Formalizing and Enforcing Purpose Restrictions in Privacy Policies

Giulia Fanti
Based on slides by Anupam Datta
Carnegie Mellon University
18734: Foundations of Privacy
Fall 2019

Administrative

- HW1 – due on Friday at 12:20 pm ET/9:20 am PT
  - Submit on Gradescope
  - DON'T FORGET to associate problems with your answers

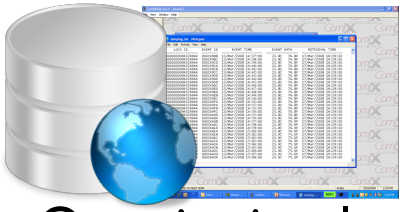
- Recitation on Friday at 12:30 pm ET/9:30 am PT
  - Tutorial on using Docker by Sruti
    - Tool for creating/using containers
  - Will be used on HW2 (to be released early next week)

Last class assignment: Read HIPAA

- Think about at least these questions:
  - What are the common concepts in the 80+ clauses of the privacy rule?
  - How would you categorize the clauses?
  - How are the clauses combined to form the entire rule?
- Discussion

Detecting Policy Violations

Privacy Policy



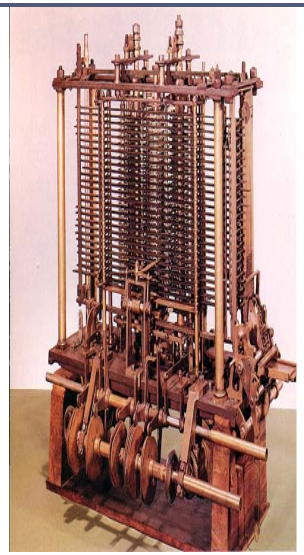
Organizational audit log

Automated audit for black-and-white policy concepts

Complete formalization of HIPAA, GLBA

$$\mathbf{G}\,\Big(\forall p_1, p_2, m.\ \mathsf{send}(p_1, p_2, m) \supset (\forall d, u, q, t.\ (m = \mathrm{info}(d, u)) \wedge \mathsf{contains}(m, q, t) \supset (\bigvee_i \varphi_i^+) \wedge (\bigwedge_j \varphi_j^-)) \wedge (\forall t.\ (m = \mathrm{req\_for\_access}(p_1, t)) \supset \varphi^-_{\mathtt{164.524b2i'}} \wedge \varphi^-_{\mathtt{164.524b2ii'}})\Big)$$

Computer-readable privacy policy



Audit

Detect policy violations

Oracles to audit for grey policy concepts

Purpose Restrictions in Privacy Policies

Not for

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

Only for

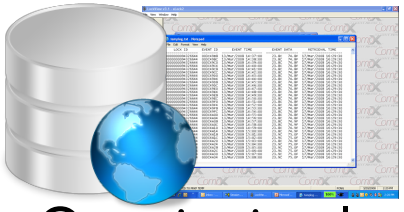
- By providing your personal information, you give [Social Security Administration] consent to use the information **only for** the **purpose** for which it was collected.

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

What might be the difficulties of auditing for purpose?

Privacy Policy

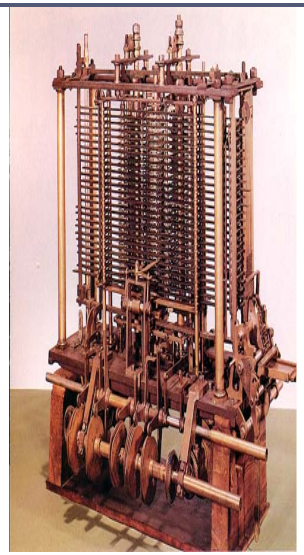


Organizational audit log

Complete formalization of HIPAA, GLBA

$$\mathbf{G}\,\Big(\forall p_1, p_2, m.\ \mathsf{send}(p_1, p_2, m) \supset (\forall d, u, q, t.\ (m = \mathrm{info}(d, u)) \wedge \mathsf{contains}(m, q, t) \supset (\bigvee_i \varphi_i^+) \wedge (\bigwedge_j \varphi_j^-)) \wedge (\forall t.\ (m = \mathrm{req\_for\_access}(p_1, t)) \supset \varphi^-_{\mathtt{164.524b2i'}} \wedge \varphi^-_{\mathtt{164.524b2ii'}})\Big)$$

Computer-readable privacy policy



Audit

Automated audit for black-and-white policy concepts

Detect policy violations

Oracles to audit for grey policy concepts

Formalizing and Enforcing Purpose Restrictions in Privacy Policies

M. C. Tschantz (CMU → Berkeley) and
Anupam Datta (CMU SV)
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

Add x-ray

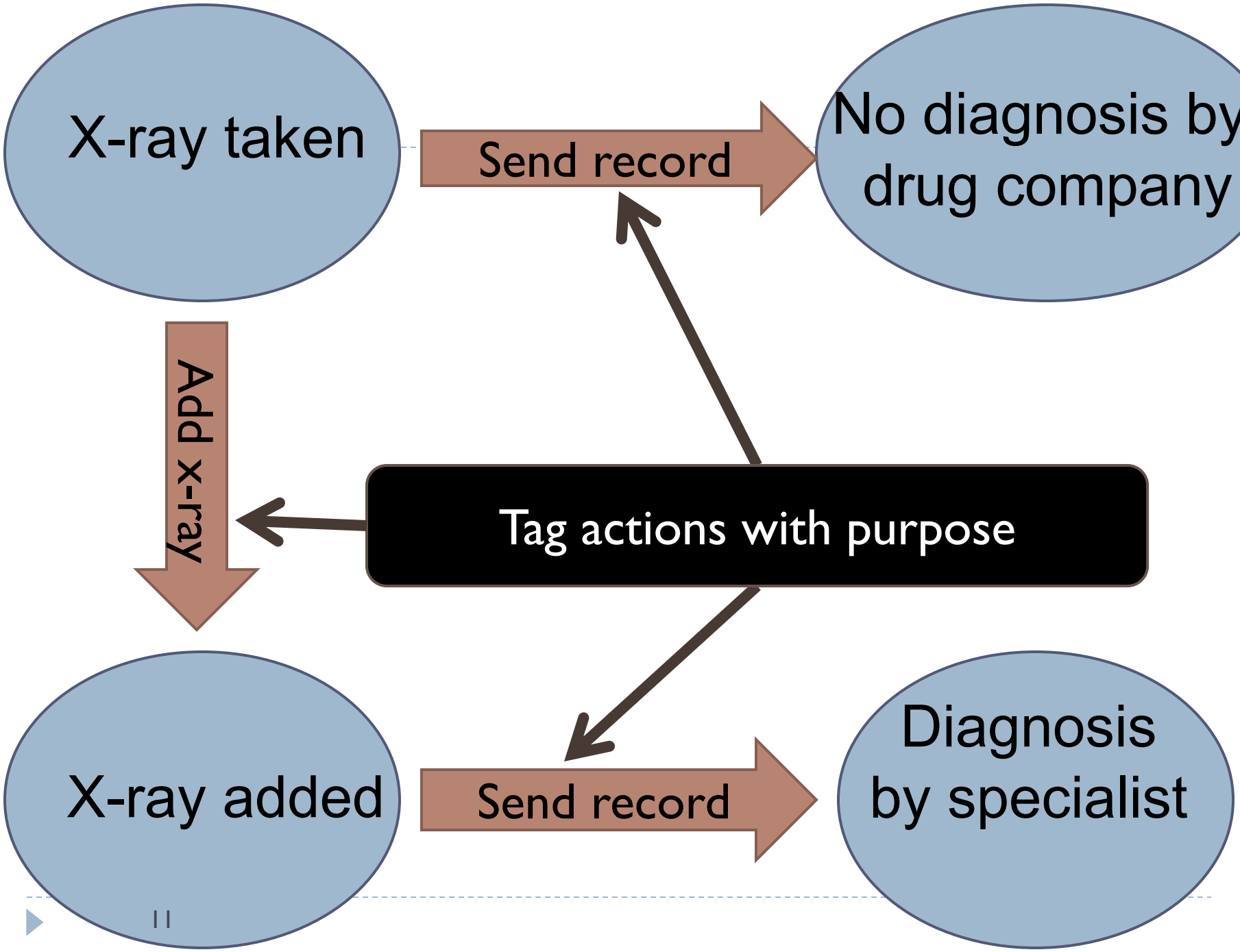
Medical Record

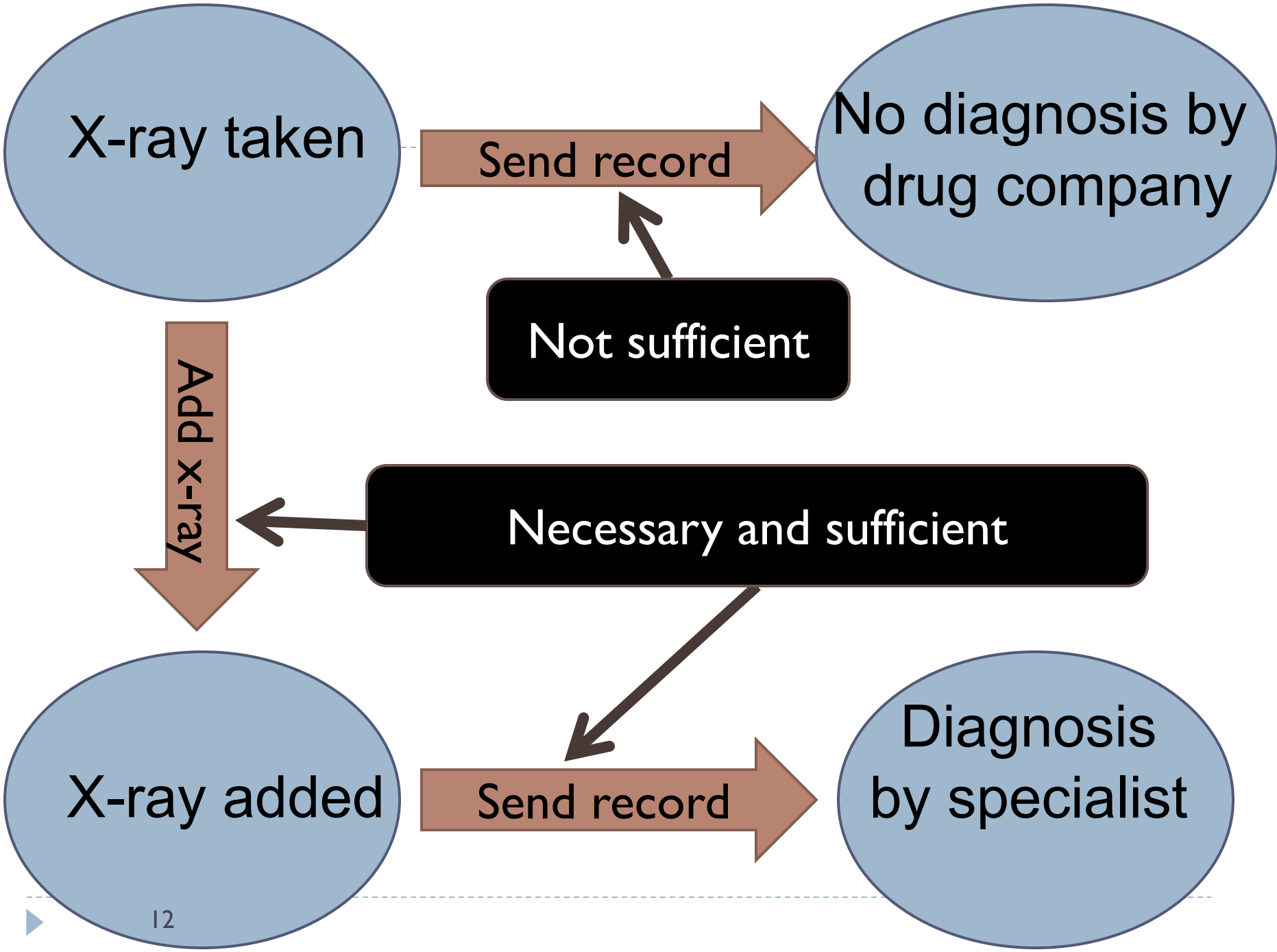
Med records used only for diagnosis

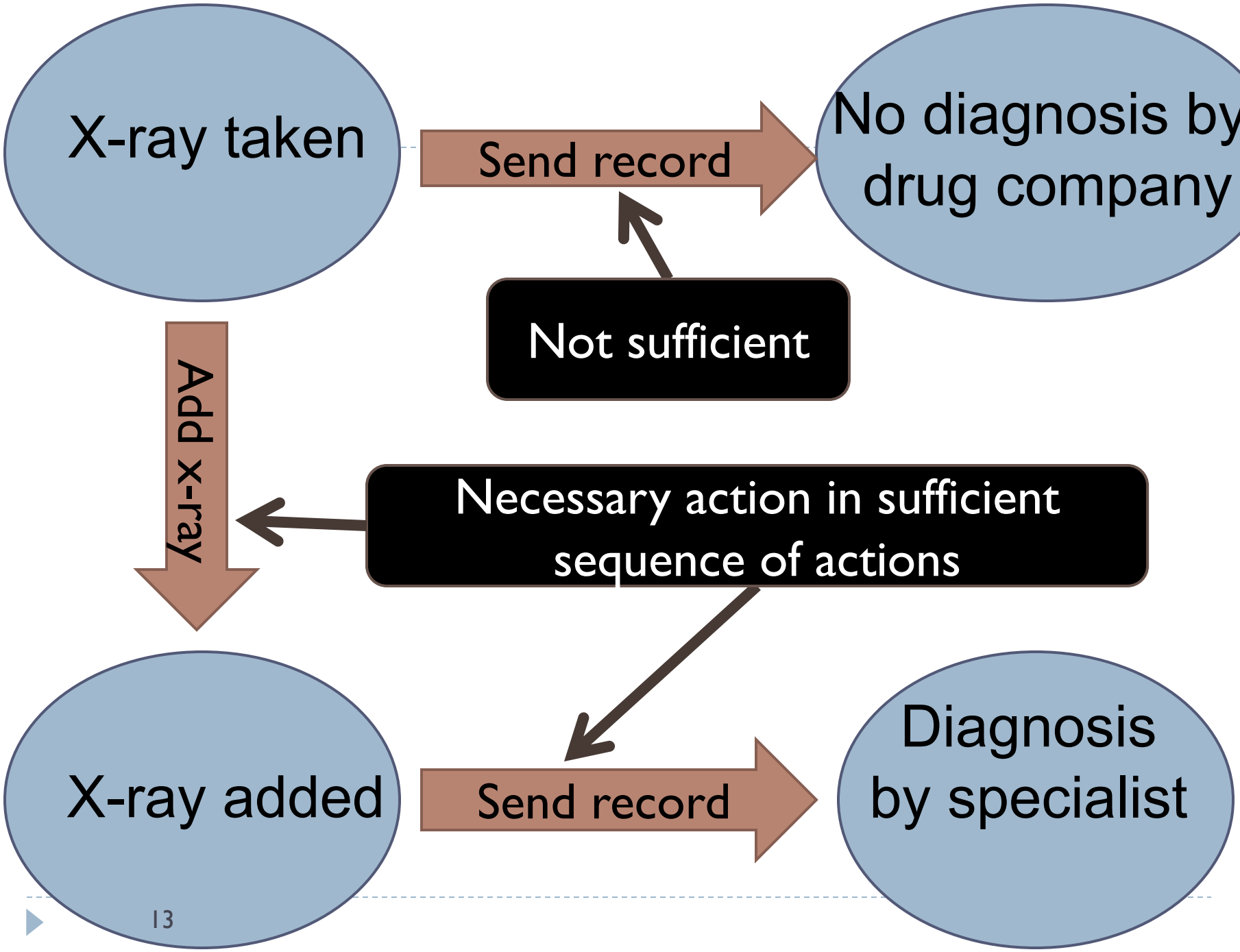
X-ray added

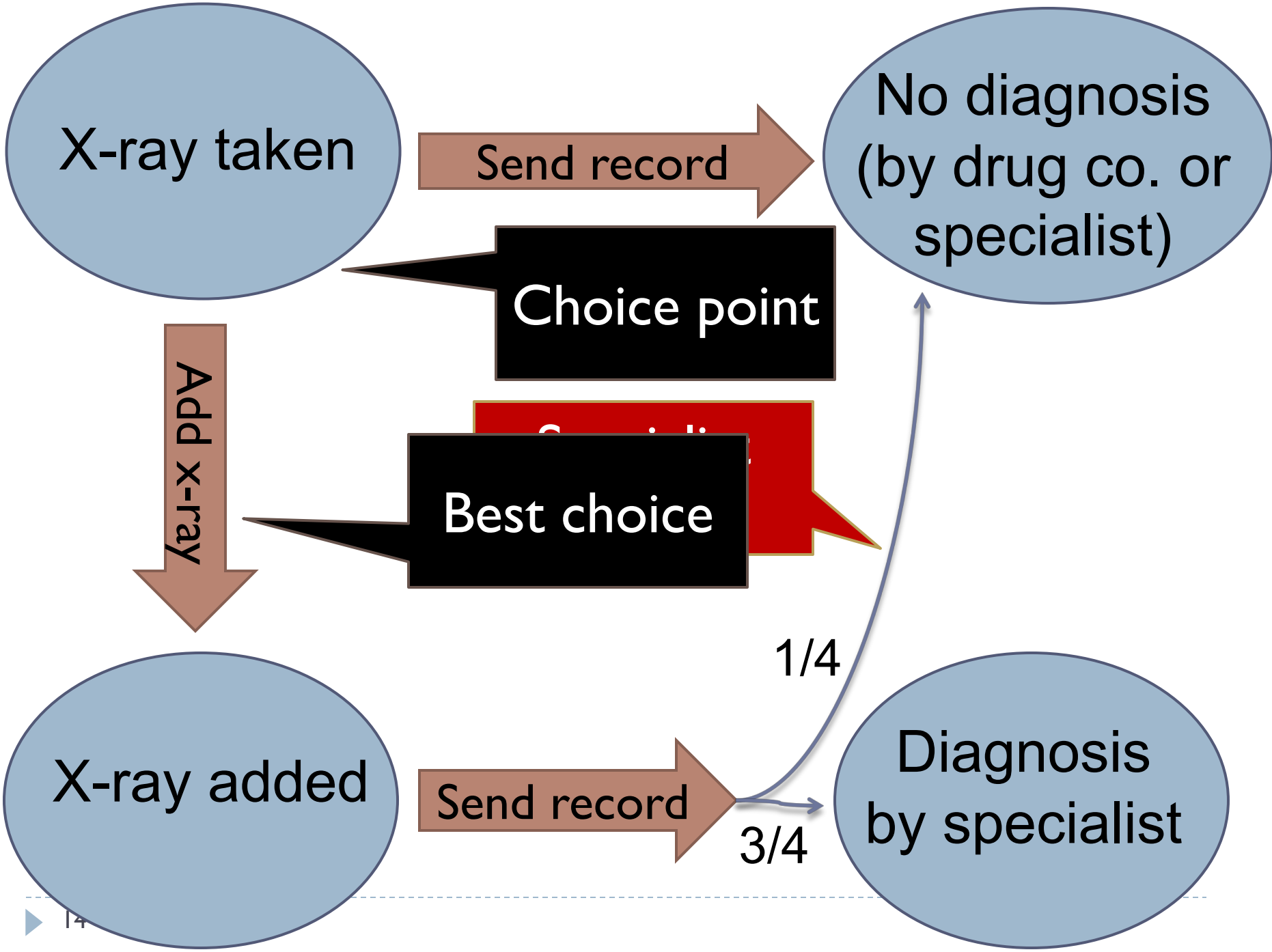
Send record

Diagnosis by specialist


X-ray taken
Send record
No diagnosis by drug company
Add x-ray
Tag actions with purpose
X-ray added
Send record
Diagnosis by specialist


X-ray taken
Send record
No diagnosis by drug company
Not sufficient
Add x-ray
Necessary and sufficient
X-ray added
Send record
Diagnosis by specialist

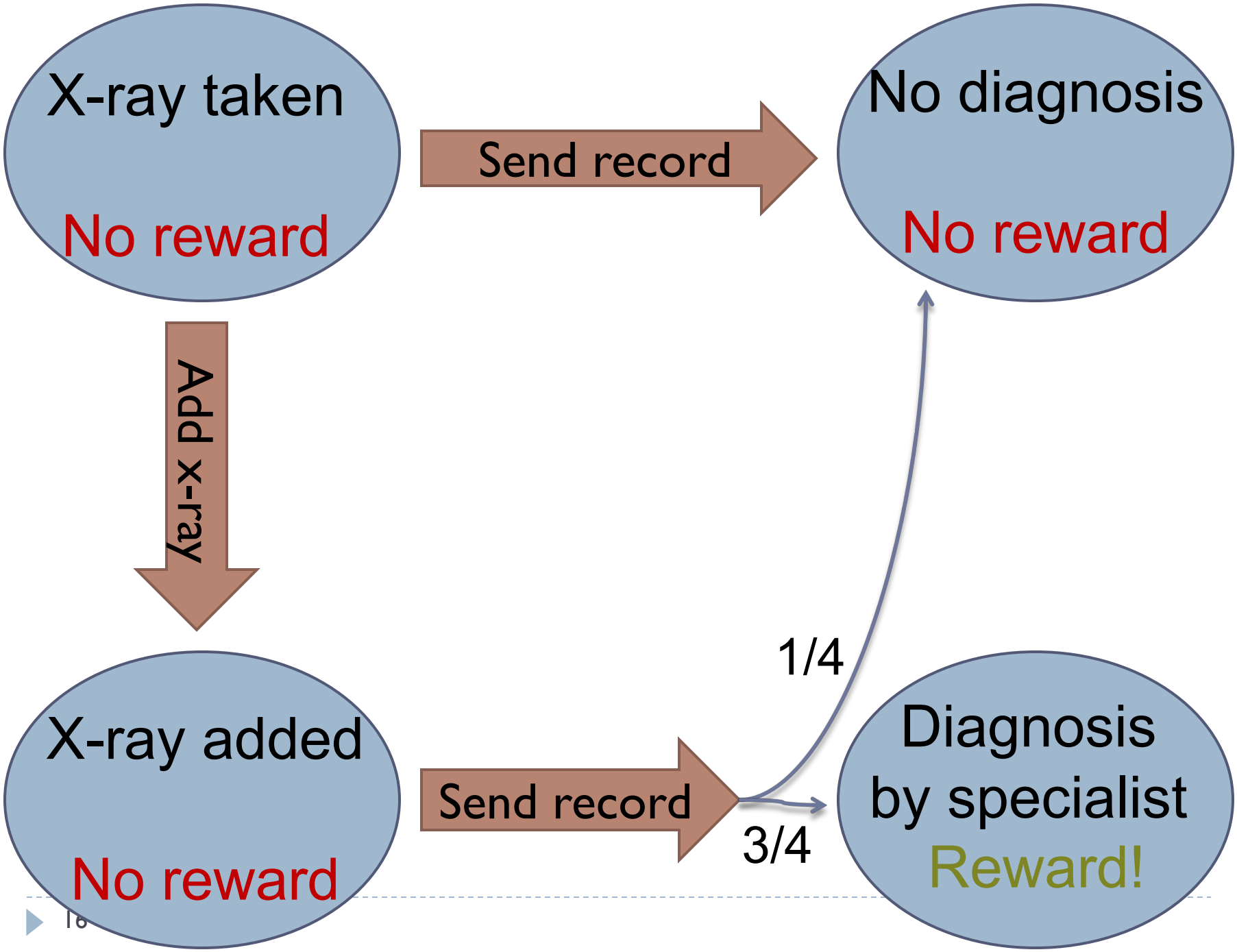

X-ray taken
Send record
No diagnosis by drug company
Not sufficient
Add x-ray
Necessary action in sufficient sequence of actions
X-ray added
Send record
Diagnosis by specialist


X-ray taken
Send record
No diagnosis (by drug co. or specialist)
Choice point
Add x-ray
Best choice
1/4
X-ray added
Send record
3/4
Diagnosis by specialist

Planning

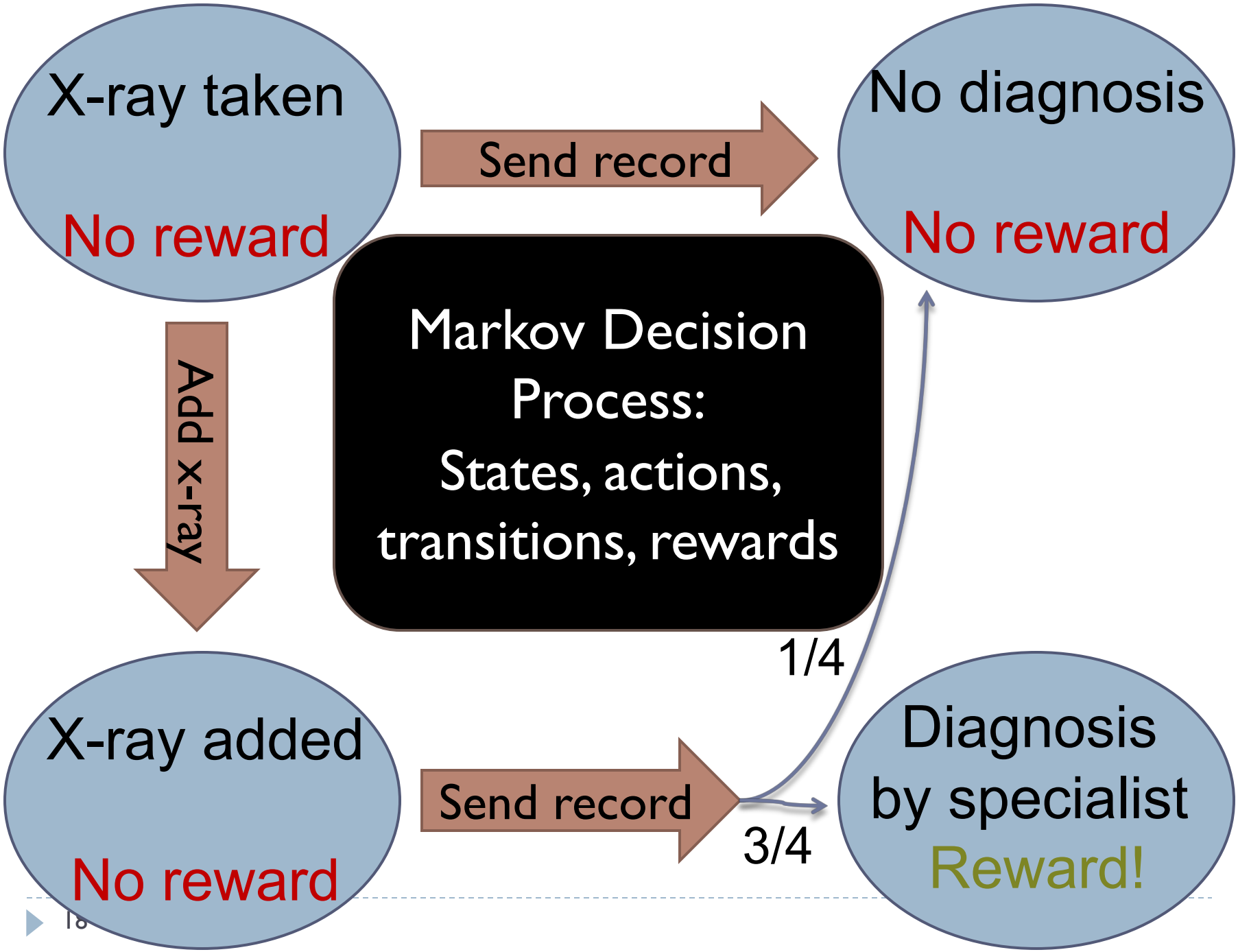
Thesis: An action is for a purpose iff that action is part of a plan for furthering the purpose

i.e., always makes the best choice for furthering the purpose

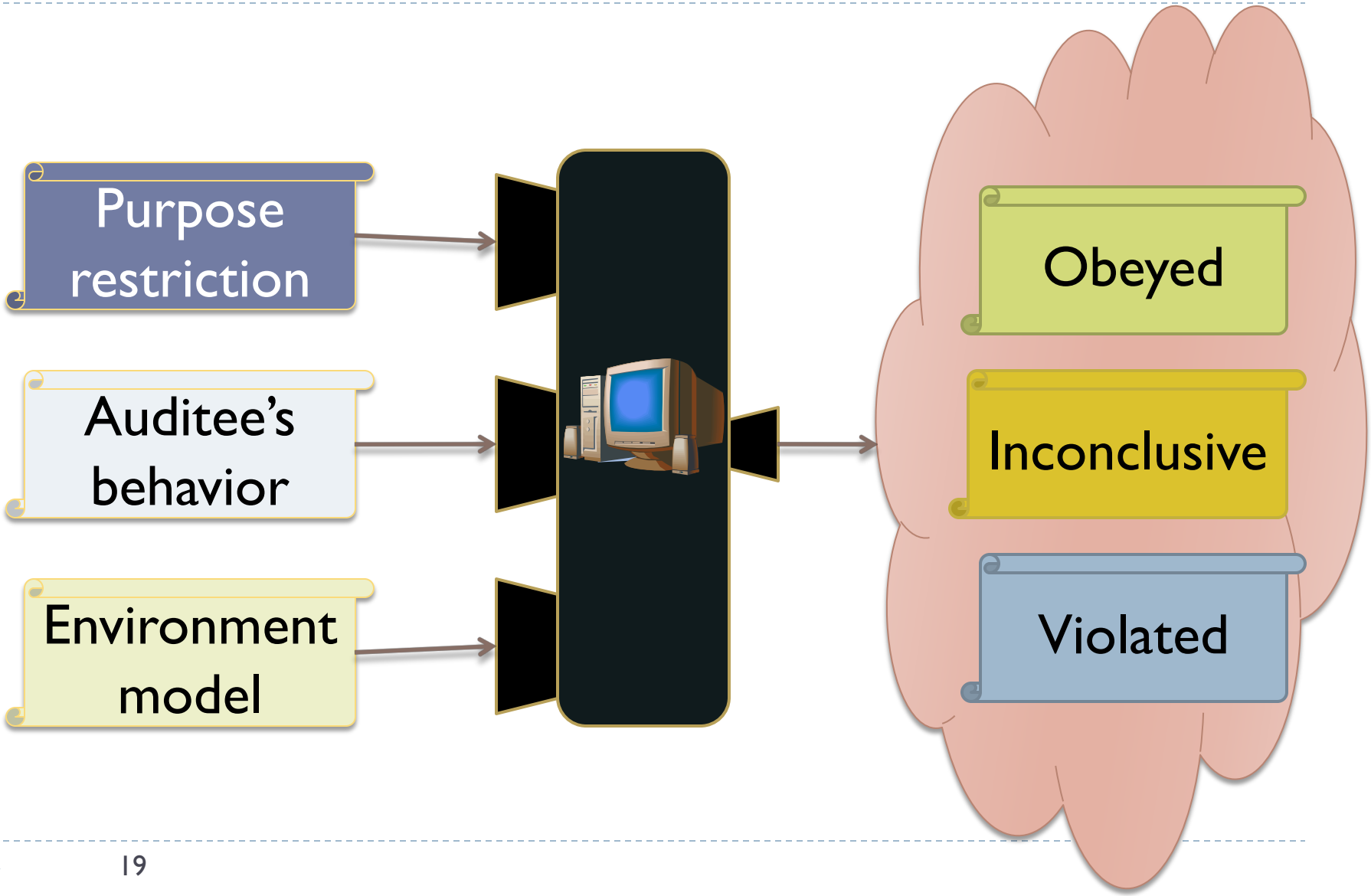

X-ray taken
No reward
Send record
No diagnosis
No reward
Add x-ray
X-ray added
No reward
Send record
1/4
3/4
Diagnosis by specialist
Reward!

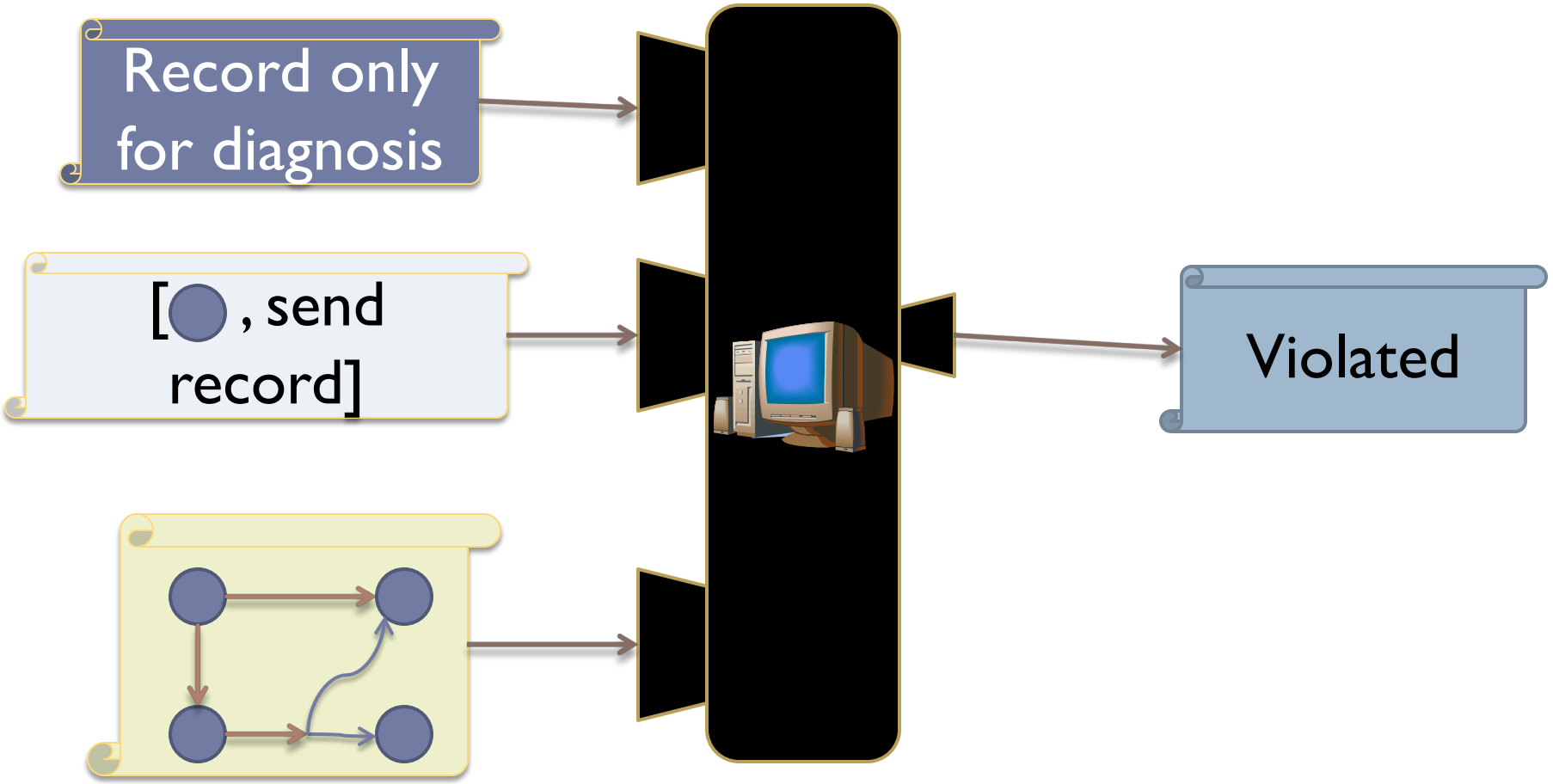
Interlude

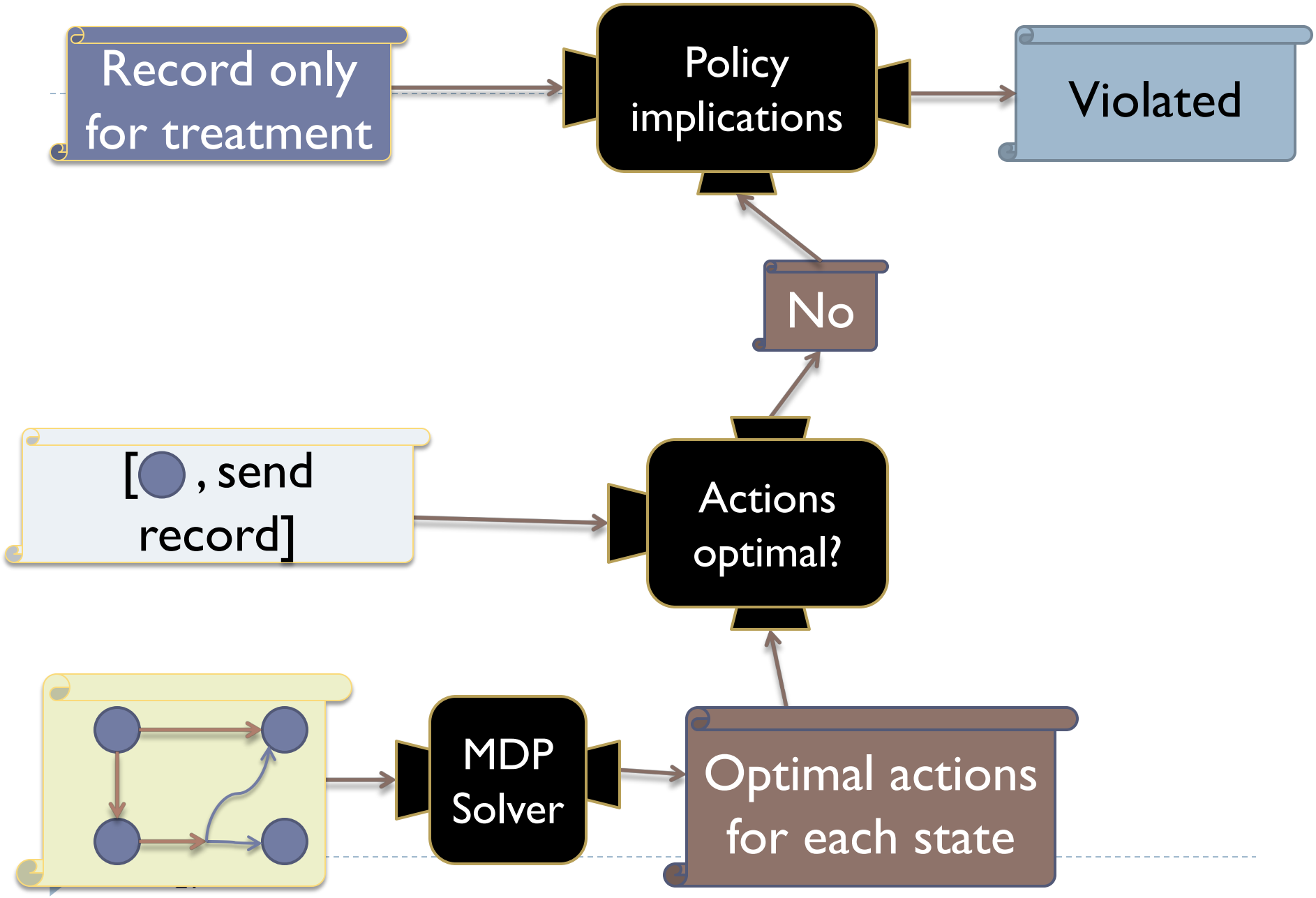
- Primer on Markov Decision Processes


X-ray taken
No reward
Send record
No diagnosis
No reward
Add x-ray
Markov Decision Process:
States, actions, transitions, rewards
1/4
X-ray added
No reward
Send record
3/4
Diagnosis by specialist
Reward!

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

Three steps

- Write MDP → Define environment
- Solve MDP to maximize reward (i.e., purpose expressed as a quantity)
- Check if actions are consistent with optimal strategy/strategies

No False Positives

- Theorem (Soundness):
  If the algorithm returns "violation", then the actions recorded in the log are not only for the purpose

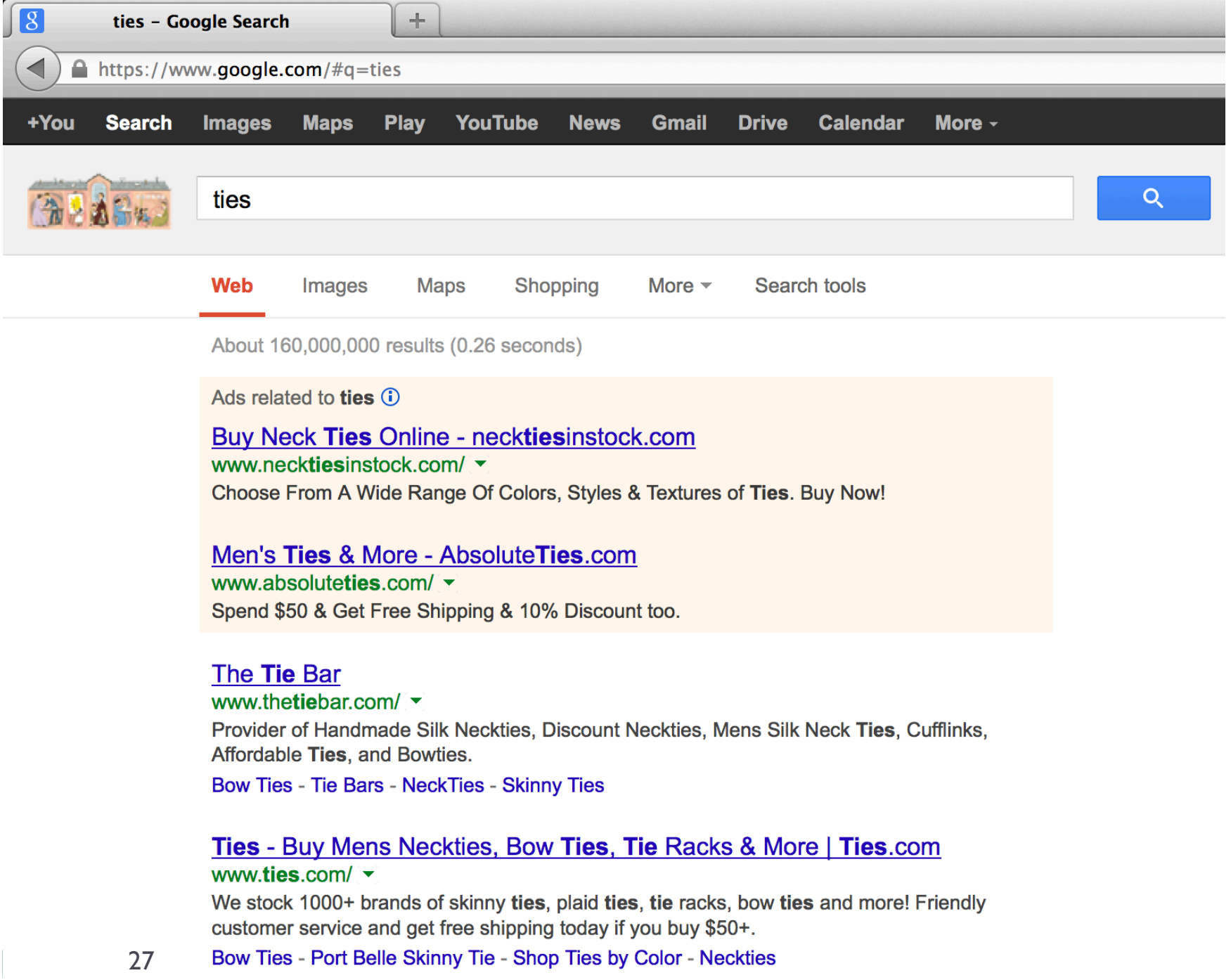
What are some challenges in this approach?

- Defining MDP
- Quantifying purpose
- Users may be trying to satisfy purpose even if they are not acting to maximize it at all stages
- We may not be able to observe the exact state of our users!

Purpose Restrictions on Information Use

M. C. Tschantz (CMU → Berkeley)
Anupam Datta (CMU)
J. M. Wing (CMU → MSR)

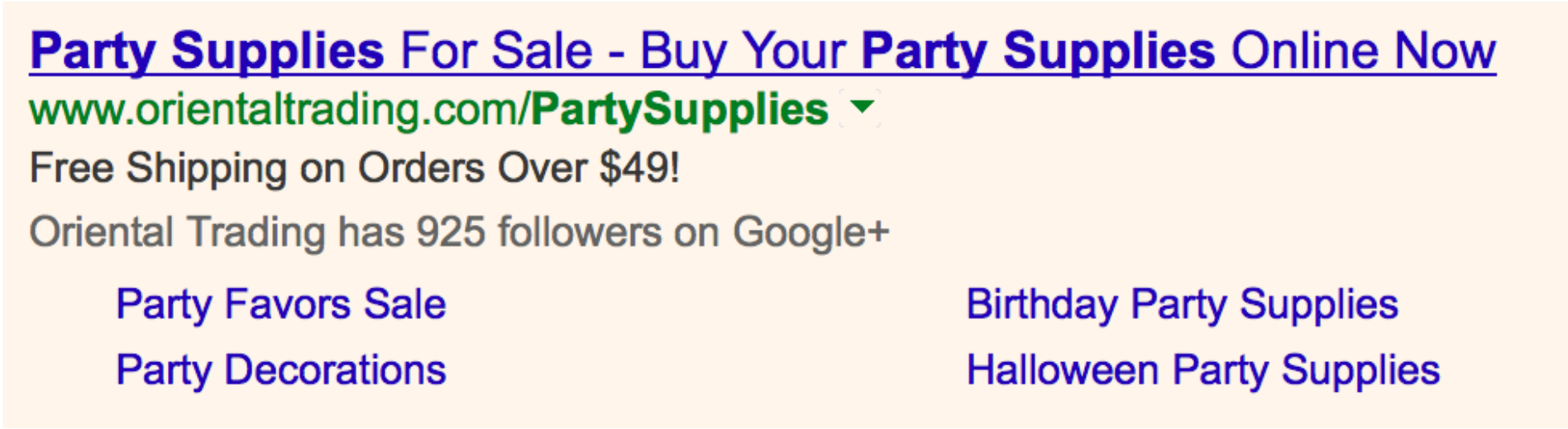
2013 European Symposium on Research in Computer Security


ties - Google Search
https://www.google.com/#q=ties
+You Search Images Maps Play YouTube News Gmail Drive Calendar More
ties
Web Images Maps Shopping More Search tools
About 160,000,000 results (0.26 seconds)
Ads related to ties
Buy Neck Ties Online - necktiesinstock.com
www.necktiesinstock.com/
Choose From A Wide Range Of Colors, Styles & Textures of Ties. Buy Now!
Men's Ties & More - AbsoluteTies.com
www.absoluteties.com/
Spend $50 & Get Free Shipping & 10% Discount too.
The Tie Bar
www.thetiebar.com/
Provider of Handmade Silk Neckties, Discount Neckties, Mens Silk Neck Ties, Cufflinks, Affordable Ties, and Bowties.
Bow Ties - Tie Bars - NeckTies - Skinny Ties
Ties - Buy Mens Neckties, Bow Ties, Tie Racks & More | Ties.com
www.ties.com/
We stock 1000+ brands of skinny ties, plaid ties, tie racks, bow ties and more! Friendly customer service and get free shipping today if you buy $50+.
Bow Ties - Port Belle Skinny Tie - Shop Ties by Color - Neckties

Antidepressant Medication - Info On An Rx **Antidepressant** Drug

knowmydepression.com/**antidepressant**

Visit For Treatment Info & Facts.

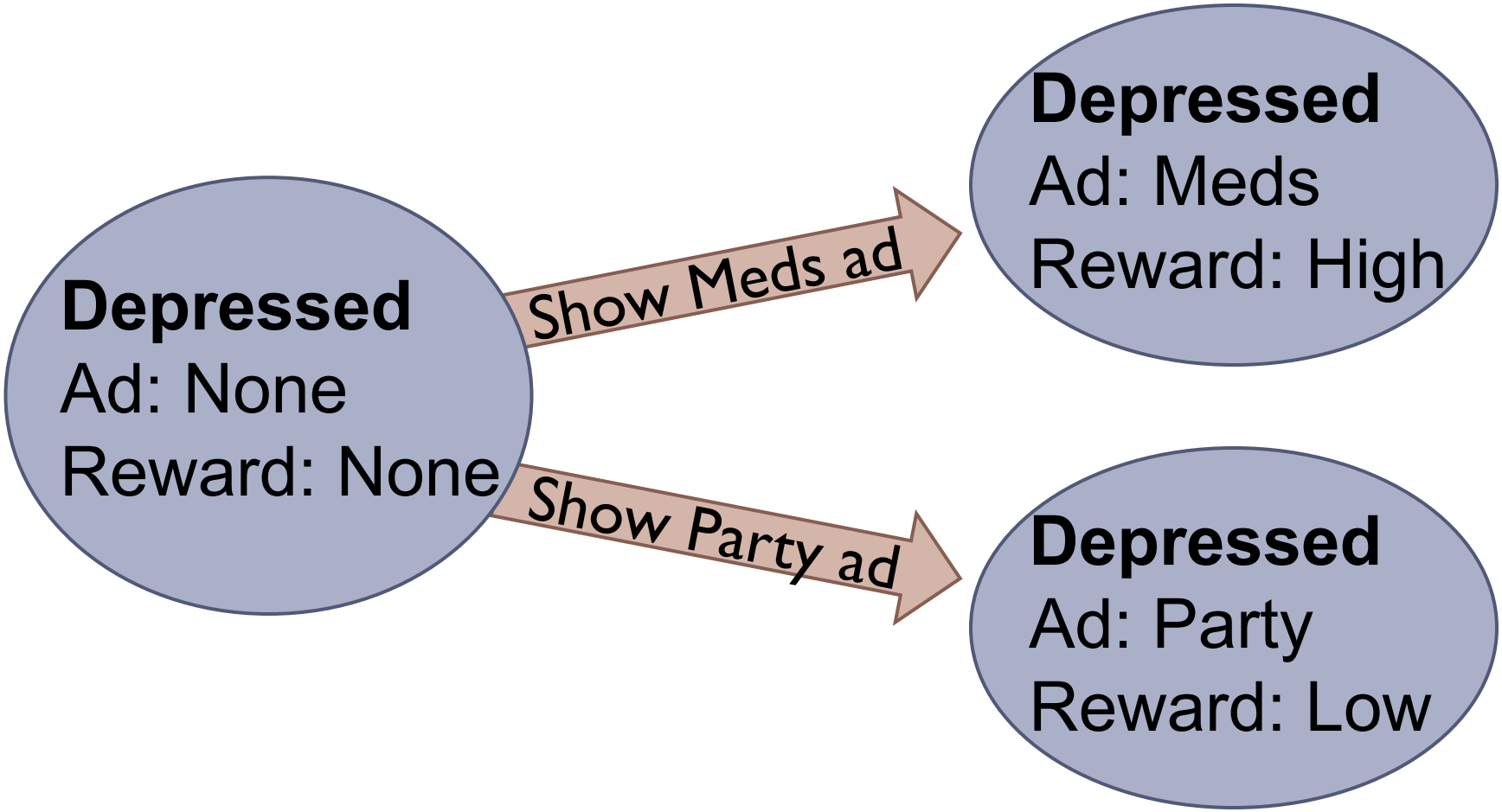

Party Supplies For Sale - Buy Your Party Supplies Online Now
www.orientaltrading.com/PartySupplies
Free Shipping on Orders Over $49!
Oriental Trading has 925 followers on Google+
Party Favors Sale
Party Decorations
Birthday Party Supplies
Halloween Party Supplies

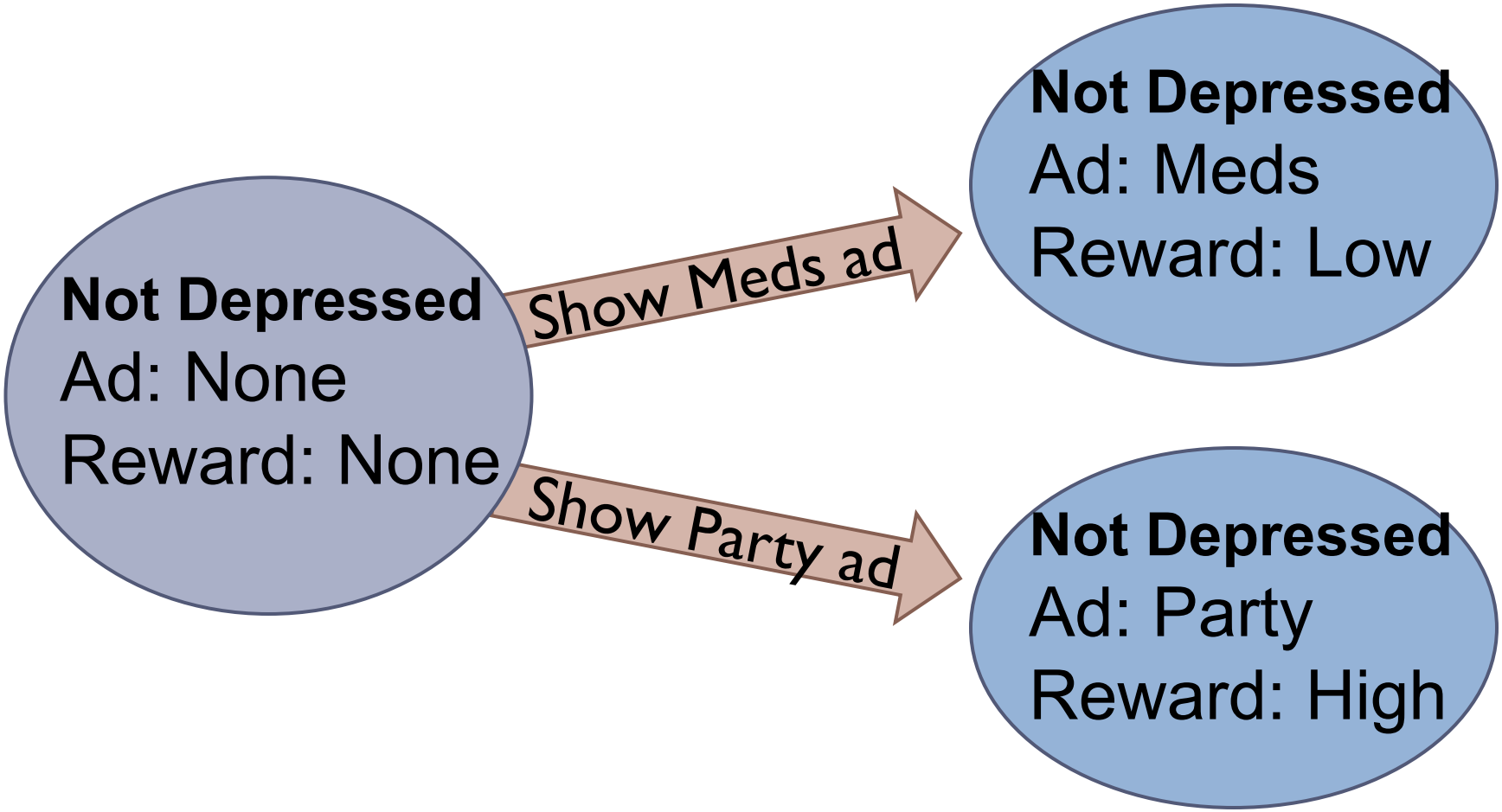
Google's Privacy Policy

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.

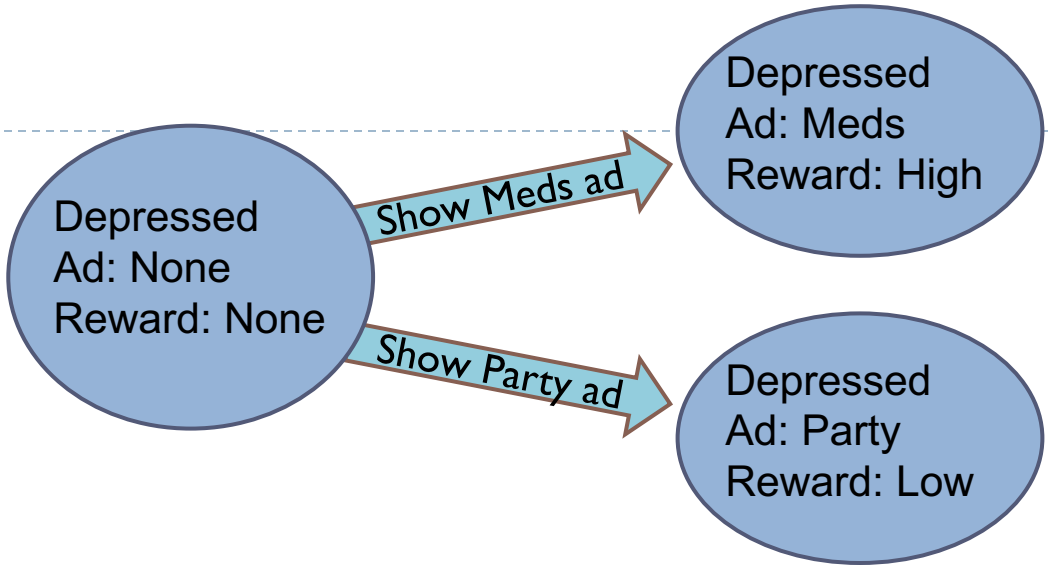
Rewards from ads

	Depressed	Not Depressed
Meds	High	Low
Party	Low	High

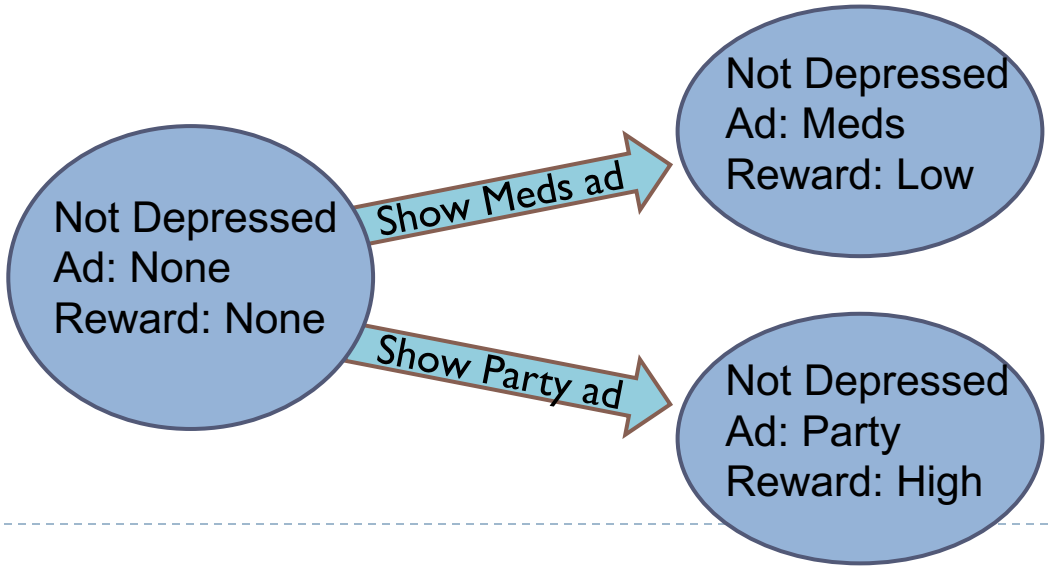

Depressed
Ad: None
Reward: None
Show Meds ad
Show Party ad
Depressed
Ad: Meds
Reward: High
Depressed
Ad: Party
Reward: Low


Not Depressed
Ad: None
Reward: None
Show Meds ad
Show Party ad
Not Depressed
Ad: Meds
Reward: Low
Not Depressed
Ad: Party
Reward: High

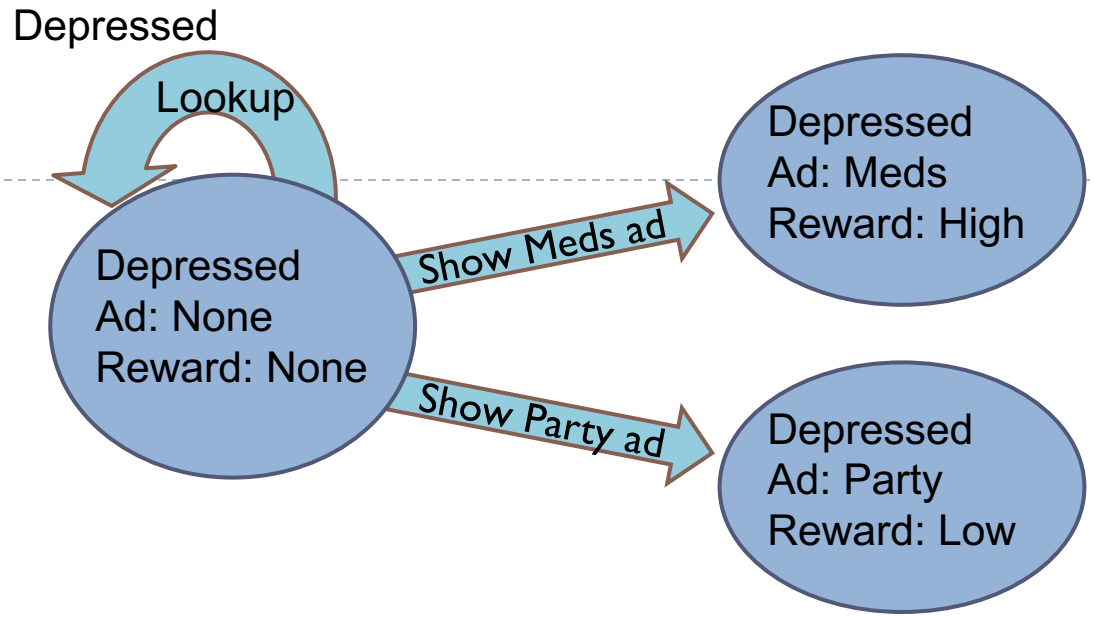
Depressed Case



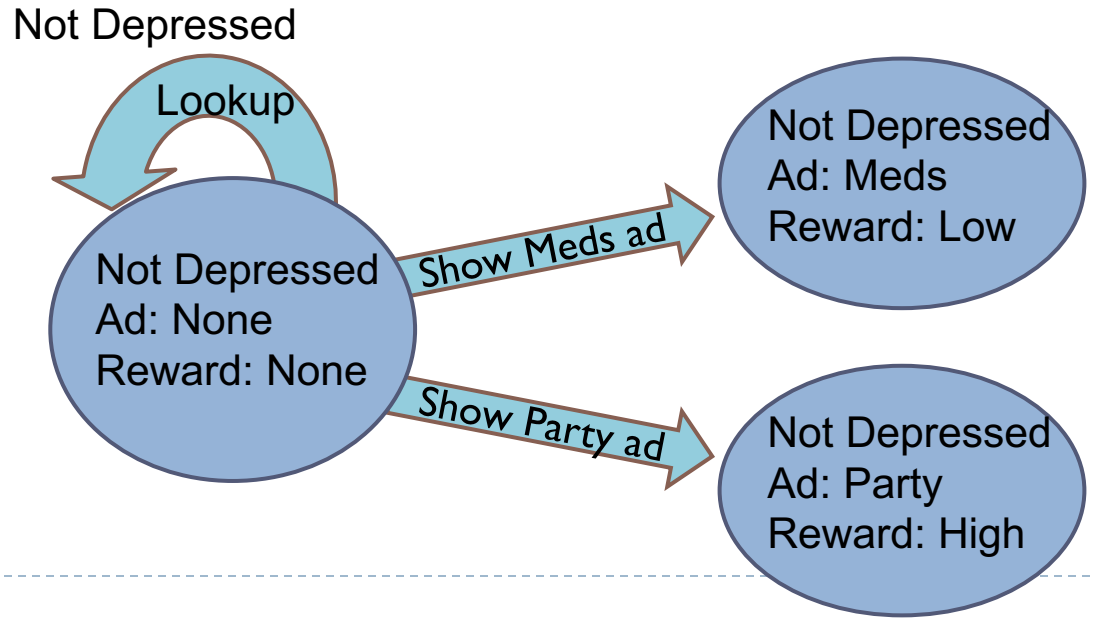
Not Depressed Case



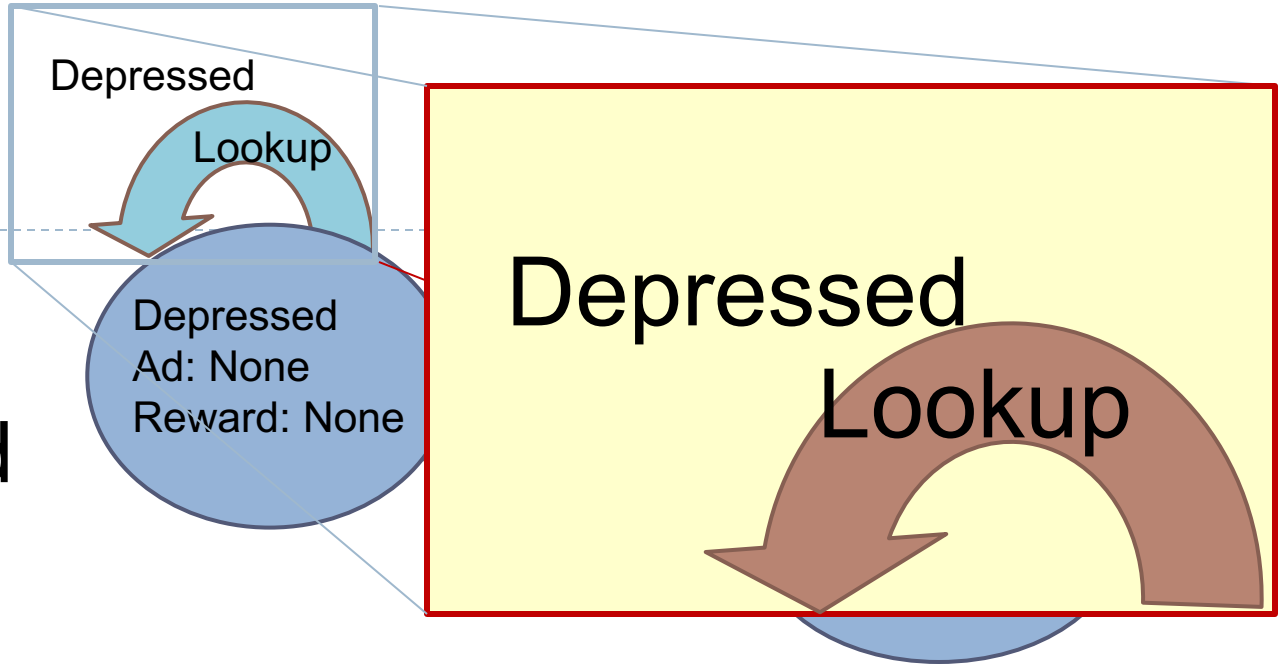
Depressed Case



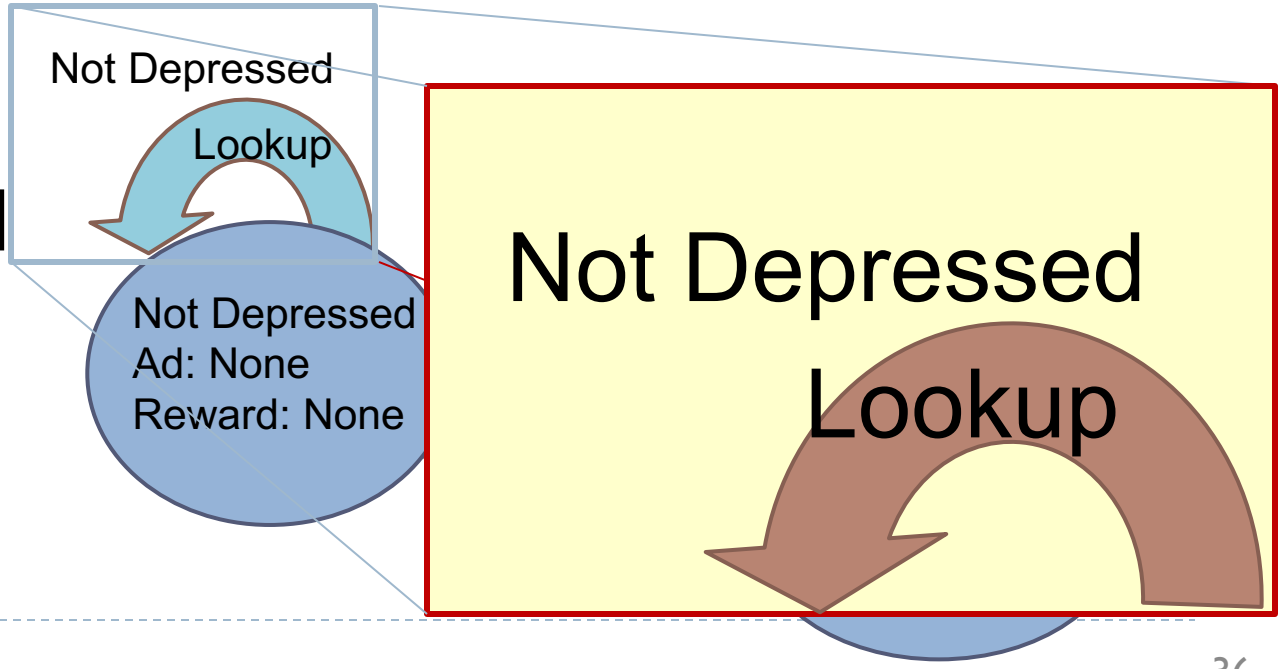
Not Depressed Case

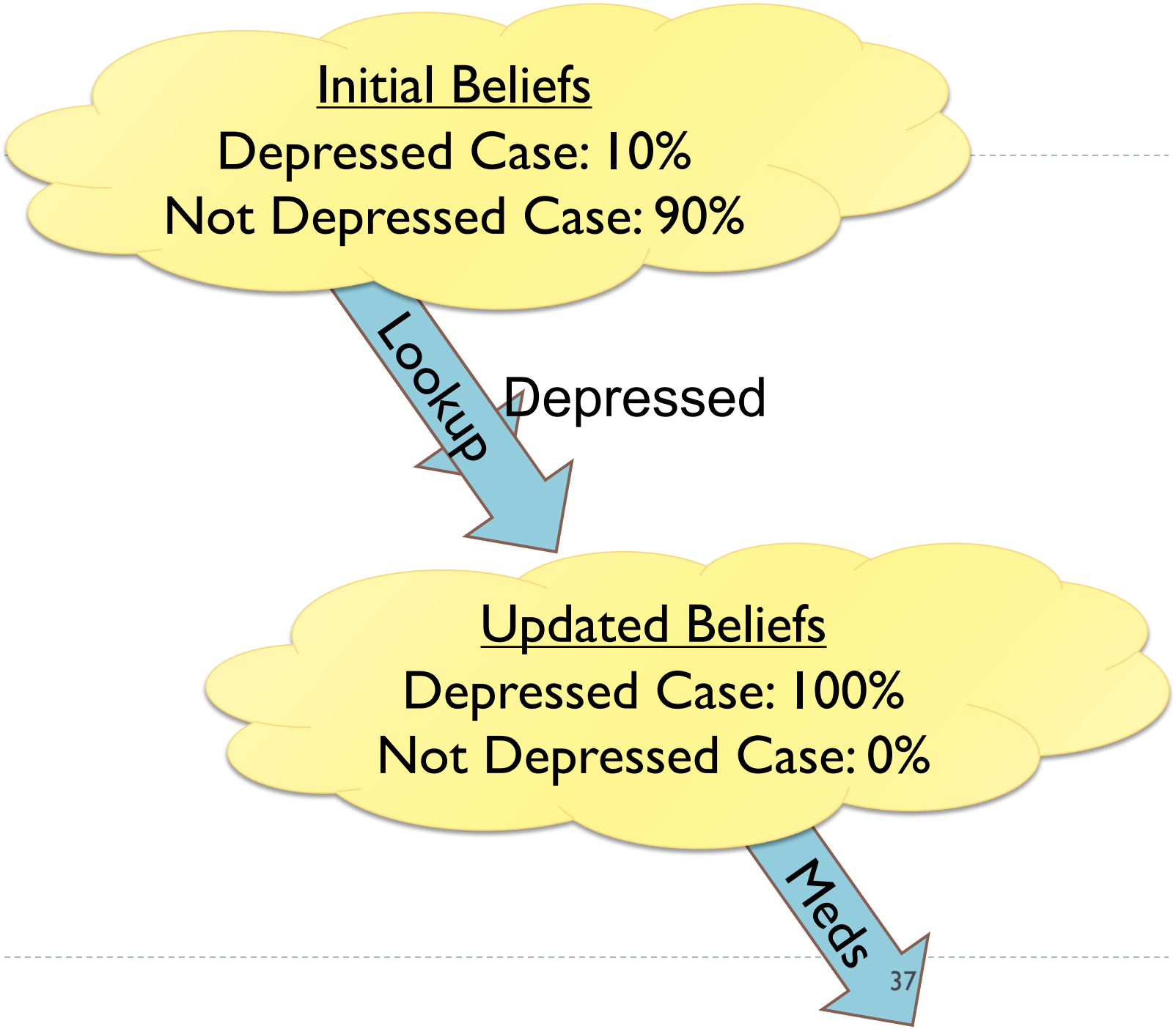


Depressed Case

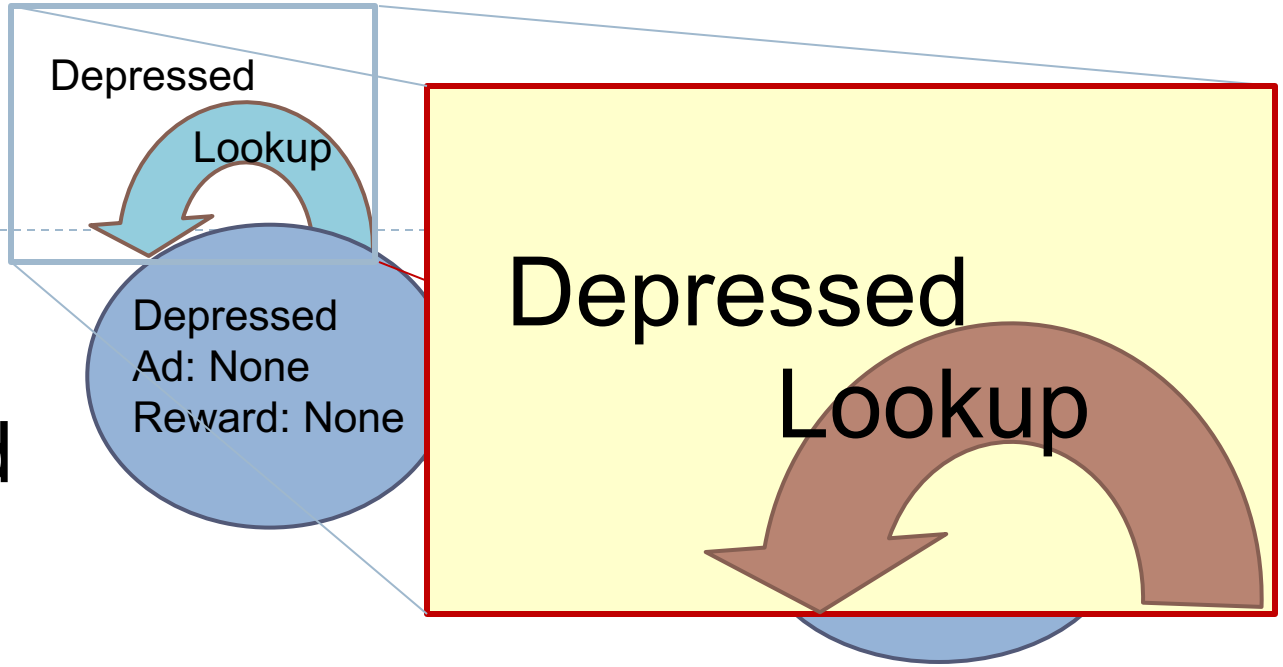


Not Depressed Case

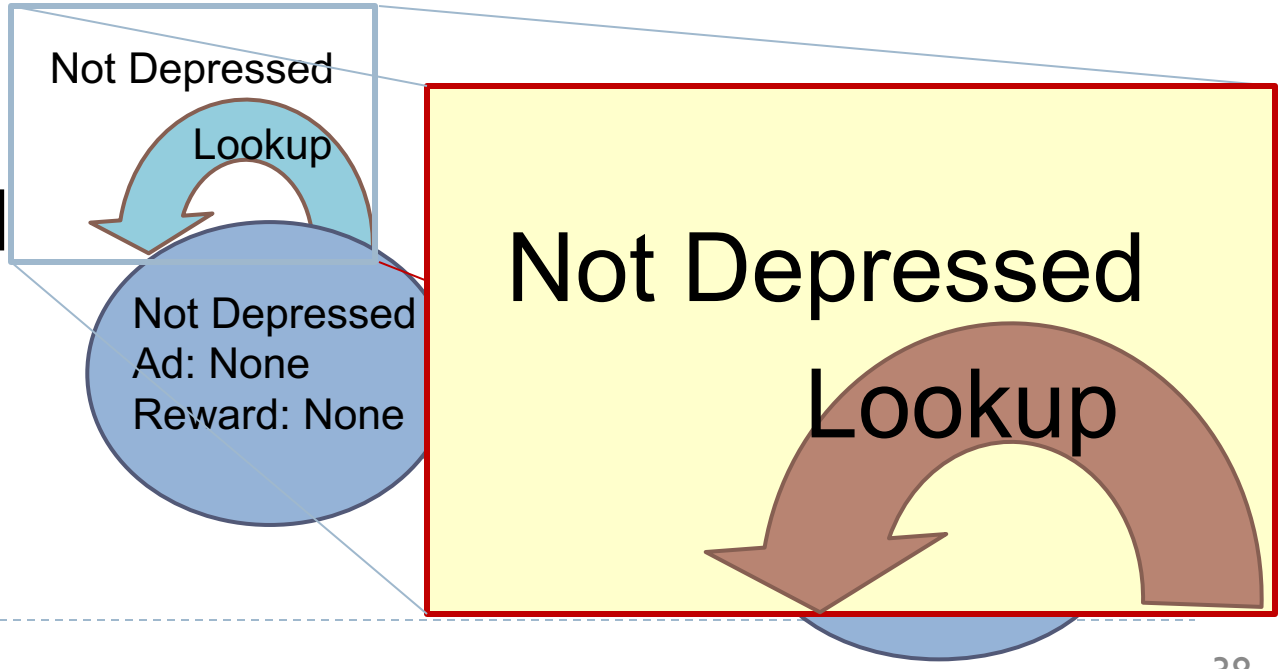



Initial Beliefs
Depressed Case: 10%
Not Depressed Case: 90%
Lookup
Depressed
Updated Beliefs
Depressed Case: 100%
Not Depressed Case: 0%
Meds

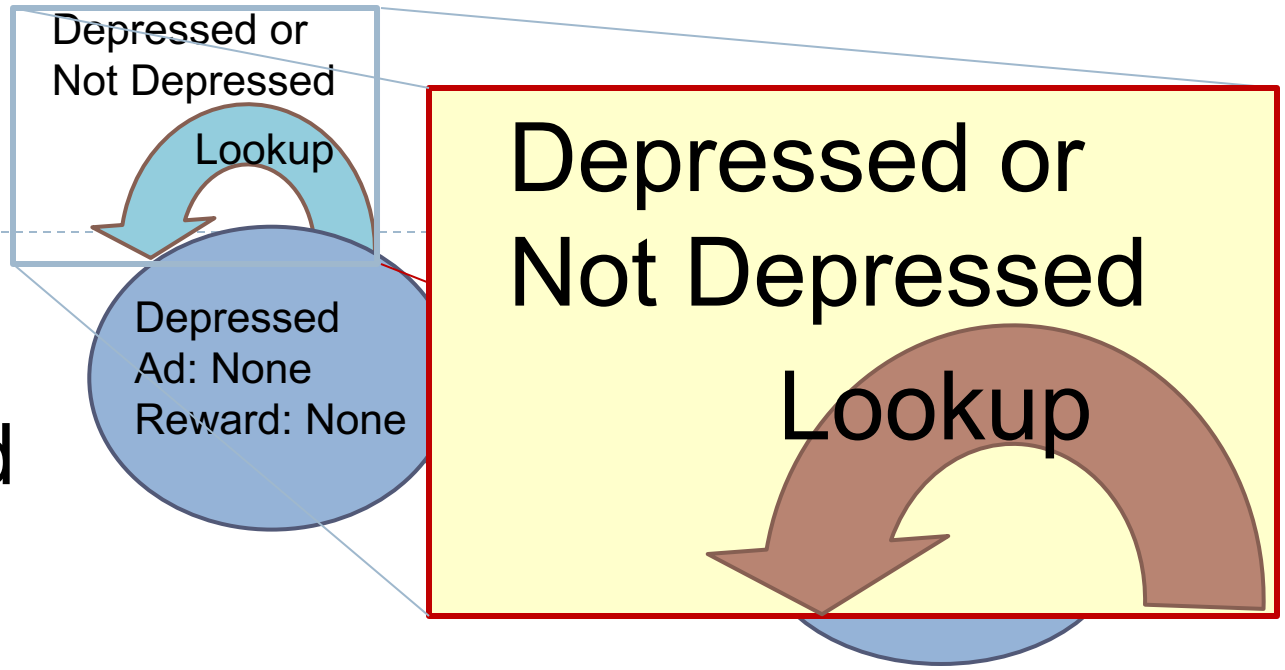
Depressed Case



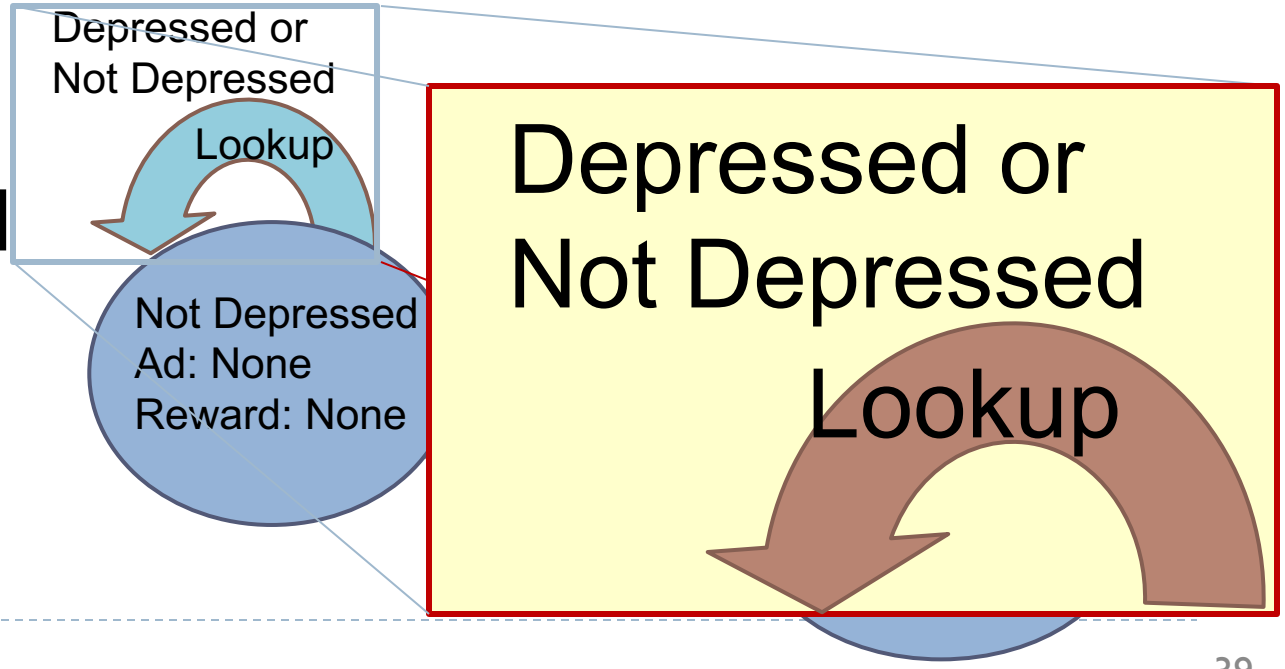
Not Depressed Case

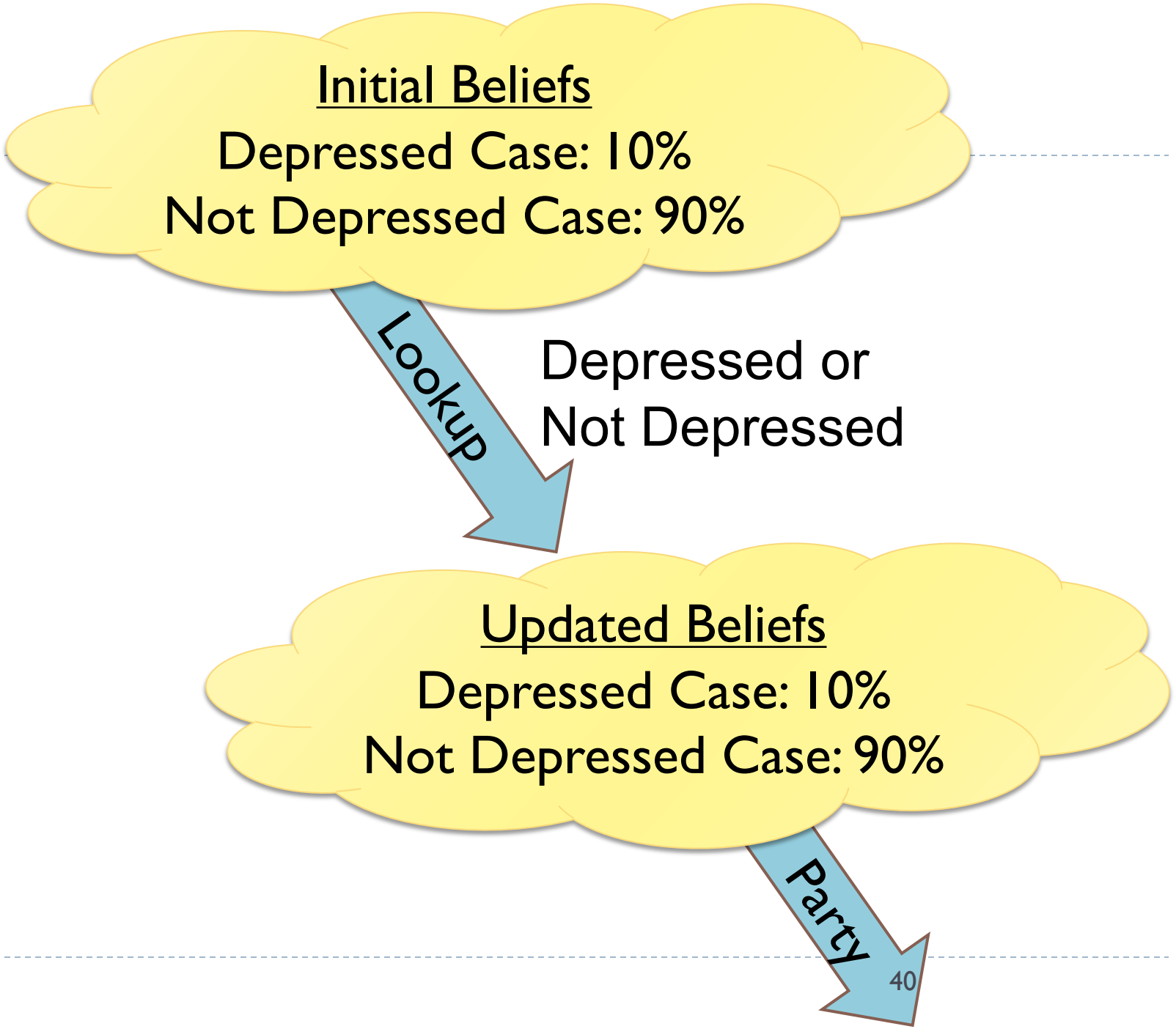


Depressed Case

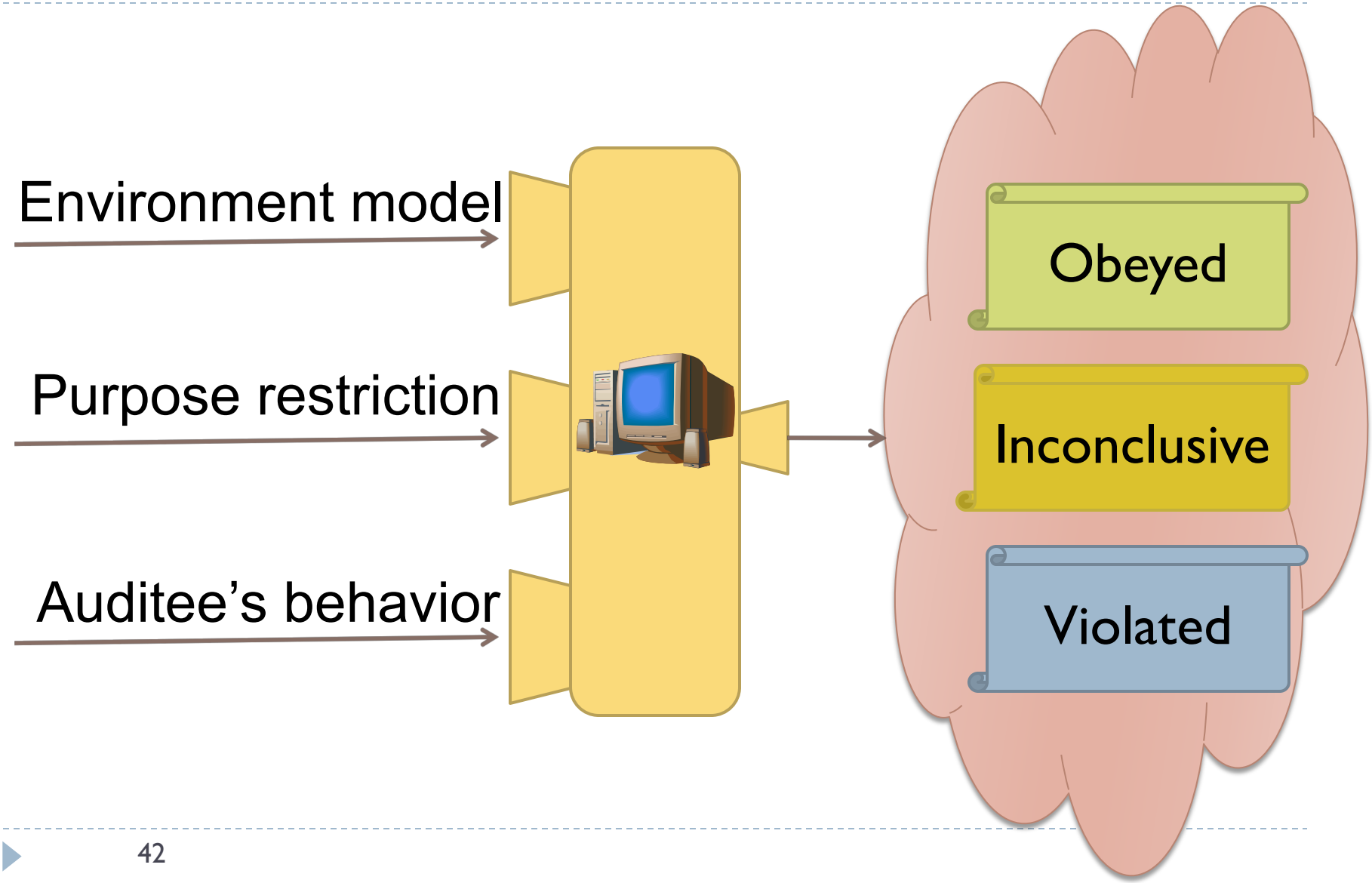


Not Depressed Case

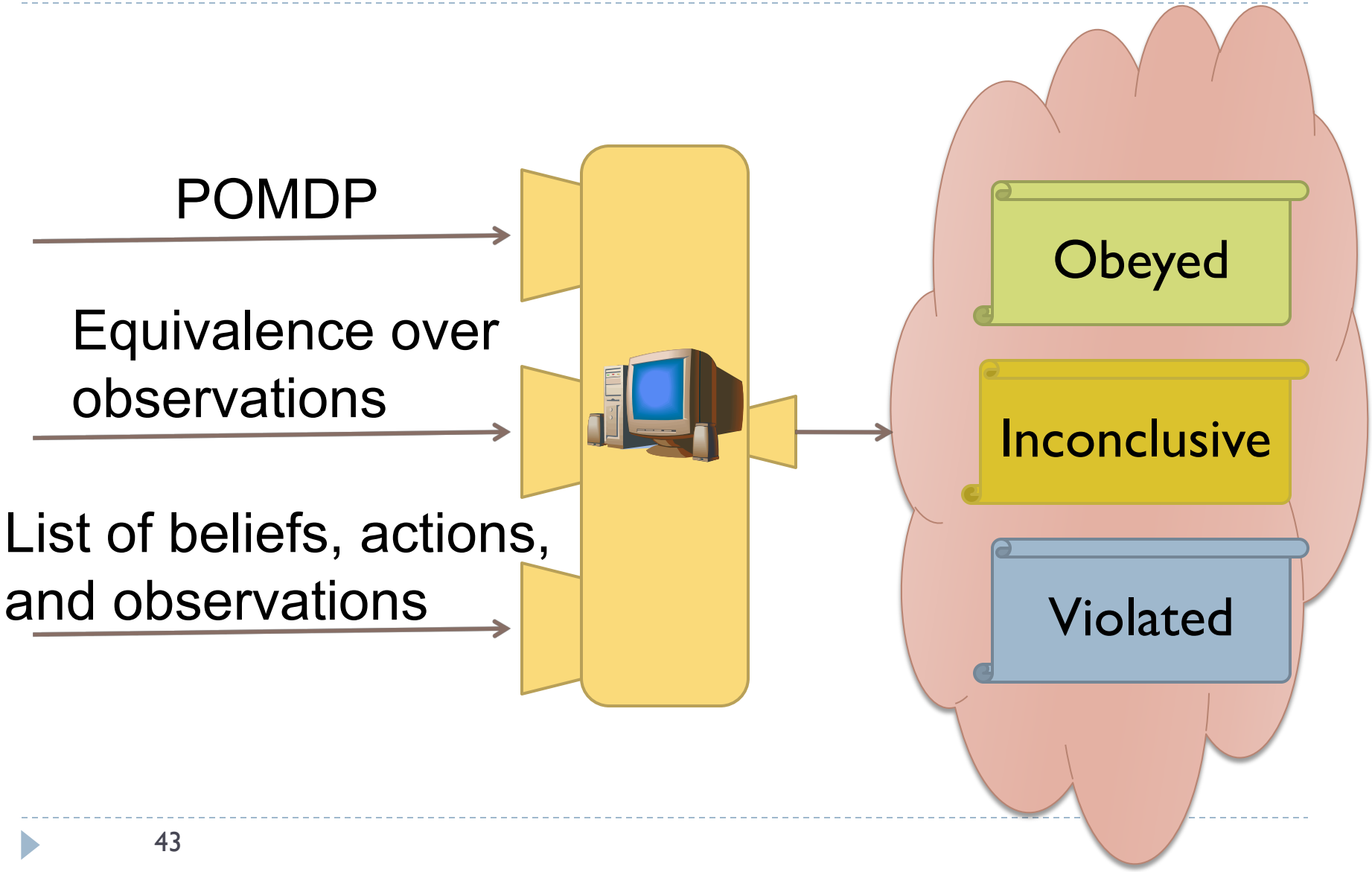



Initial Beliefs
Depressed Case: 10%
Not Depressed Case: 90%
Lookup
Depressed or
Not Depressed
Updated Beliefs
Depressed Case: 10%
Not Depressed Case: 90%
Party

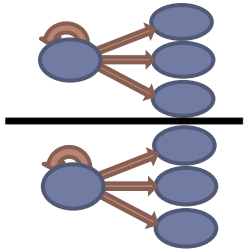
Auditing


Environment model
Purpose restriction
Auditee's behavior
Obeyed
Inconclusive
Violated

Auditing

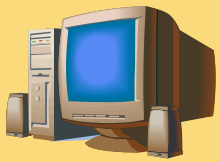

POMDP
Equivalence over observations
List of beliefs, actions, and observations
Obeyed
Inconclusive
Violated

Auditing



Depressed ≡
Not Depressed

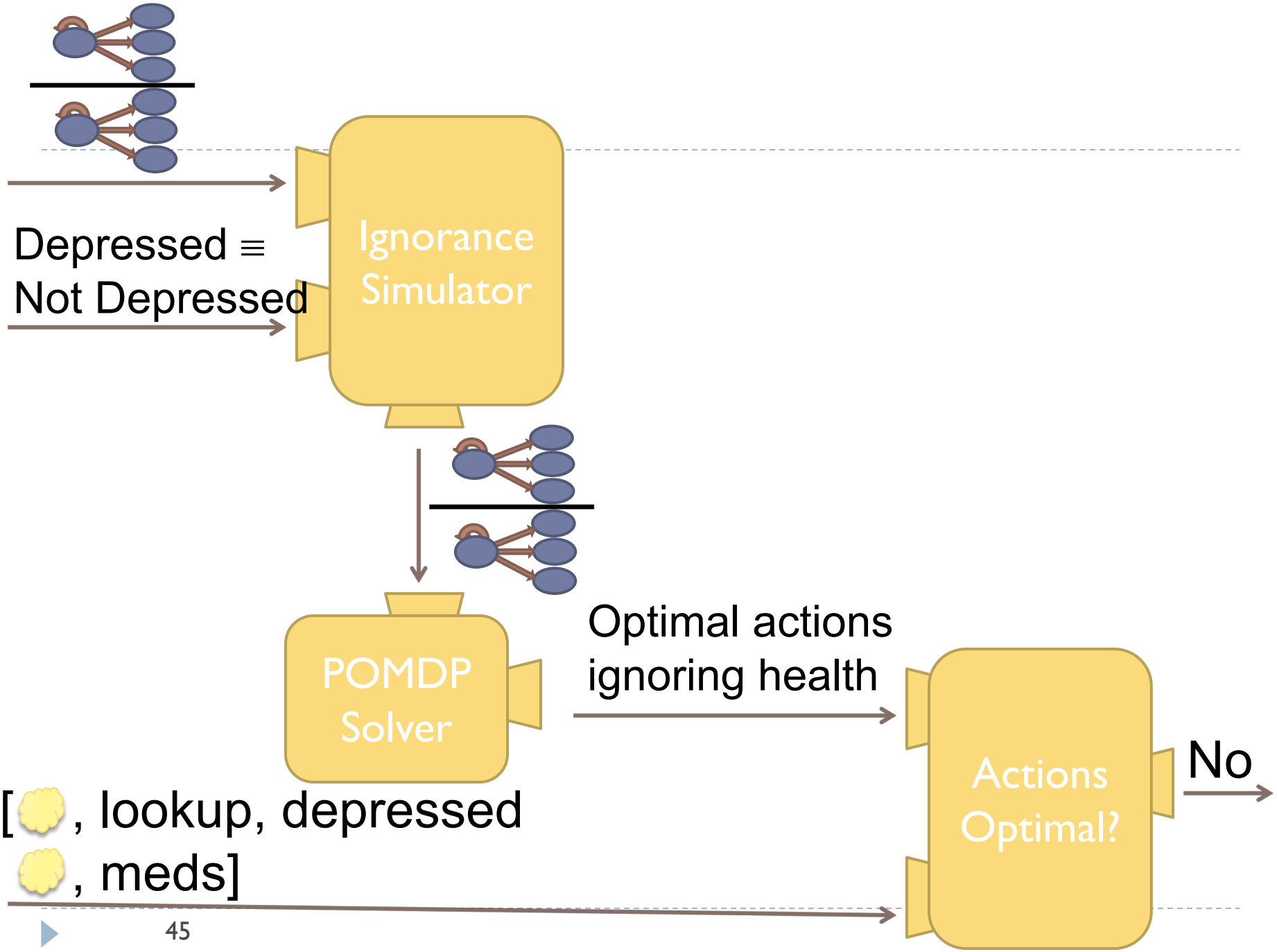
[, lookup, depressed
, meds]



Obeyed

Inconclusive

Violated


Depressed ≡
Not Depressed
Ignorance Simulator
POMDP Solver
Optimal actions ignoring health
Actions Optimal?
No
[, lookup, depressed
, meds]

Implications

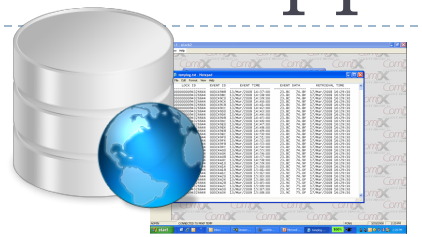
- The actions were not for the purpose of marketing without using health data
  - Violates: "marketing without using health data"
- Either (1) used health data for marketing or (2) performed actions for some other purpose
  - In case (1) violates: "health data not for marketing"

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)
- This work provides a semantic foundation
- Shows the expressiveness of each approach

Summary: Audit Approach

Privacy Policy



Organizational audit log

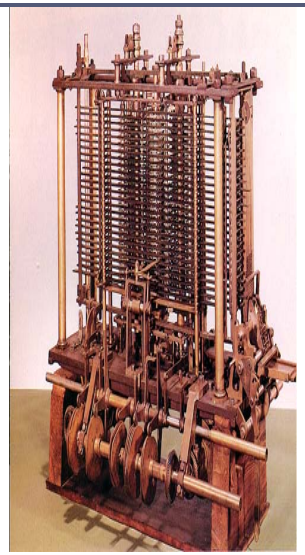
Automated audit for black-and-white policy concepts

Complete formalization of HIPAA, GLBA

$$\mathbf{G}\,\Big(\forall p_1, p_2, m.\ \mathsf{send}(p_1, p_2, m) \supset (\forall d, u, q, t.\ (m = \mathrm{info}(d, u)) \wedge \mathsf{contains}(m, q, t) \supset (\bigvee_i \varphi_i^+) \wedge (\bigwedge_j \varphi_j^-)) \wedge (\forall t.\ (m = \mathrm{req\_for\_access}(p_1, t)) \supset \varphi^-_{\mathtt{164.524b2i'}} \wedge \varphi^-_{\mathtt{164.524b2ii'}})\Big)$$

Computer-readable privacy policy

Environment Model



Audit

Detect policy violations

Oracles to audit for grey policy concepts