18734: Foundations of Privacy

Information Flow Experiments + Introduction to Machine Learning

Giulia Fanti
Based on slides by Anupam Datta
CMU

Fall 2019

Administrative

- Project proposals due on Friday, Sept 20!
  - 5 pm ET/2 pm PT
  - Submit on Gradescope
- HW2 due next Friday, Sept 27
  - 5 pm ET/2 pm PT
- Reminder: my OH this week TIME CHANGE
  - 11:30-1pm ET/ 8:30-10 at PT
  - SV: Join the Google hangout on the course website

10-minute quiz

- On Canvas

- Please take survey
  - https://forms.gle/D5ma1HABAq42zhxf9
  - Sent out link on Canvas

Last time

- Almost sure convergence
- Permutation test

Permutation test

- Document cam example

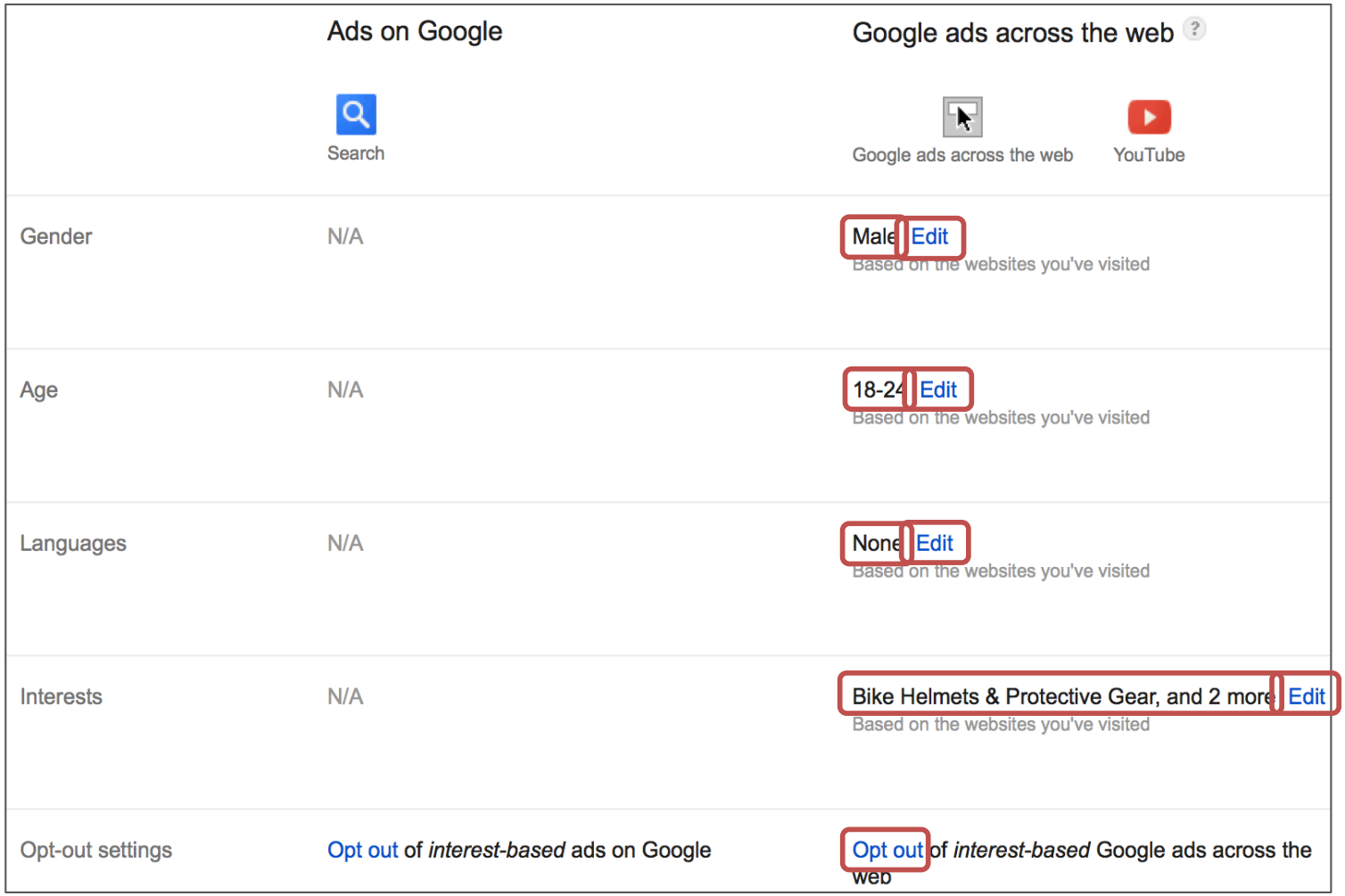
Information Flow Experiments on Personalized Ads and Ad Settings

Amit Datta, CMU
Michael Tschantz, ICSI
Anupam Datta, CMU

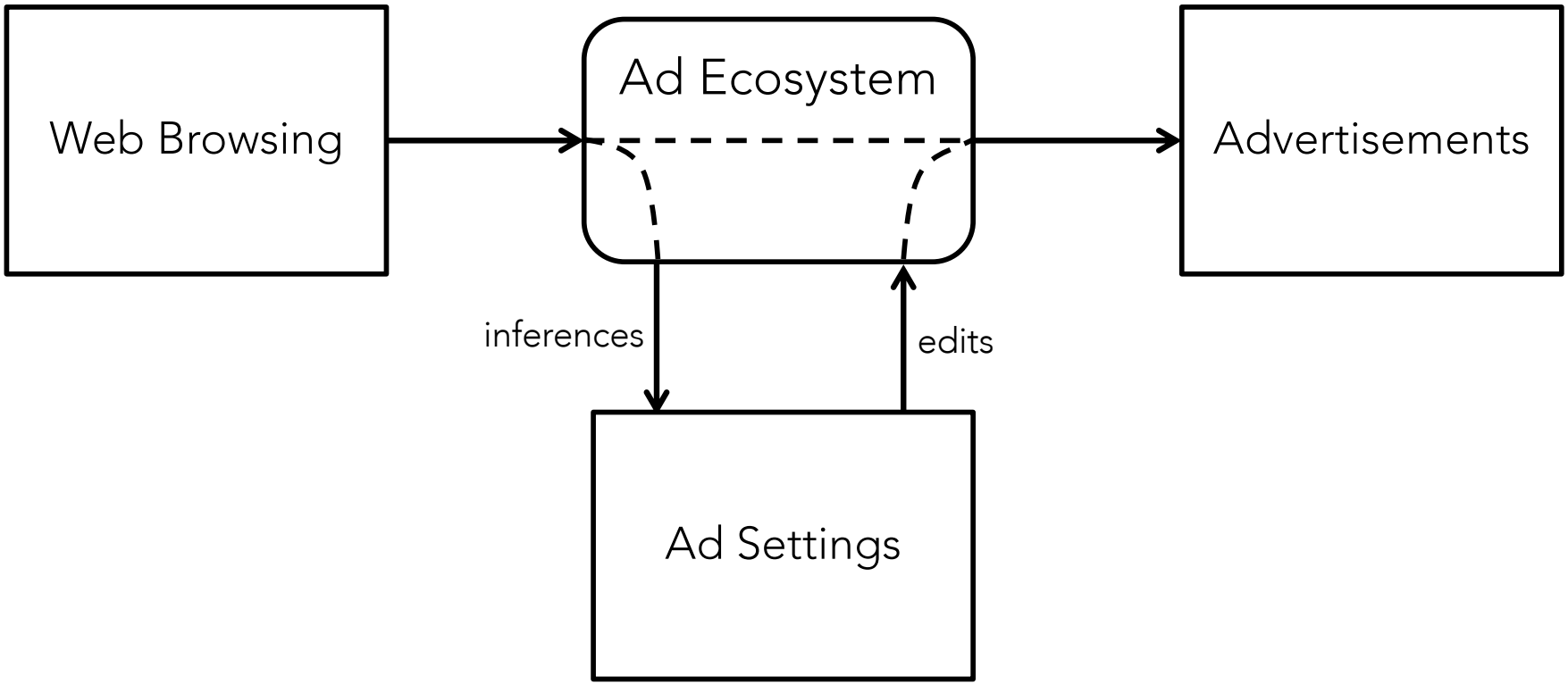
Privacy Enhancing Technology Symposium (PETS) 2015

Ad Settings

www.google.com/settings/ads



Model of Interactions



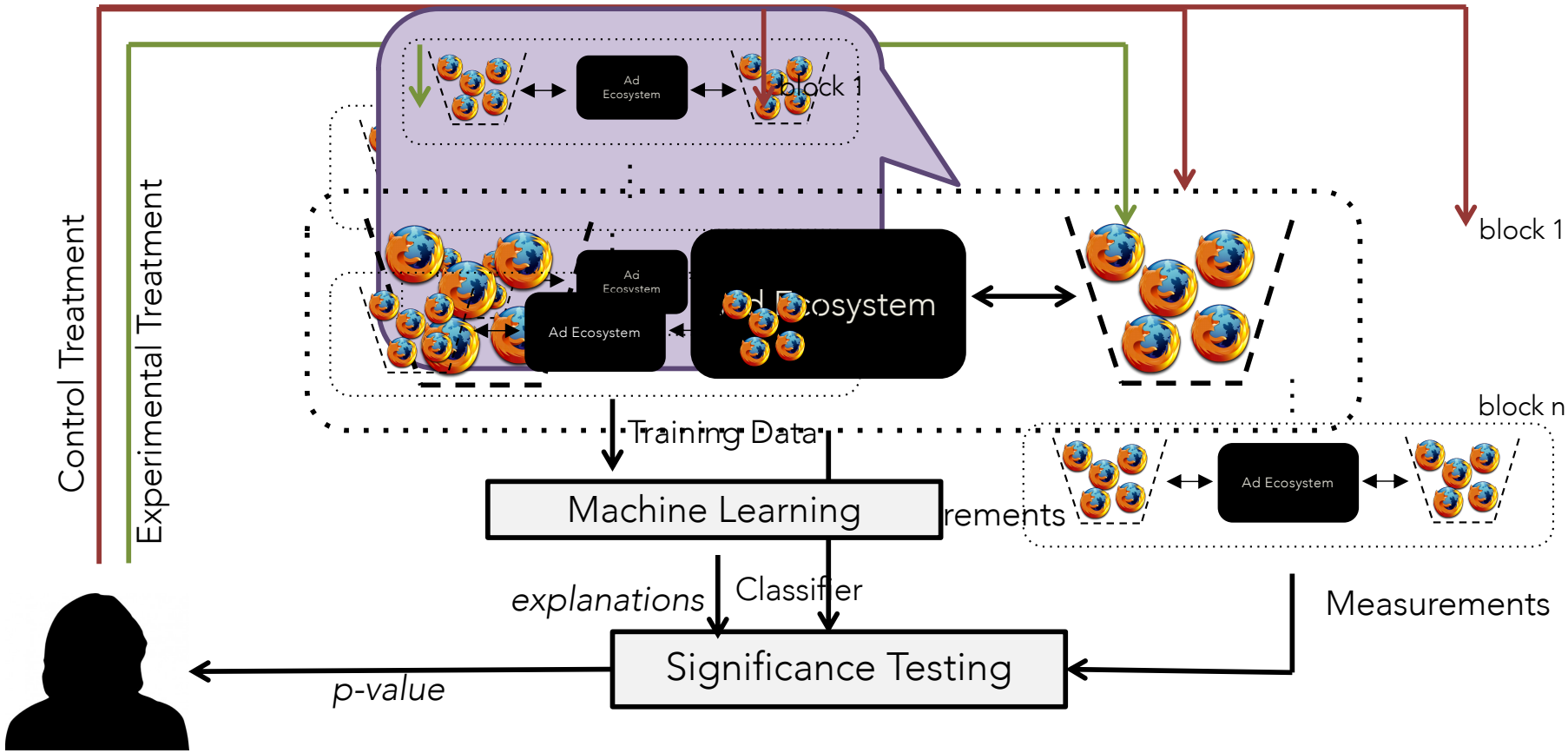
Scaling Challenges

- Limited samples

- Selection of test statistic

Test Statistic

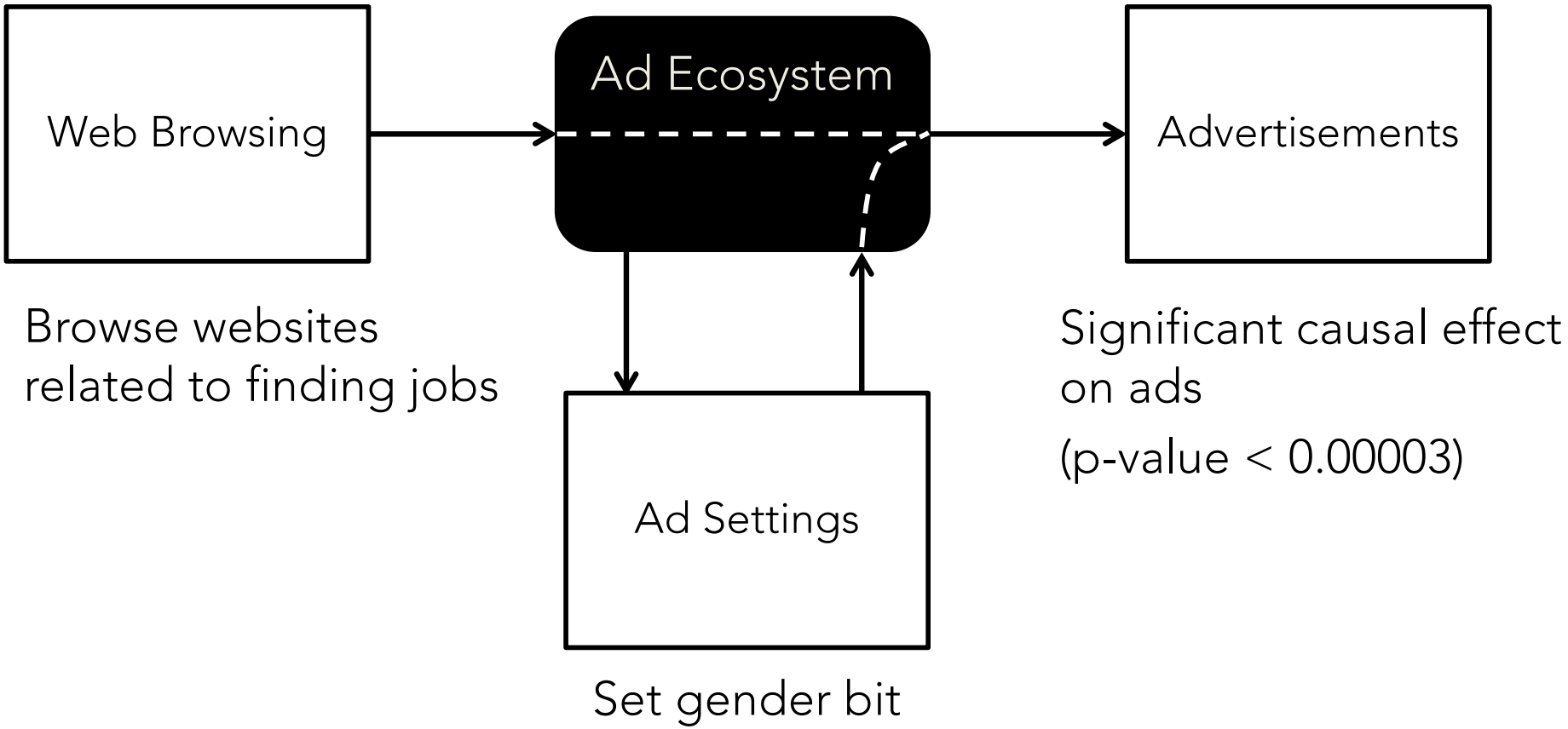
AdFisher Methodology



We study three properties on the Ad Ecosystem

- Discrimination
- Transparency
- Choice

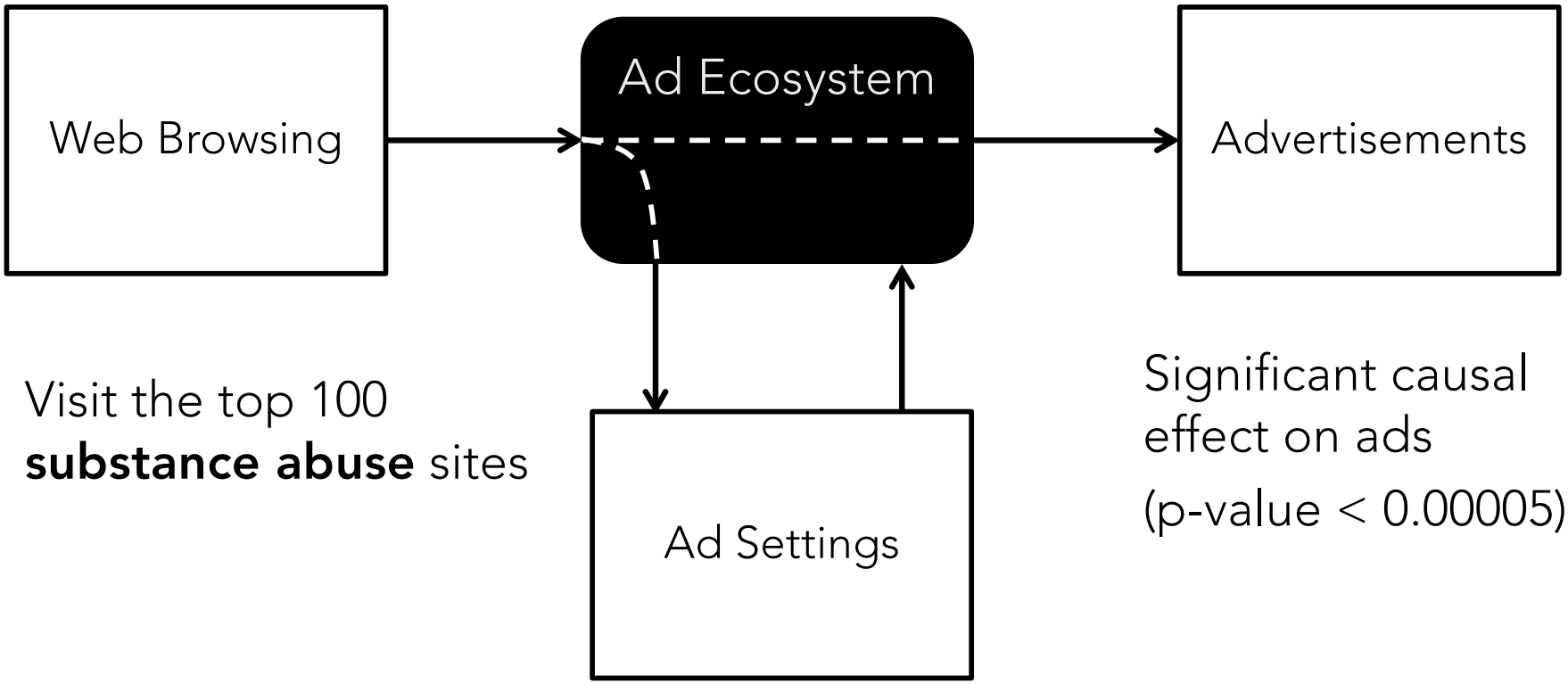
Discrimination



Discrimination Explanations

Female Group	Male Group
Jobs (Hiring Now) www.jobsinyourarea.co 45 vs. 8	$200k+ Jobs - Execs Only careerchange.com 311 vs. 1816
4Runner Parts Service www.westernpatoyotaservice.com 36 vs. 5	Find Next $200k+ Job careerchange.com 7 vs. 36
Criminal Justice Program www3.mc3.edu/Criminal+Justice 29 vs. 1	Become a Youth Counselor www.youthcounseling.degreeleap.com 0 vs. 310

Transparency



Visit the top 100 **substance abuse** sites

Significant causal effect on ads

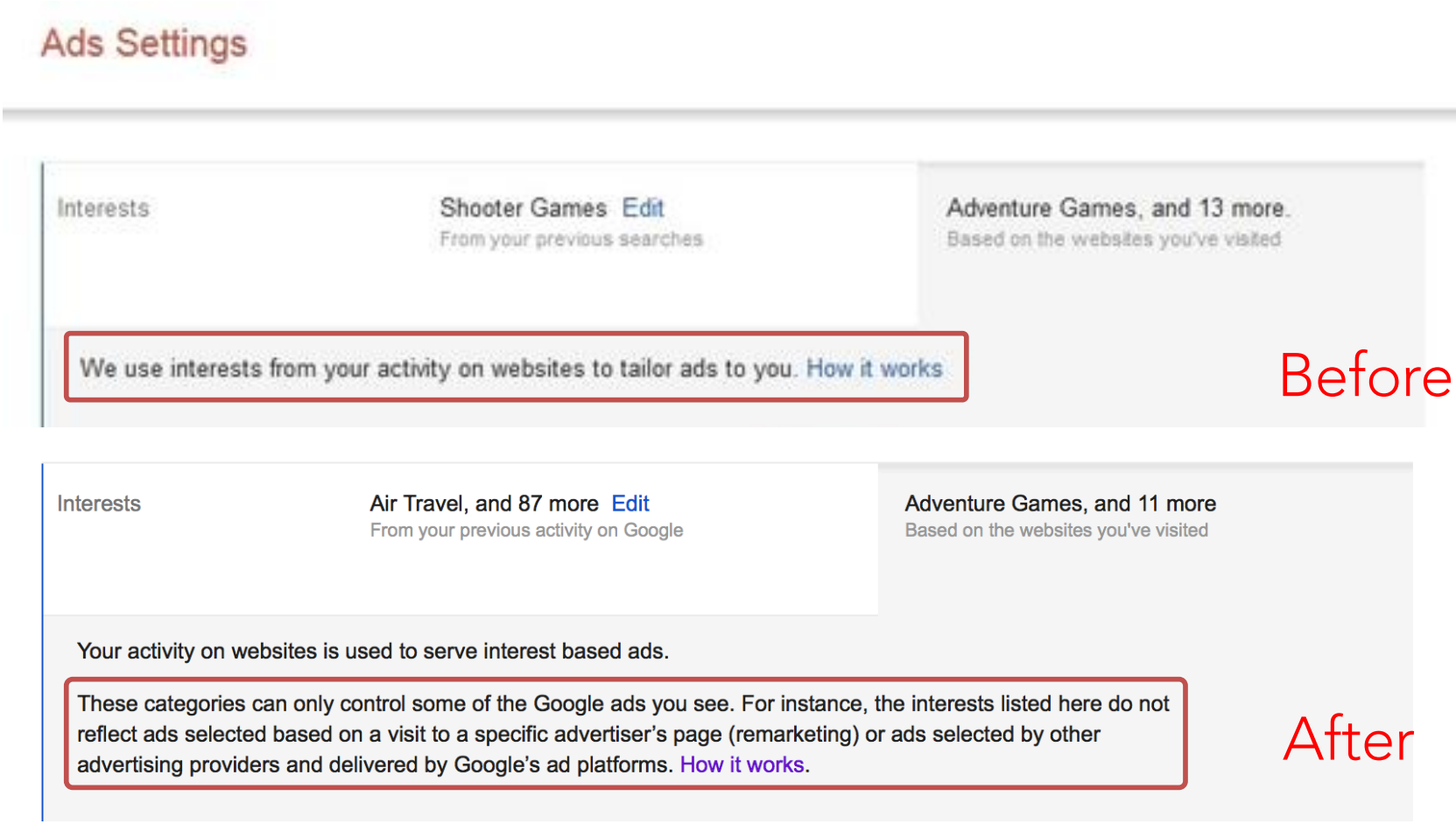
(p-value < 0.00005)

No effect on ad settings

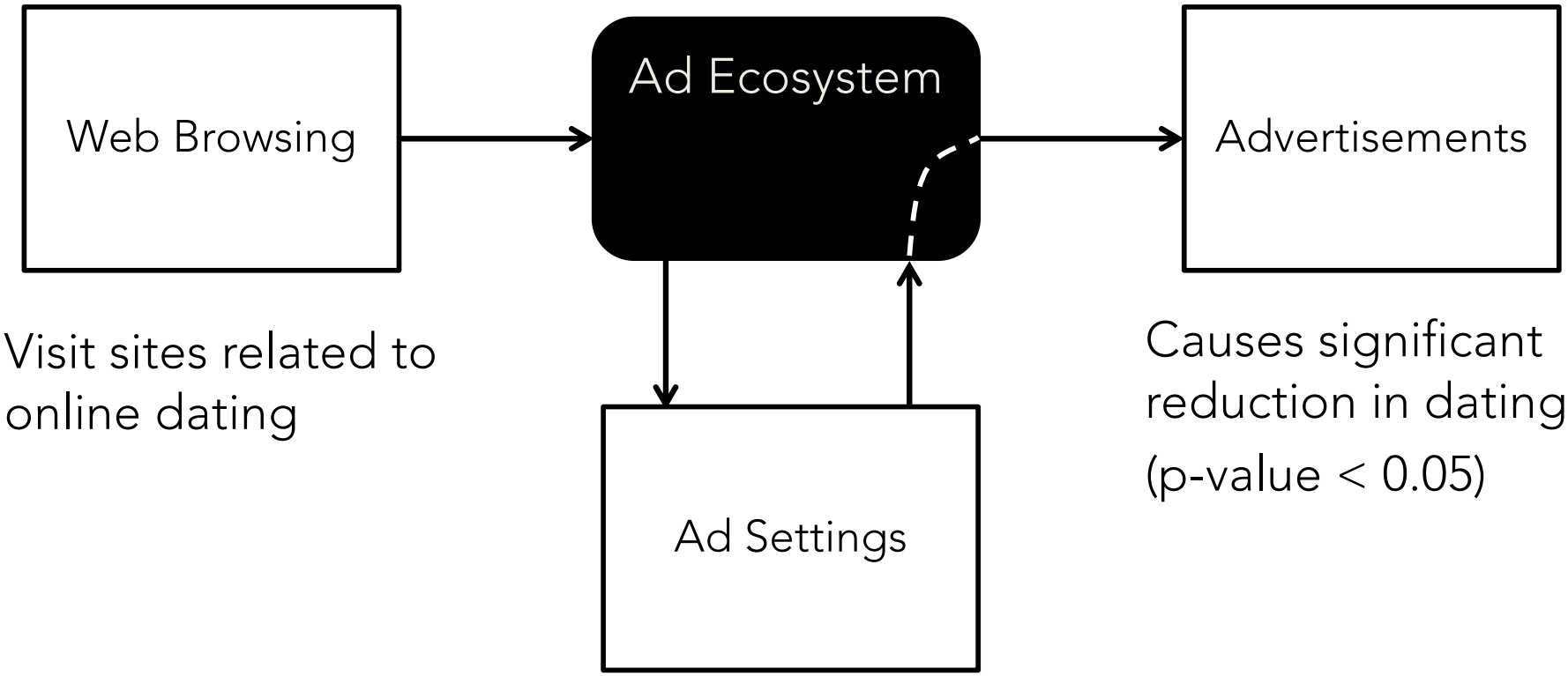
Transparency Explanations

Substance Abuse Visitors	Control Group
The Watershed Rehab www.thewatershed.com/Help 2276 vs. 0	Alluria Alert www.bestbeautybrand.com 0 vs. 9
Watershed Rehab www.thewatershed.com/Rehab 362 vs. 0	Best Dividend Stocks dividends.wyattresearch.com 24 vs. 54
The Watershed Rehab (none) 771 vs. 0	10 Stocks to Hold Forever www.streetauthority.com 76 vs. 118

Additional notice on Ad Settings



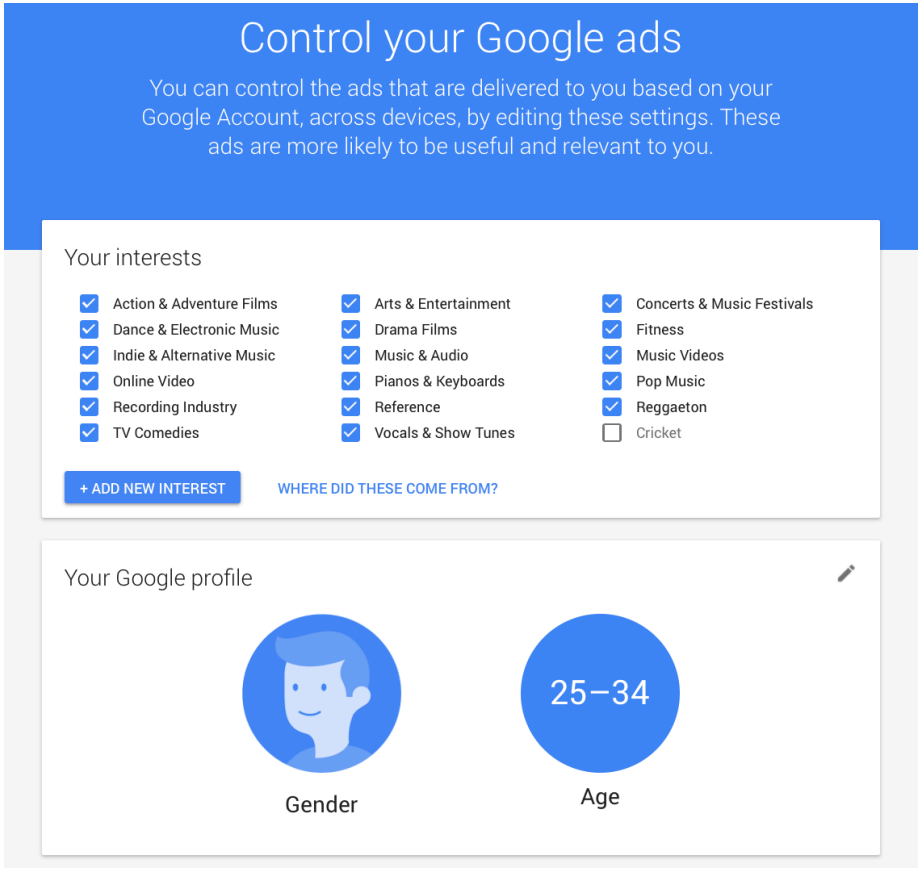
Choice


Web Browsing
Ad Ecosystem
Advertisements
Visit sites related to online dating
Causes significant reduction in dating ads
(p-value < 0.05)
Ad Settings
Remove interests related to online dating

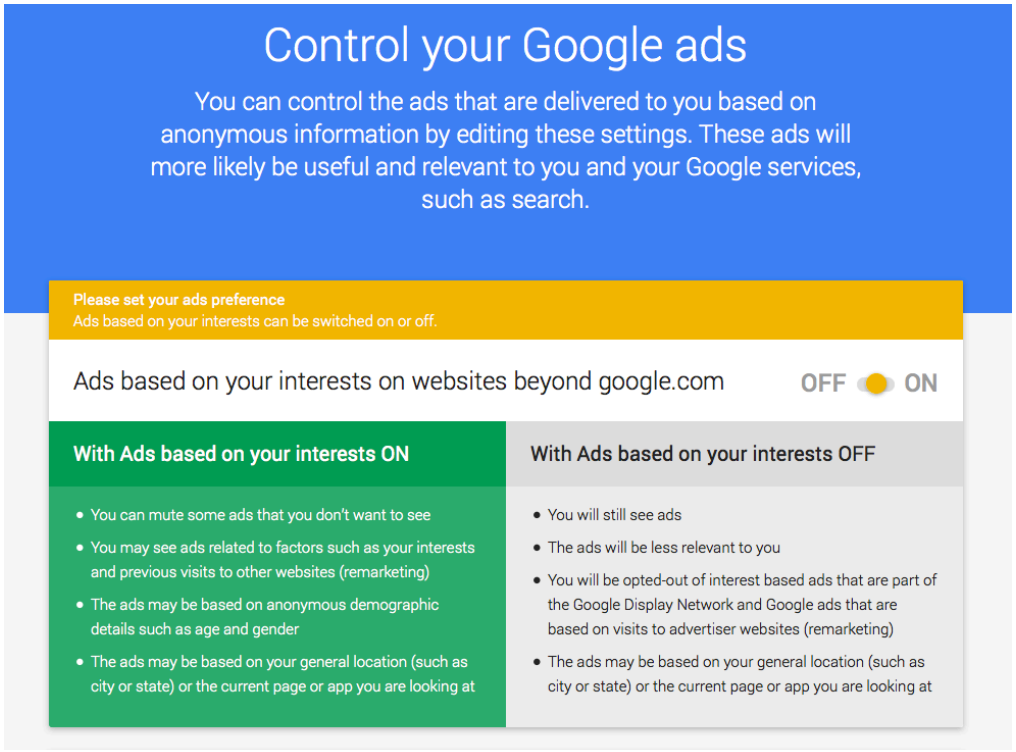
Choice Explanations

Keep Dating Interest	Remove Dating Interest
Are You Single? www.zoosk.com/Dating 2433 vs. 78	Car Loans w/ Bad Credit www.car.com/Bad-Credit-Car-Loan 8 vs. 37
Top 5 Online Dating Sites www.consumer-rankings.com/Dating 408 vs. 13	Individual Health Plans www.individualhealthquotes.com 21 vs. 46
Why can't I find a date? www.gk2gk.com 51 vs. 5	Crazy New Obama Tax www.endofamerica.com 22 vs. 51

Possible Impact on Ad Settings



Possible Impact on Ad Settings



Conclusions

1. Findings of discrimination, lack of transparency, and choice.

2. Scalable methodology
   - Blocked design
   - Automated selection of test statistic

3. AdFisher is freely available online:
   github.com/tadatitam/info-flow-experiments

End of Unit 1

- Privacy perspective
  - Ways to audit privacy policies
  - Insider
    - Enforcing use restrictions (MDPs)
    - Legalease + Grok
  - Outsider
    - XRay
    - Information Flow experiments
- Tools/concepts we have seen
  - Randomized sampling for group testing
  - Markov decision processes (MDPs)
  - Statistical significance tests
  - Lattices