Formalizing and Enforcing Purpose Restrictions in Privacy Policies

Anupam Datta
Carnegie Mellon University
18734: Foundations of Privacy
Fall 2015
Privacy as Restrictions on Personal Information Flow

- Direct Interference
- Probabilistic Interference
- Differential Privacy
- Purpose & Role based
  - EPAL
  - XACML
  - *-access control

- Temporal
  - FOTLs
    - [Formal Contextual Integrity, Reduce audit algorithm, Basin et al.]
  - Grok + Legalease

- Information Flow Experiments
- Differential Privacy

Purpose → Planning
Detecting Policy Violations

The Oracle

The Matrix character

<table>
<thead>
<tr>
<th>Species</th>
<th>Computer Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>A program designed to investigate the human psyche.</td>
</tr>
</tbody>
</table>

Computer-readable privacy policy

Audit

Automated audit for black-and-white policy concepts

Detect policy violations

Oracles to audit for grey policy concepts
Purpose Restrictions in Privacy Policies

Yahoo!'s practice is not to use the content of messages [...] for marketing purposes.

By providing your personal information, you give [Social Security Administration] consent to use the information only for the purpose for which it was collected.
Purpose Restrictions are Ubiquitous

- OECD’s Privacy Guidelines
- US Privacy Laws
  - HIPAA, GLBA, FERPA, COPPA,…
- EU Privacy Directive
- Organizational Privacy Policies
  - Google, Facebook, Yahoo,…
  - Hospitals, banks, educational institutions, govt
  - Defense: Mission-based information access
Purpose Restrictions on Actions

With M. C. Tschantz (CMU → Berkeley) and J. M. Wing (CMU → MSR)
2012 IEEE Symposium on Security & Privacy
Goal

- Give a semantics to
  - “Not for” purpose restrictions
  - “Only for” purpose restrictions
  that is parametric in the purpose

- Provide automated enforcement of purpose restrictions for that semantics
X-ray taken

Send record

No diagnosis by drug company

Med records used only for diagnosis

Diagnosis by specialist

Add x-ray

Medical Record

X-ray added

Send record
X-ray taken

Send record

Choice point

X-ray added

Send record

No diagnosis (by drug co. or specialist)

Add x-ray

Best choice

Specialist fails

1/4

3/4

Diagnosis by specialist
Planning

Thesis: An action is for a purpose iff that action is part of a plan for furthering the purpose

i.e., always makes the best choice for furthering the purpose
Markov Decision Process: States, actions, transitions, rewards

- X-ray taken
  - No reward
- X-ray added
  - No reward
- Diagnosis by specialist
  - Reward!
- No diagnosis
  - No reward

Add x-ray

Send record
Auditing

Purpose restriction
Auditee’s behavior
Environment model

Obeyed
Inconclusive
Violated
Record only for diagnosis

[send record]

Violated
Record only for treatment

Policy implications

Violated

No

[●, send record]

Actions optimal?

MDP Solver

Optimal actions for each state

No
No False Positives

- **Theorem (Soundness):**
  If the algorithm returns “violation”, then the actions recorded in the log are not only for the purpose
Utility + Privacy

- Learn MDPs from large audit logs
  - E.g., using reinforcement learning techniques

- Compute optimal plans in MDP
  - Improve functional outcomes (e.g., healthcare outcomes, corporate/defense mission)
  - Improve privacy/security (e.g., detect inappropriate accesses to sensitive information by authorized insiders)
Purpose Restrictions on Information Use

With M. C. Tschantz (CMU → Berkeley) and
J. M. Wing (CMU → MSR)

2013 European Symposium on Research in Computer Security
Antidepressant Medication - Info On An Rx Antidepressant Drug
knowmydepression.com/antidepressant
Visit For Treatment Info & Facts.
Party Supplies For Sale - Buy Your Party Supplies Online Now
www.orientaltrading.com/PartySupplies
Free Shipping on Orders Over $49!
Oriental Trading has 925 followers on Google+

Party Favors Sale  Birthday Party Supplies
Party Decorations  Halloween Party Supplies
Google’s Privacy Policy

When showing you tailored ads, we will not associate a cookie or anonymous identifier with sensitive categories, such as those based on race, religion, sexual orientation or health.
## Rewards from ads

<table>
<thead>
<tr>
<th></th>
<th>Depressed</th>
<th>Not Depressed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meds</td>
<td>High</td>
<td>Low</td>
</tr>
<tr>
<td>Party</td>
<td>Low</td>
<td>High</td>
</tr>
</tbody>
</table>
Depressed Case

- Depressed
  - Ad: None
  - Reward: None
  - Show Meds ad
  - Show Party ad

- Depressed
  - Ad: Meds
  - Reward: High

Not Depressed Case

- Not Depressed
  - Ad: None
  - Reward: None
  - Show Meds ad
  - Show Party ad

- Not Depressed
  - Ad: Party
  - Reward: Low

- Not Depressed
  - Ad: Meds
  - Reward: Low

- Not Depressed
  - Ad: Party
  - Reward: High
Depressed Case

- Depressed
  - Ad: None
  - Reward: None

Not Depressed Case

- Not Depressed
  - Ad: None
  - Reward: None

Depressed Lookup

- Depressed
  - Ad: Party
  - Reward: Meds

Not Depressed Lookup

- Not Depressed
  - Ad: None
  - Reward: None
Initial Beliefs
Depressed Case: 10%
Not Depressed Case: 90%

Updated Beliefs
Depressed Case: 100%
Not Depressed Case: 0%
Depressed Case

Depressed
Ad: None
Reward: None

Not Depressed
Lookup

Not Depressed
Ad: None
Reward: None

Depressed
Lookup

Not Depressed
Lookup

Depressed
Lookup
Depressed Case

Depressed or Not Depressed

Lookup

Depressed
Ad: None
Reward: None

Not Depressed
Ad: None
Reward: None

Depressed or Not Depressed

Lookup

Depressed or Not Depressed

Lookup

Not Depressed
Ad: None
Reward: None

Depressed or Not Depressed

Lookup

Depressed or Not Depressed

Lookup
Initial Beliefs
Depressed Case: 10%
Not Depressed Case: 90%

Updated Beliefs
Depressed Case: 10%
Not Depressed Case: 90%

Lookup
Depressed or Not Depressed

Party
Planning + Information Flow

- Cognitive: Actions are for a purpose without using some information if they came from a plan selected by optimizing a model with disallowed information conflated.
  - Requires mind reading for enforcement

- Behaviorist: Actions are for a purpose without using some information if they are consistent with a plan optimizing a model with disallowed information conflated.
  - Could be consistent by coincidence and actually be for another purpose using the information
Auditing

- Environment model
- Purpose restriction
- Auditee’s behavior

Results:
- Obeyed
- Inconclusive
- Violated
Auditing

POMDP → Equivalence over observations → List of beliefs, actions, and observations

- Obeyed
- Inconclusive
- Violated
Auditing

Depressed $\equiv$ Not Depressed

[lookup, depressed, meds]

Obeyed
Inconclusive
Violated
Ignorance Simulator

Depressed $\equiv$ Not Depressed

Optimal actions ignoring health

[ lookup, depressed, meds]

No

Actions Optimal?
Implications

- The actions were not for the purpose of marketing without using health data
  - Violates: “marketing without using health data”
- Either (1) used health data for marketing or (2) performed actions for some other purpose
  - In case (1) violates: “health data not for marketing”
Prior Approaches

- Prior approaches:
  - Labeling actions (industry practice)
  - Labeling sequences of actions (Al-Fedaghi 07, Jafari et al. 09)
  - Labeling roles (Byun et al. 05, 08, 10)
  - Labeling code (Hayati and Abadi 05)

- Our work provides a semantic foundation
- Shows the expressiveness of each approach
Interesting Points: only-for rules

- Cannot catch all violations of only-for rules
  - Coincidences provide tenable deniability

- Enforcing only-for rules can improve both privacy and utility
  - Keeps auditees on task
Interesting Point: not-for rules

- Not-for rules restrict very little
  - May still perform actions for very similar purposes

- FIPPs principle on **purpose specification** tries to address this concern

  “The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfilment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.”
Future Work

- Improving accuracy
  - Human models of planning

- Furthering practicality
  - Automated creation of environment models

- Applications
  - Minimum necessary disclosure

- Generalizations
  - Multiple purposes
Summary: Audit Approach

Privacy Policy

Organizational audit log

Complete formalization of HIPAA, GLBA

Computer-readable privacy policy

Environment Model

Audit

Automated audit for black-and-white policy concepts

Detect policy violations

Oracles to audit for grey policy concepts
POMDPs. To define POMDPs, let \( \text{Dist}(X) \) denote the space of all distributions over the set \( X \) and let \( \mathbb{R} \) be the set of real numbers. A POMDP is a tuple \( (Q, A, \tau, \rho, \mathcal{O}, \nu, \gamma) \) where

- \( Q \) is a finite state space representing the states of the agent’s environment;
- \( A \), a finite set of actions;
- \( \tau : Q \times A \rightarrow \text{Dist}(Q) \), a transition function from a state and an action to a distribution over states representing the possible outcomes of the action;
- \( \rho : Q \times A \rightarrow \mathbb{R} \), a reward function measuring the immediate impact on the satisfaction of the purpose when the agent takes the given action in the given state;
- \( \mathcal{O} \), a finite observation space containing any observations the agent may perceive while performing actions;
- \( \nu : A \times Q \rightarrow \text{Dist}(\mathcal{O}) \), a distribution over observations given an action and the state resulting from performing that action; and
- \( \gamma \), a discount factor such that \( 0 \leq \gamma < 1 \).
We say that a POMDP *models a purpose* if $\rho$ measures the degree to which the purpose is satisfied. To select actions for that purpose, the agent should select those that maximizes its expected total discounted reward, $\mathbb{E} \left[ \sum_{i=0}^{\infty} \gamma^i u_i \right]$ where $i$ represents time and $u_i$, the reward from the agent’s $i$th action.
Belief States

This goal is complicated by the agent not knowing \textit{a priori} which of the possible states of the POMDP is the current state of its environment. Rather it holds beliefs about which state is the current state. In particular, the agent assigns a probability to each state $q$ according to how likely the agent believes that the current state is the state $q$. A belief state $\beta$ captures these beliefs as a distribution over states of $Q$ (i.e., $\beta \in \text{Dist}(Q)$). An agent updates its belief state as it performs actions and makes observations. When an agent takes the action $a$ and makes the observation $o$ starting with the beliefs $\beta$, the agent develops the new beliefs $\beta'$ where $\beta'(q')$ is the probability that $q'$ is the next state.
Optimal Strategy

To maximize its expected total discounted reward, the agent does not need to track its history of actions and observations independently of its beliefs as such beliefs are a sufficient statistic. Thus, the agent need only consider for each possible belief $\beta$ it can have, what action it would perform. That is, the agent can plan by selecting a strategy: a function from the space of beliefs $\text{Dist}(Q)$ to the space of actions $\mathcal{A}$. (We use the word “strategy” instead of the more common “policy” to avoid confusion with privacy policies.)