IBM TJ Watson Research Center

Making Privacy Possible: Research on Organizational Privacy Technology

Clare-Marie Karat, Carolyn Brodie, and John Karat
ckarat,brodiec,jkarat@us.ibm.com
Privacy Enabling Technology Research
Security, Networking and Privacy (SNAP)

Privacy Research Statement

- Most organizations store personal information (PI) data in heterogeneous server system environments.
- Currently they do not have a unified way of defining or implementing a privacy policy that encompasses both web and legacy applications across the different server platforms.
- This makes the management of PI data difficult for both enterprises and end users.

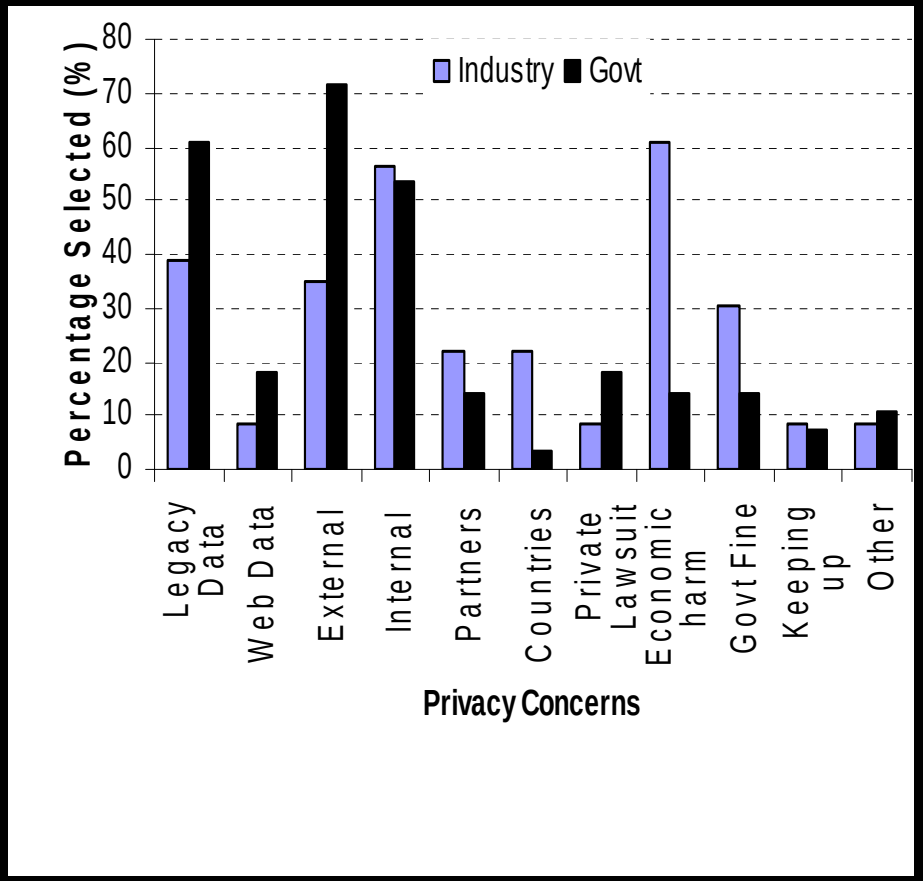
Progress to Date

- **Identified Organizational Needs – Initial survey (51 participants) asking about "top privacy concerns and technology needs"**
- **Established Scenarios - In-Depth follow up (13 participants) to identify data flow and architectural concepts for privacy technology (e.g., sticky policy)**
- **Iterated on Designs - Scenario-based walkthrough sessions of the privacy management prototype (SPARCLE) with target users (2 design iterations, 22 participants)**
- **Conducted Evaluations - Laboratory study examining methods for policy authoring (36 participants)**
- **Developed Architecture - Ongoing technical feasibility analysis**

Identify Organizational Needs

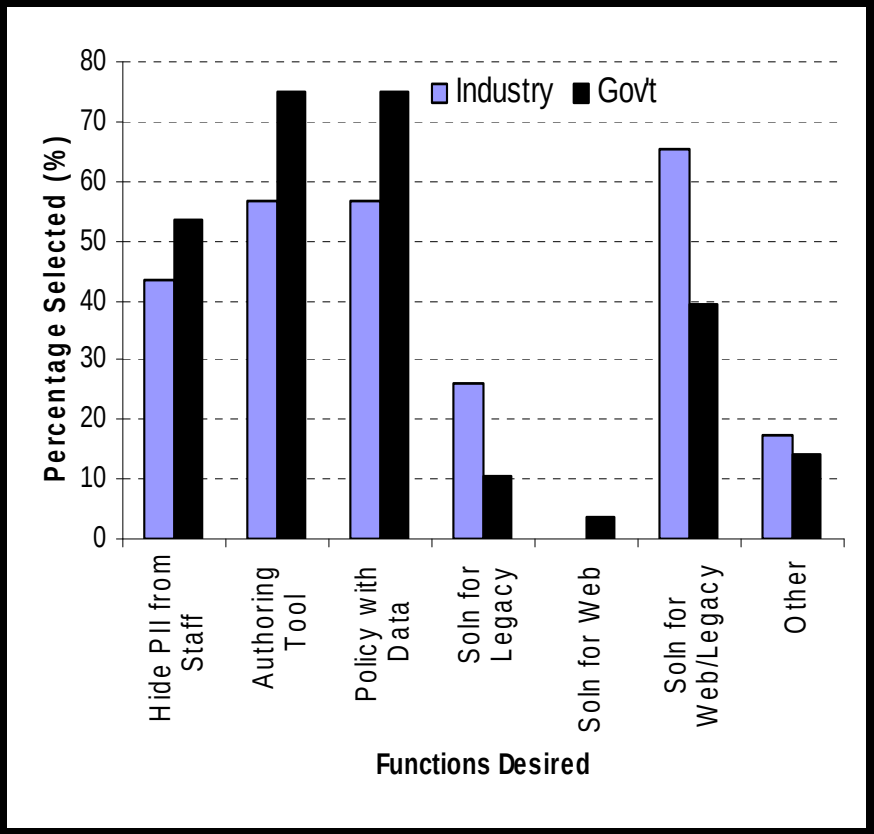
- **Recruited 51 Participants from Industry and Government:**
  - North America
  - Europe
  - Asia Pacific
- **Sent Participants Privacy Questionnaires by E-Mail**
- **Asked about Top Concerns, Desired Function, Current Activities**
- **Analyzed Data by Industry (N=23) and Government (N=28)**
- **Questionnaire Response Rate was Approximately 80% from Customers**

Top Privacy Concerns Expressed



- **Industry and government patterns of concerns similar**
- **Industry more concerned about economic harm to brand**
- **Government more concerned about privacy violations by users outside the organization**

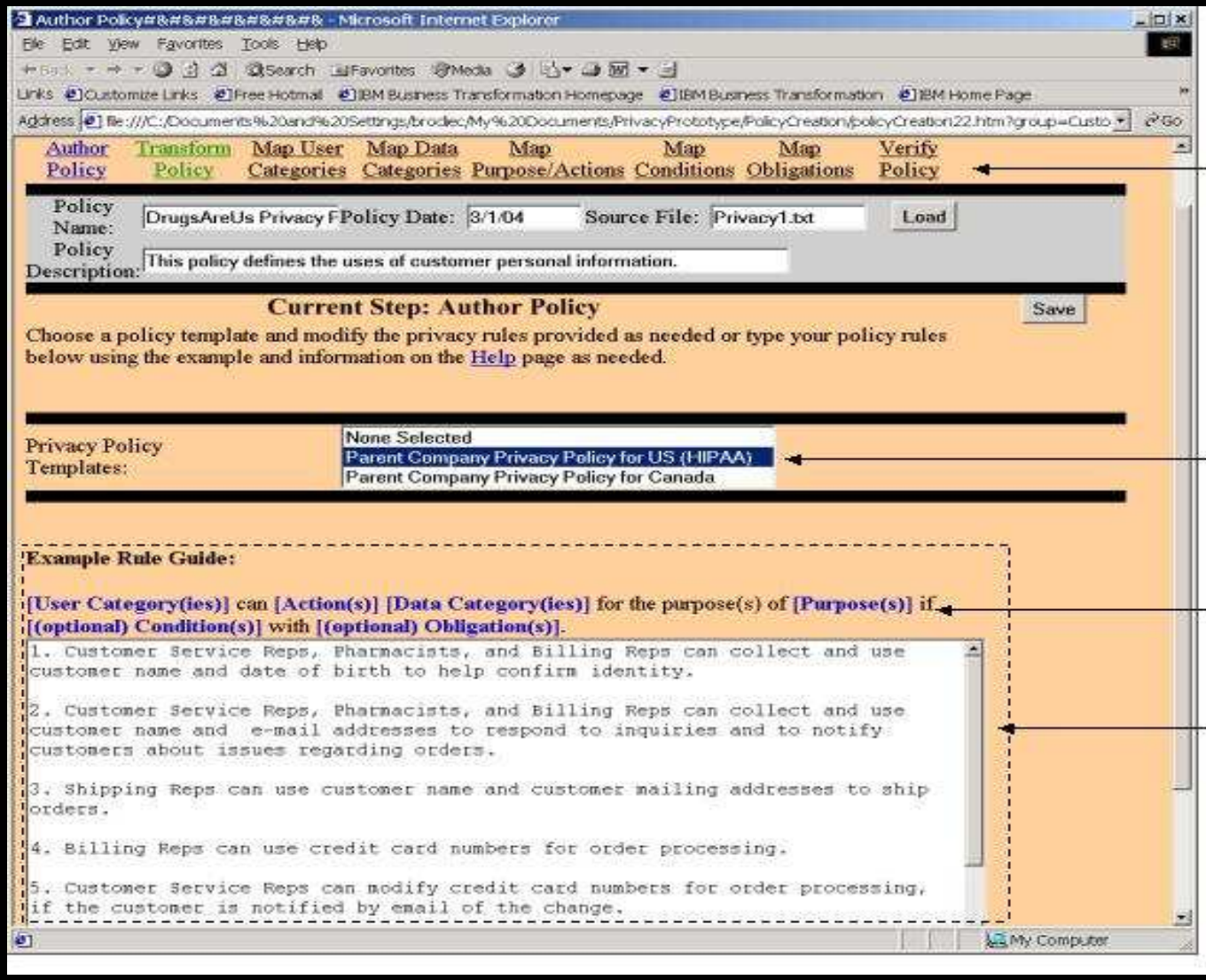
Desired Privacy Functions



- **Similar pattern across industry and government**
- **Desired policy/data portability**
- **Looked for easy to use authoring environment**
- **Wanted one solution for all organizational data**

Iterative Design of Privacy Enabling Technology

- **Focused on key privacy steps from previous analysis**
- **Established interaction requirements and a customer-validated design of a highly usable and effective privacy management tool called SPARCLE (Server Privacy ARchitecture and CapabiLity Enablement). Scope:**
  - **Author policies**
  - **Connect policy definition to system entities (Implement)**
  - **Check policy compliance (Audit)**
- **Iteratively designed and reviewed with customers**
- **10 sessions with 22 target users over 2 design iterations**

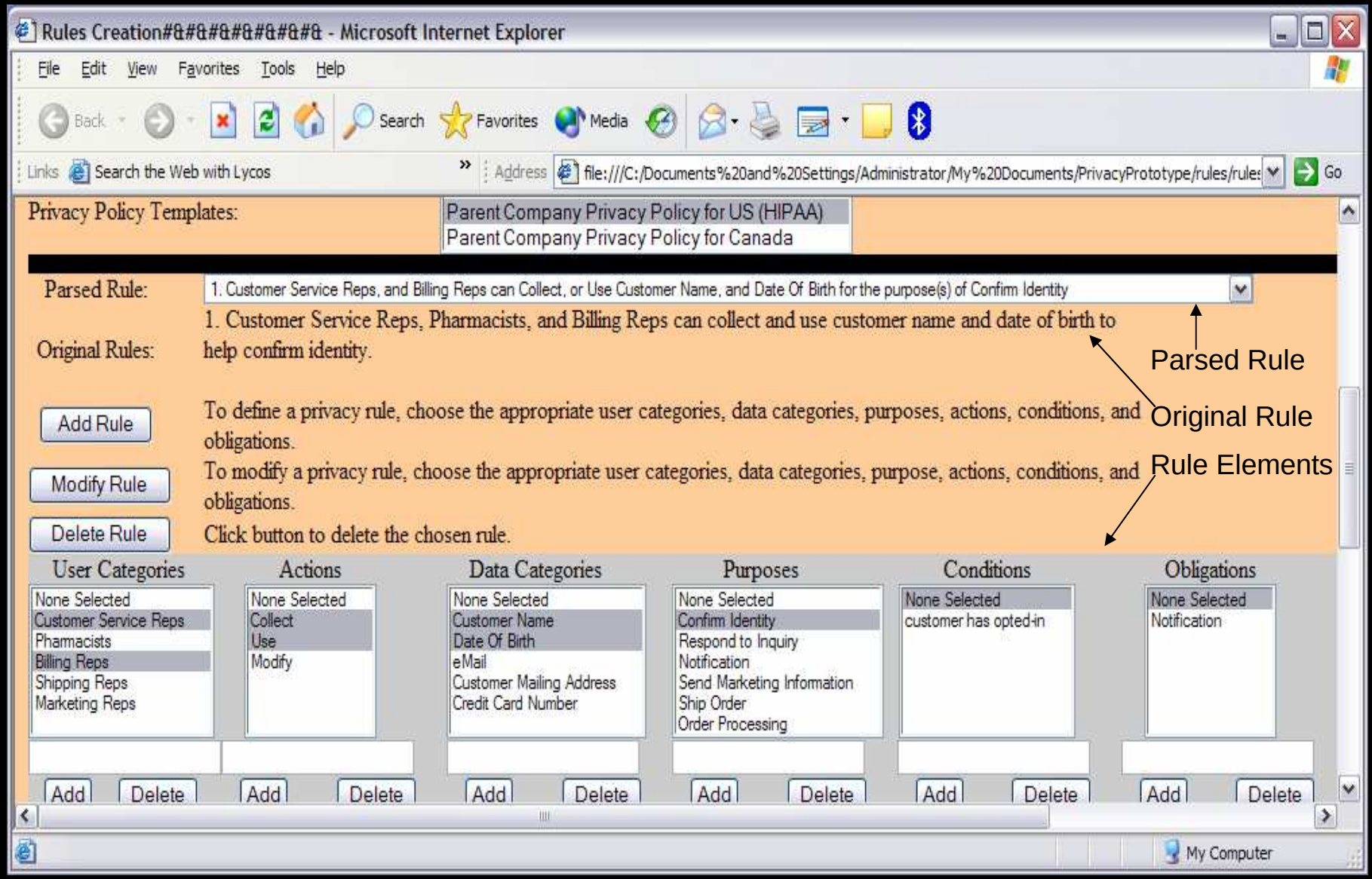


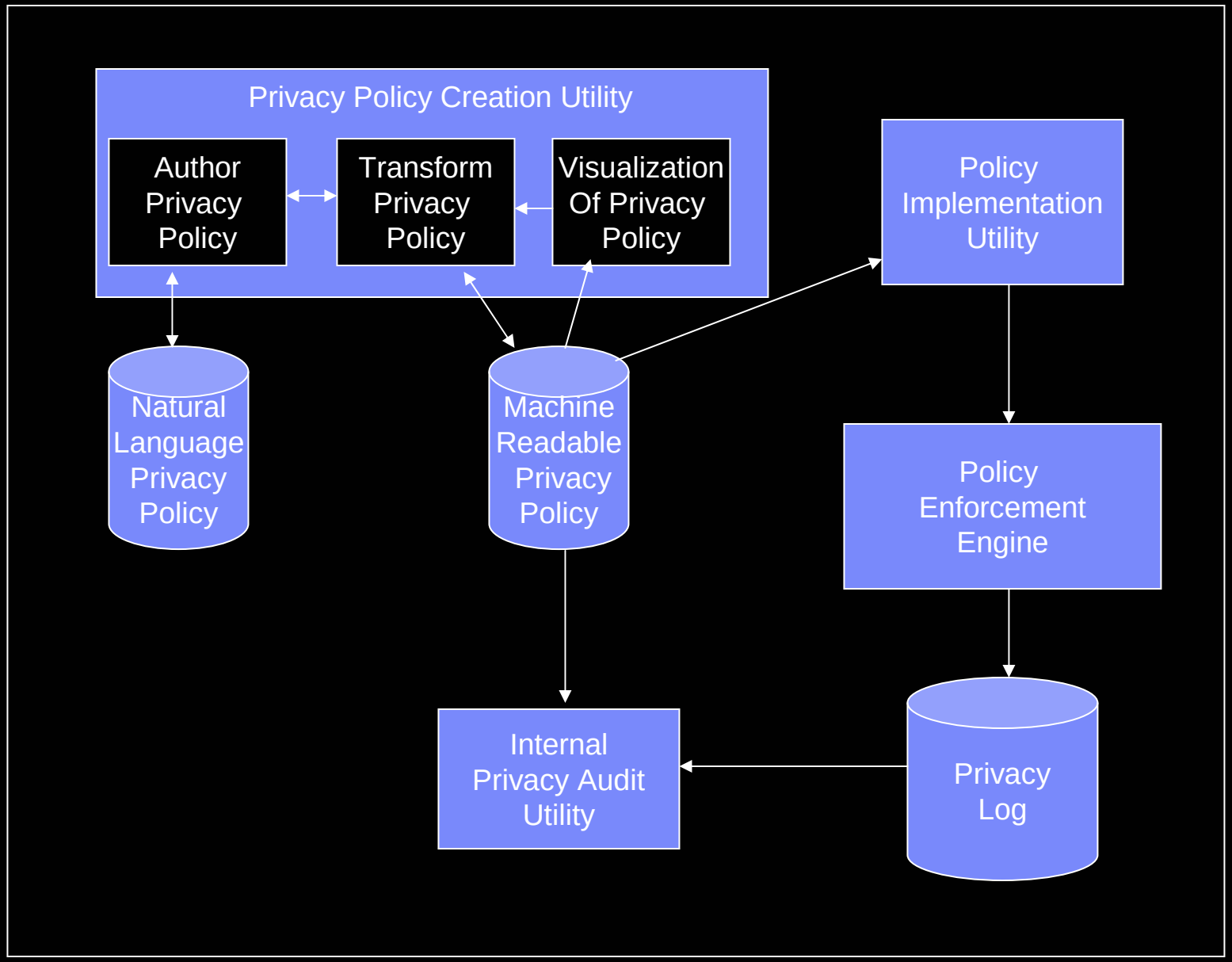
Policy Authoring And Implementation Task Steps

Privacy Policy Template Selection List

Privacy Policy Rule Guide

Free Form Area for Typing Natural Language Privacy Policy





Next Steps

- **Continue enrichment and testing of the prototype with target customers!**
- **Exploring relationship to compliance issues**