Formalizing Purpose Restrictions in Privacy Policies

Michael Carl Tschantz, Anupam Datta (PI), and Jeannette M. Wing (PI)

### Policy
- **Purpose** shows up in privacy policies:
  - “Yahoo!’s practice is not to use the content of messages stored in your Yahoo! Mail account for marketing purposes”
  - HIPAA requires covered entities to only use protected health information for a fixed list of purposes (e.g., treatment, payment, and research)

### Goals
- Provide a semantics of purpose to formalize when an action is for a purpose
- Provide algorithms to automate auditing
- Past work avoids the issue by presuming that an oracle labels sequences of actions with their purpose

### Planning for a Purpose
- An auditee acts for a purpose if he performs that action as part of a plan for optimizing the fulfillment of that purpose
- If an action is not part of any such plan, then it was not for that purpose

### Action Model
- Model planning with a modified version of Markov Decision Processes (MDPs)
  - Disallow pointless redundant actions
  - Taking an X-ray has 0.9 probability of enabling a diagnosis
  - When it doesn’t, sending the X-ray for further analysis has a 0.8 probability of enabling a diagnosis

### Agent Behavior Logs
- The auditor detects a violation from [s1, take, s2, send, s3, diagnose, s6] but not upon seeing [s1, take, s4, send, s5, diagnose, s6]

### Auditing Algorithm
- Uses PO/MDP optimization to compares the auditee's behavior to the optimal behavior
  - Detects a violation from showing Ads A or C but not from showing Ad B

### Prior Work: Furthering
- Use Partially Observable Markov Decision Processes (POMDPs) to make information explicit
- Website wants to select an ad to show
- Ad A best for females, Ad C for males, Ad B is middle ground
- Policy: will not use gender for marketing
- Compare behavior to conflated POMDP

### Further Information
M.C. Tschantz, A. Datta, J. M. Wing
Formalizing and Enforcing Purpose Restrictions in Privacy Policies
33rd IEEE Symposium on Security and Privacy, 2012