# Formalizing and Enforcing Purpose Restrictions on Information Use

Michael Carl Tschantz
Carnegie Mellon University
mtschant@cs.cmu.edu

Anupam Datta
Carnegie Mellon University
danupam@cmu.edu

Jeannette M. Wing
Carnegie Mellon University
wing@cs.cmu.edu

**Problem.** *Purpose* is a key concept for privacy policies. For example, the HIPAA Privacy Rule limits the purposes for which health care providers may use health information [1]. Thus, verifying that an organization obeys a privacy policy such as HIPAA requires the ability to determine whether an organization obeys a *purpose restriction*, a constraint on the purposes for which the organization uses information. In the context of auditing for policy compliance, an auditor must be able to determine whether an agent (an audited person, organization, or even computer system in some cases) used information for a given purpose.

Since manual enforcement of purpose restrictions is labor intensive and error prone, hospitals use automated services for detecting suspicious behavior [2]. However, this work is ad hoc and no rigorous approaches to enforcing purpose restrictions on information use exist.

**Solution Approach.** The goal of this work is to place purpose restrictions governing information use on a formal footing and to automate their enforcement. We do so by reducing their enforcement to using planning algorithms for *goal inference*. Planning is key to purpose restrictions since an agent's behavior is for a purpose when the agent chooses that behavior while planning to satisfy the purpose [3]. Prior work has shown how to formalize when an observable action is for a purpose by determining whether that action is part of a plan for furthering that purpose [4].

However, we must go beyond standard goal inference to provide a semantics of *information use*. Purpose restrictions on information use limit the use of information sources, or observations, including inferences that would be impossible without them. Similar to how noninterference characterizes information use for computer programs, these restrictions require understanding how observations of information change the agent's behavior. However, whereas noninterference starts with the automaton model of programs, enforcing purpose restrictions requires understanding a purpose-driven planning agent.

We formalize such a planning agent using a Partially Observable Markov Decision Process (POMDP) that models the agent's environment with the purpose in question defining the reward function of the POMDP. In particular, we build on prior work that infers the purpose (or "goal" in their nomenclature) of an agent from a POMDP of the agent's environment [5]. However, whereas their algorithm attempts to determine the probability that a sequence of actions are for a purpose, we are concerned with whether a use of information could be for a purpose. Thus, we must first develop a formalism for information use.

The explicitness of partial observations in the POMDP model allows us to consider how the agent would plan if some observations were conflated to ignore information of interest. We test whether an agent uses information for a purpose by comparing the behaviors of the agent to the behaviors it would manifest had it planned its actions in this simulated state of ignorance.

**Contributions.** This work offers two contributions (detailed elsewhere [6]). First, we provide a formalization, using POMDPs, of information use. The POMDP model allows us to formalize information use by quotienting the space of observations. We quotient by an equivalence relation that treats two observations as indistinguishable if they only differ by information whose use is prohibited by the purpose restriction. By ignoring this distinguishing information, we simulate ignorance.

Our second contribution is an auditing algorithm using our formalism to compare the behavior of an agent to how it would behave under such ignorance. Our algorithm performs goal inference using an off-the-shelf approximation algorithm for POMDPs. Our algorithm automates much of the enforcement of purpose restrictions on information use.

[1] Office for Civil Rights, "Summary of the HIPAA privacy rule," OCR Privacy Brief, U.S. Dept. of Health and Human Services, 2003.

[2] FairWarning, "Privacy breach detection for healthcare," White Paper, 2010. http://www.fairwarningaudit.com/documents/2010-privacy-breach-detection-fairwarning.pdf

[3] R. Taylor, *Action and Purpose*. Prentice-Hall, 1966.

[4] M. C. Tschantz, A. Datta, and J. M. Wing, "Formalizing and enforcing purpose restrictions in privacy policies," in *Proc. of the IEEE Symp. on Security and Privacy*, 2012, pp. 176–190.

[5] M. Ramírez and H. Geffner, "Goal recognition over POMDPs: Inferring the intention of a POMDP agent," in *IJCAI*, 2011, pp. 2009–2014.

[6] M. C. Tschantz, "Formalizing and enforcing purpose restrictions," Ph.D. dissertation, School of Computer Science, Carnegie Mellon University, May 2012.