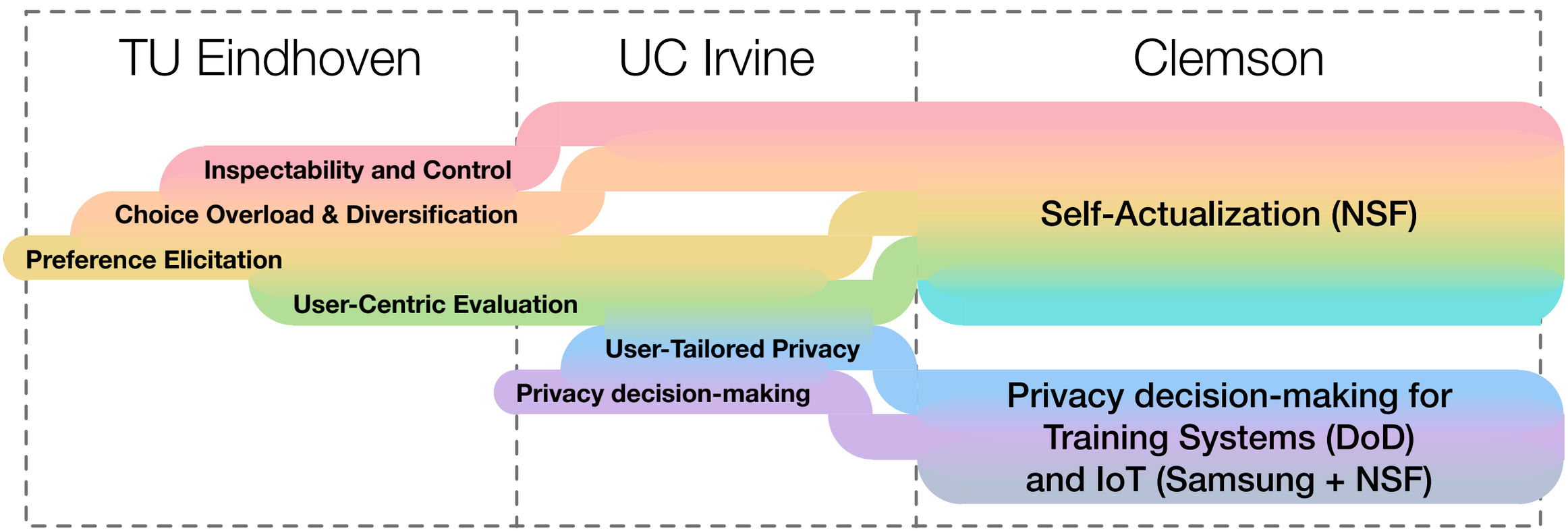
CAN YOU DESCRIBE PROJECTS YOU ARE INVOLVED IN?

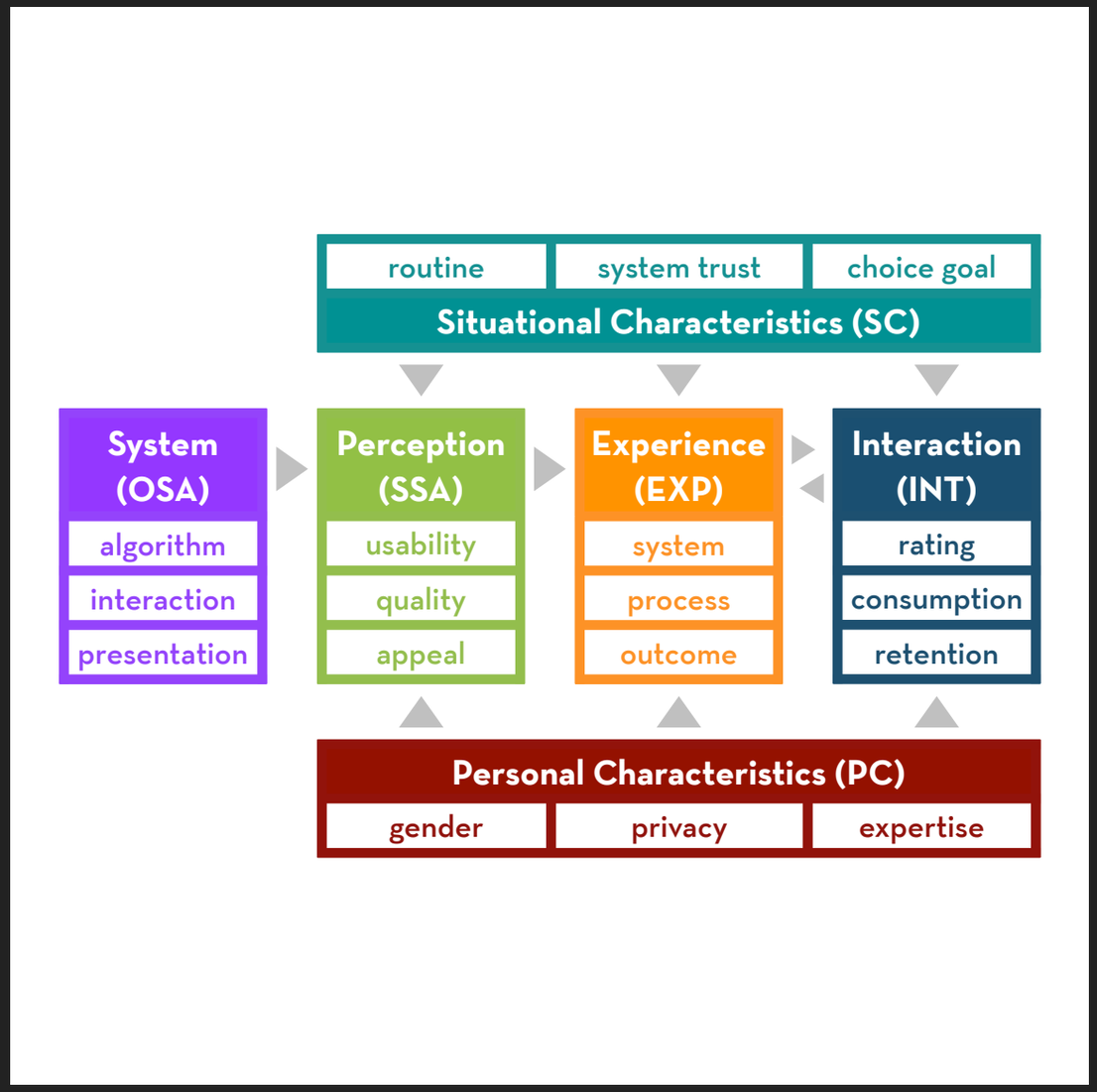
CAN YOU DESCRIBE PROJECTS YOU ARE INVOLVED IN?

OVERVIEW



RECOMMENDER SYSTEMS

- Recommender Systems for Self-Actualization (NSF CRII)
  - Adaptive systems that support rather than replace decision-making
- User-centric aspects of recommender systems
  - Preference elicitation
  - Recommendation diversification
  - User-centric evaluation

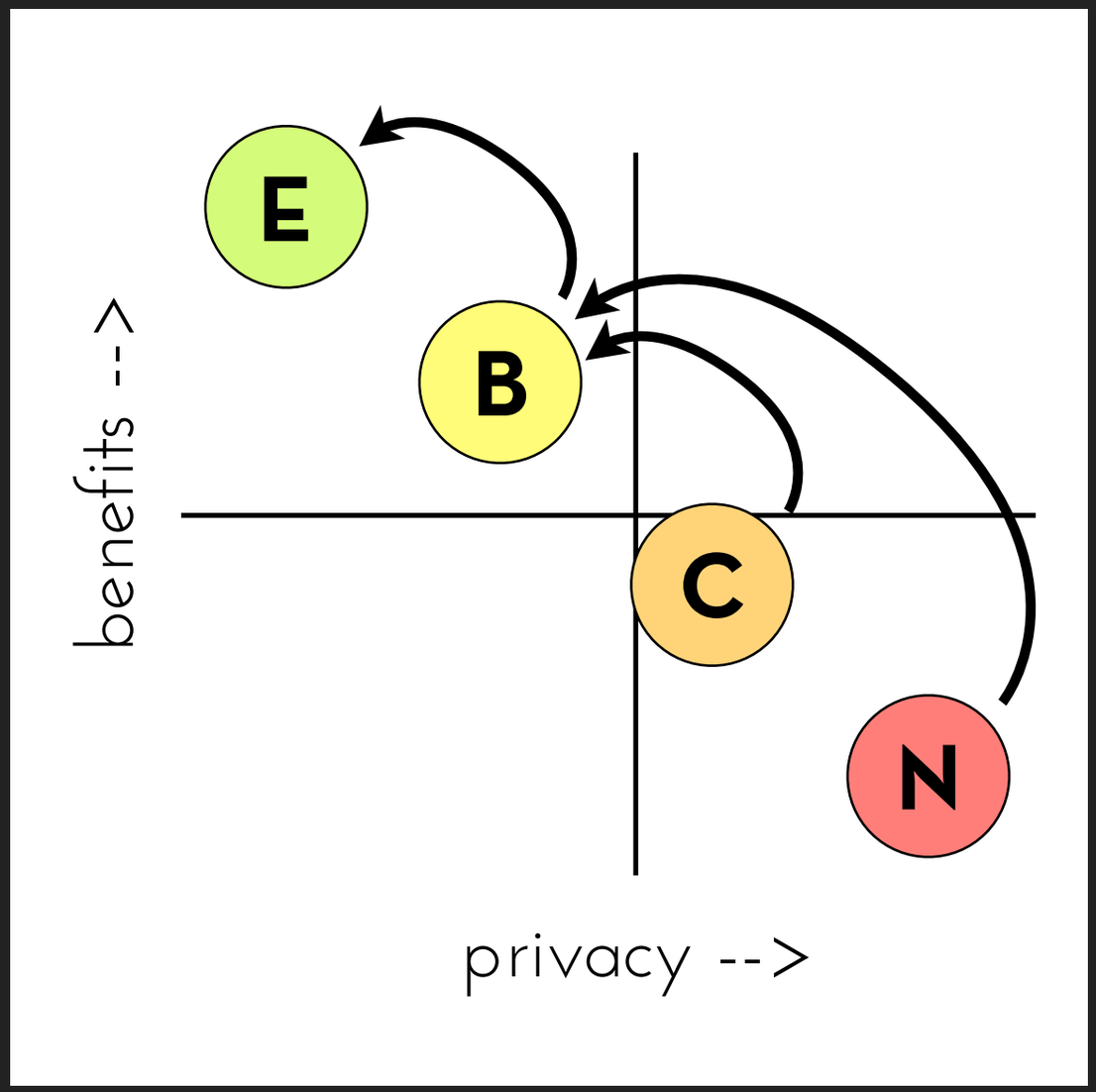


PRIVACY-ENHANCING TECHNOLOGIES

- Privacy comics
  - Enhancing transparency
  - Especially useful for lower-literacy users
- Form auto-completion tools
  - Enhancing control
  - Subtle design changes overcome default effects!

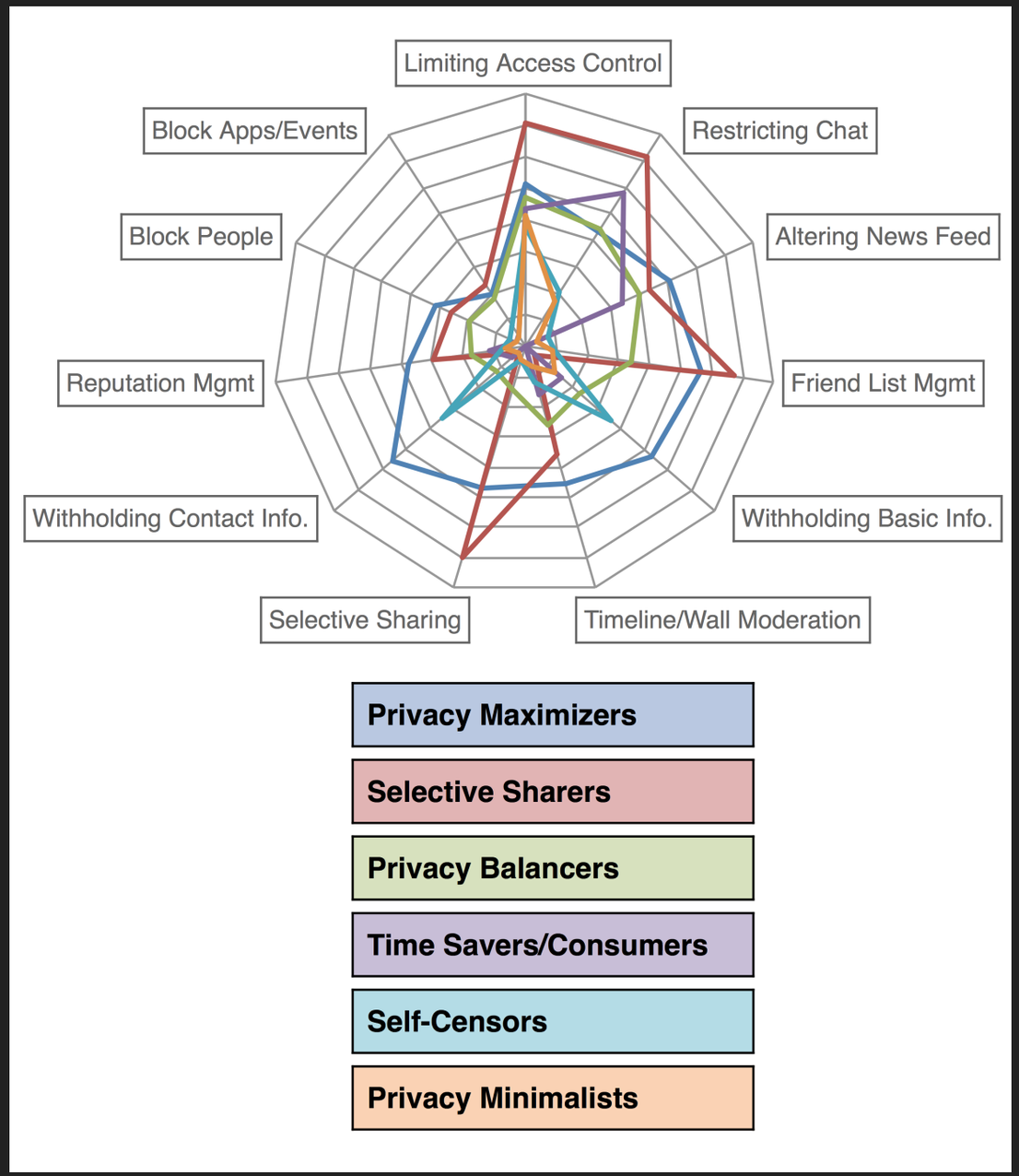
PRIVACY DECISION-MAKING

- Default effects
  - Default settings have a huge impact
- Context effects
  - Users' privacy decisions are influenced by irrelevant options
- Justifications
  - They have an opposite effect



USER-TAILORED PRIVACY

- Understanding decision processes (in IoT: NSF EAGER; in learning systems: DoD)
  - Privacy is multi-dimensional!
  - Discernible profiles
  - Cross-cultural differences
- Adaptive nudges
  - Adapt default settings or request order to user privacy concerns
  - Adapt justifications to user characteristics



PRIVACY IS INTERESTING, BECAUSE NORMS ARE RELATIVE AND PERSONAL, SO LOOKING AT THE INDIVIDUAL LEVEL IS AN INHERENT NEED!

WHAT IS YOUR APPROACH TO STUDYING INDIVIDUALS AND NORMS?

A TYPICAL RESEARCH CYCLE:

- Large-scale, online, multi-variate, scenario-based experiments
- Decision mapping (with contextual antecedents and attitudinal mediators)
- Machine learning (to uncover dimensions, profiles)
- Controlled experiments with prototypes

SCENARIO-BASED EXPERIMENTS

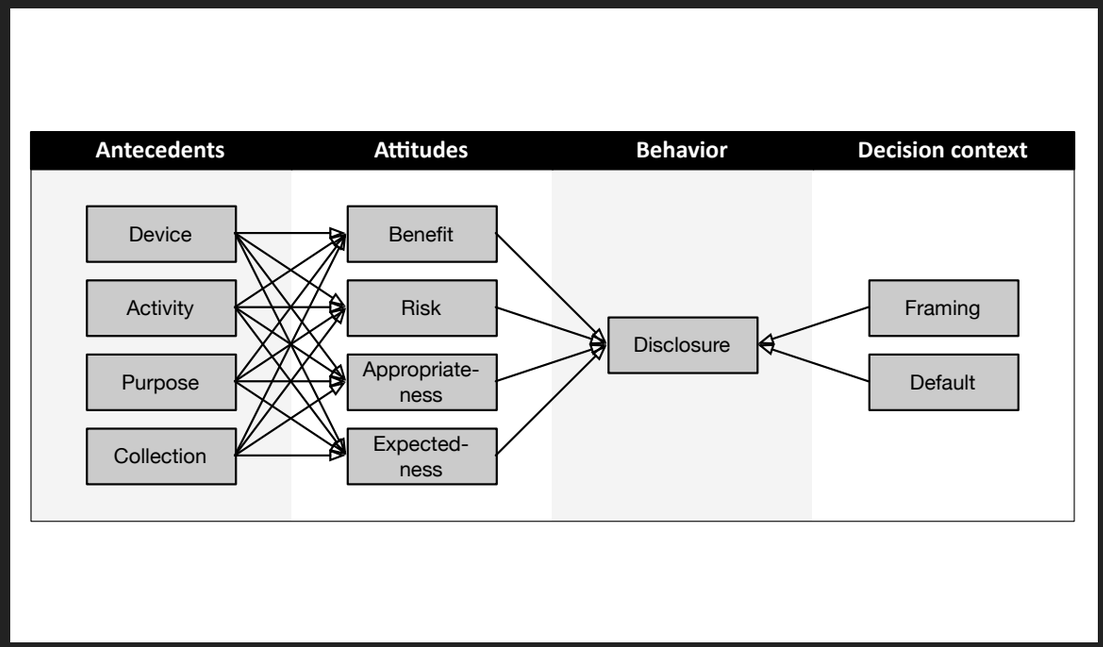
- Large-scale, online, multi-variate
  - 50,000+ contextual privacy decisions, from 9,000+ participants, in 8 countries
- 2,800 public IoT-related decisions, from 200 participants
- Upcoming: 13,000+ household IoT-related decisions, from 1,000+ participants

Scenarios (8x12x4x12 mixed fractional factorial design)			
Device	**Activity**	**Purpose**	**Collection**
Your smart home security system	uses information from your smart home security system[1]	to detect your presence in the house.	The data is not stored.
Your smart refrigerator	uses information from your smart refrigerator	to detect where you are in the house.	The data is stored locally and used to optimize the service.
Your smart HVAC system	uses information from your smart HVAC system	to automate its operations.	The data is stored locally and used to give you insight into your behavior.
Your smart washing machine	uses information from your smart washing machine	to give you timely alerts.	The data is stored locally and used to recommend you other [brand] services.
Your smart lighting system	uses information from your smart lighting system		The data is stored on [brand] servers and used to optimize the service.
Your smart microwave	uses information from your smart microwave		The data is stored on [brand] servers and used to give you insight into your behavior.
Your smart TV	uses information from your smart TV		The data is stored on [brand] servers and used to recommend you other [brand] services.
Your smart alarm clock	uses information from your smart alarm clock		The data is stored on [brand] servers and sold to advertisers.
	uses a location sensor		The data is stored in the cloud and used to optimize the service.
	uses a camera		The data is stored in the cloud and used to give you insight into your behavior.
	uses a microphone		The data is stored in the cloud and used to recommend you other [brand] services.
	connects to your phone/watch		The data is stored in the cloud and sold to advertisers.

Table-1 – Scenarios are generated by selecting one row from each column.

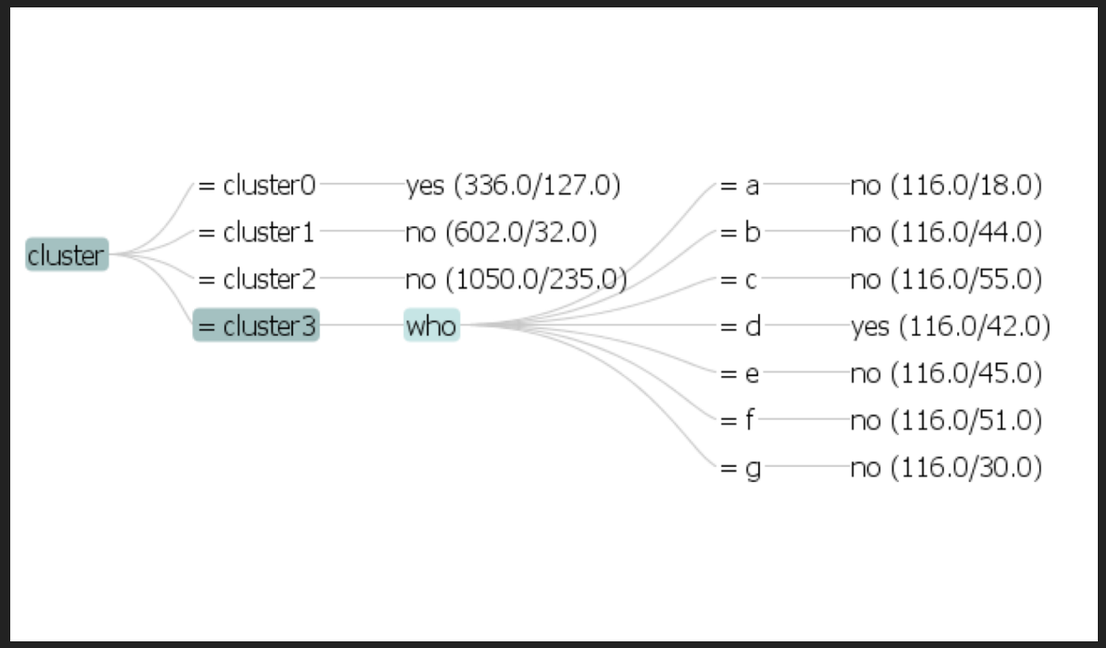
DECISION MAPPING

- How does disclosure come about?
  - Contextual antecedents
  - Attitudes as mediators
  - Influence of decision externalities



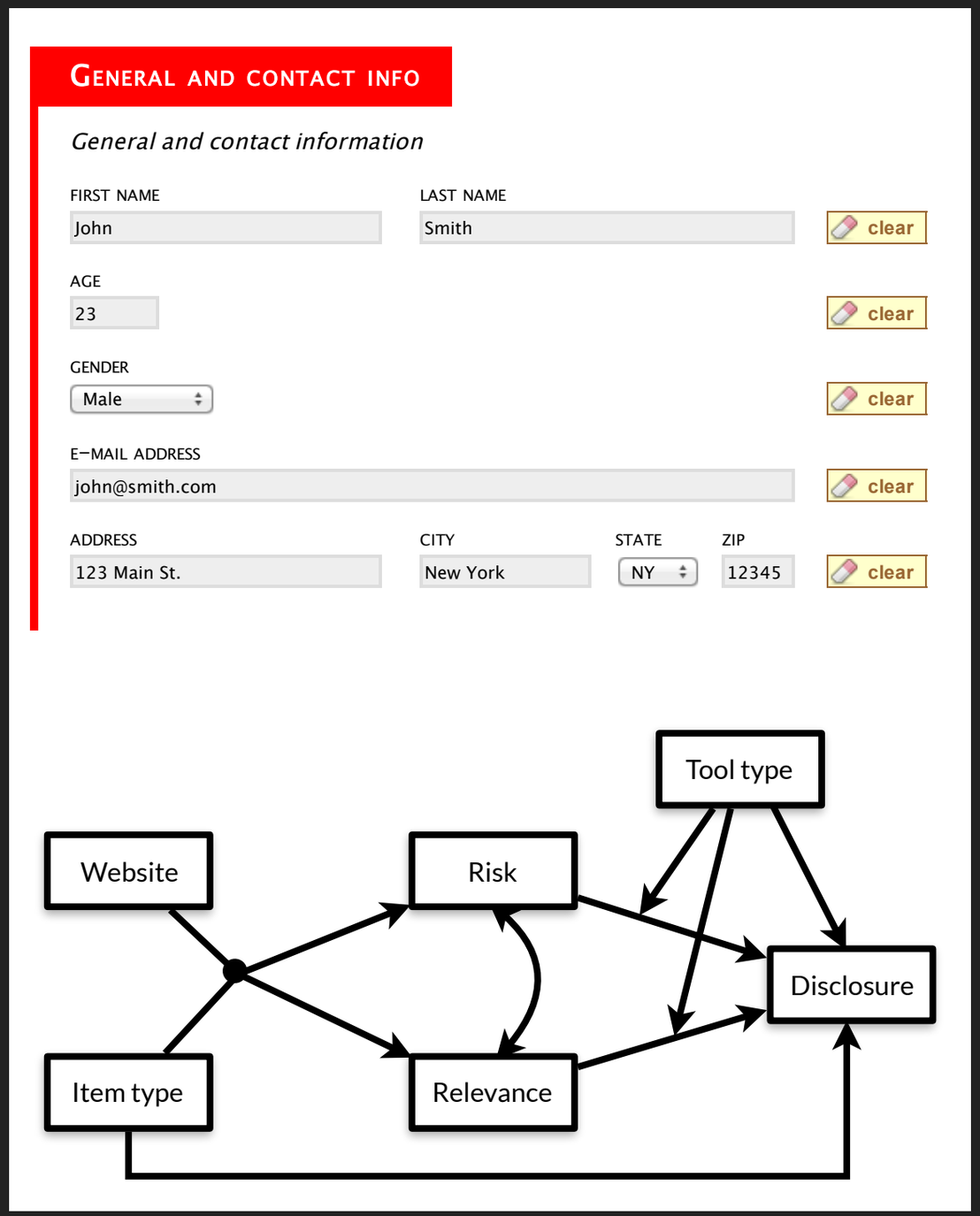
MACHINE LEARNING

- Objectives:
  - Determine relevant dimensions
  - Create privacy profiles
- Techniques:
  - (Iteratively-)clustered multi-tree learning
  - Mixture Factor Analysis
  - Convergent/discriminant validity analysis



IMPLEMENT AND TEST

- Prototype systems
- Create multiple versions
  - Controlled experiments
- Measure attitudinal and behavioral reactions



PEOPLE'S NORMS ARE EMBEDDED IN THEIR DECISIONS, AND THESE DECISIONS ARE INHERENTLY CONTEXTUAL IN NATURE!

WHAT ARE 2 MAJOR CHALLENGES IN STUDYING INDIVIDUALS AND NORMS?

CHALLENGE 1: UNDERSTAND HUMAN DECISION-MAKING

- In privacy, norms are relative and personal
- In security, humans are often the weakest link
  - Common ground: people are making decisions
- How far have we come since Kahneman and Tversky?
  - We finally have more sophisticated computing tools to do this!

CHALLENGE 2: SUPPORT HUMAN DECISION-MAKING

- In privacy and security, decisions are hard!
- What can we do to support users?
  - Notice and control: people make decisions for themselves
    - Too difficult in most scenarios, hard in cases such as IoT
  - Nudging/persuasion: alleviate decision-making burden
    - Normatively questionable
  - User-tailored support: alleviate decision burden, but avoid normative decisions by focusing on the individual

CHALLENGE 2: SUPPORT HUMAN DECISION-MAKING

- Even when you make privacy personal, questions remain:
  - Measure risk and benefit as attitudes vs. behaviors vs. objective outcomes?
  - Is the goal to support, solidify, or evolve users' current behaviors?
  - How should the adaptation be effected?
- These questions are of a normative nature! (we are organizing a CSCW workshop on this topic!)

THIS AMBIGUITY OF ATTRIBUTES,
AND THE ETHICAL QUESTIONS ABOUT
THE ULTIMATE GOAL MAKE PRIVACY
SUCH AN INTERESTING USE CASE!

WHAT ARE YOUR CHALLENGES FOR RESEARCH COLLABORATIONS?

BOUNDARY OBJECTS ARE MISSING

- Many social scientists have no idea what is possible (e.g. eye tracking, large scale experiments, adaptive manipulations)
  - Decisions are often not studied with most sophisticated tools
- Companies don't want to talk about privacy (except when they are gatekeepers)
  - There is no privacy incident database (we are building one)
- Privacy and security often confounded
  - The overlap is in human perception and decision (example: client-side/cloud-based personalization)

BOUNDARY OBJECTS SHOULD NOT JUST BE SYNTACTIC AND SEMANTIC, BUT ALSO PRAGMATIC. YOU MAY HAVE TO CHANGE YOUR RESEARCH!

CAN YOU IDENTIFY 3 AREAS THAT DESERVE MORE CAREFUL ATTENTION?

WE NEED MORE INTERDISCIPLINARY RESEARCH ON:

- "Understanding and supporting decisions"
  - Disciplines: privacy or security + decision psychology
- "Making it personal"
  - Disciplines: privacy or security + machine learning
- Focal contexts: IoT, virtual assistants, learning/training systems
  - Disciplines: all of the above + lawmakers, technologists

OTHER FOCAL AREAS COULD BE:

AUTONOMOUS VEHICLES, CONTACTLESS PAYMENT, DIGITAL VOTING, ETC...

HOW WILL YOUR RESEARCH BE APPLIED TO PRACTICE?

IN THE INTERNET-OF-THINGS:

- Current situation: each device has its own privacy settings
  - This is cumbersome and may lead to suboptimal decisions
- New situation: IoT integration platforms
  - Working on a privacy setting interface for these platforms
  - Goal: reduce complexity, need for interaction, and suboptimal decision-making

IN THE TOTAL LEARNING ARCHITECTURE:

- Current situation: lots of disparate training apps for .mil and .gov
  - Hard to keep track of qualifications, needs, and training recommendations
- New situation: Total Learning Architecture: deep, continuous tracking of users' learning and training activities; make recommendations accordingly
  - Privacy obviously a nightmare, working on a document with suggestions on how to handle it

AS PART OF THE LATTER PROJECT, I AM ORGANIZING A SUMMIT TO DISCUSS AN INDUSTRY STANDARD FOR USER-TAILORED PRIVACY