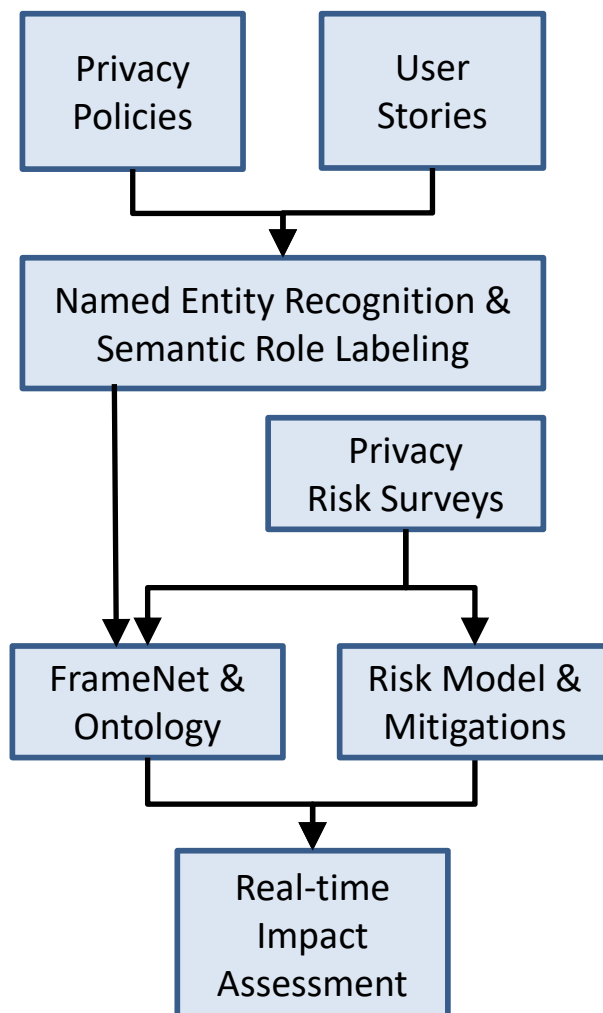
Challenge:

Privacy Impact Assessments are:

- Bolted onto / Disconnected from software process
 - Driven by legal, not deeper technical concerns
 - Performed too late to affect substantive design change
-

Solution:

- Respond to artifact changes in real-time to predict risk before design changes are fixed
- Combines natural language processing, psychometric surveys into developer-guiding tools to focus design effort



Scientific Impact:

- Generate traceable, design-time alignment of privacy risk with story-based design decisions
 - Expand our privacy vocabulary beyond policy analysis to predict when requirements (user stories) raise quantitative privacy concerns of varying risk levels
-

Broader Impact and Broader Participation:

- Extends privacy analysis to cover vulnerable demographic groups based on age, gender, income and education level
- Advances public policy with new developer tools to support privacy
- Supports mentorship of women and advances in course design

Award Number: 2007298; PI: Travis Breaux;
Organization: Carnegie-Mellon University