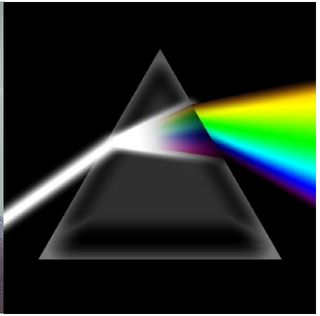
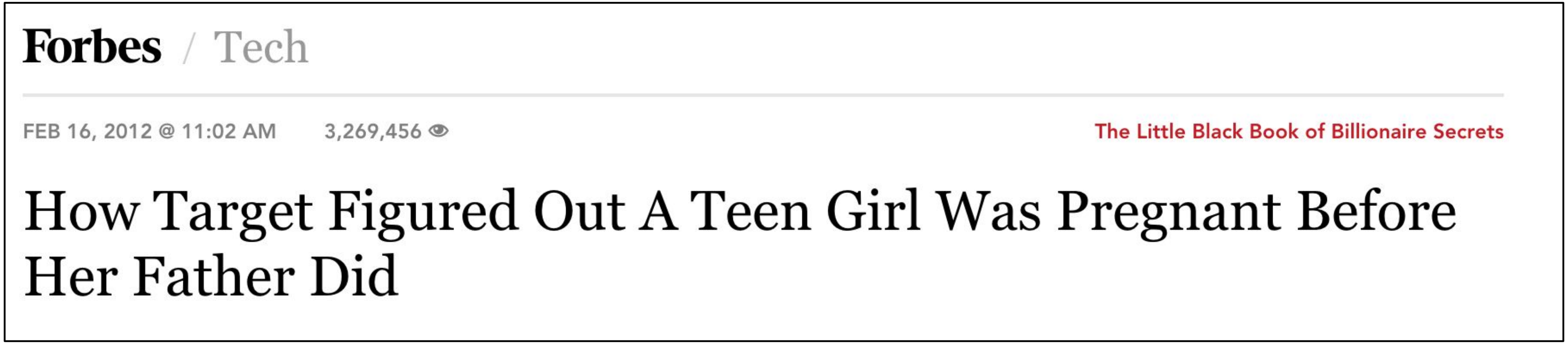
Use Privacy in Data-Driven Systems

Theory and Experiments with Machine Learnt Programs

Anupam Datta, Matt Fredrikson, Gihyuk Ko, Piotr (Peter) Mardziel, Shayak Sen



Accountable Systems Lab
fairlyaccountable.org

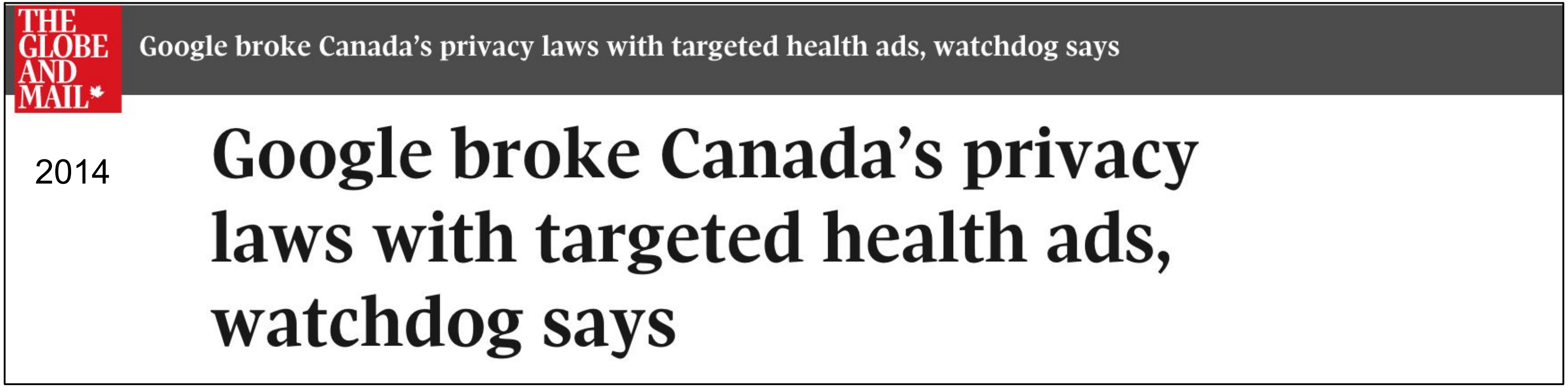


Forbes / Tech

FEB 16, 2012 @ 11:02 AM 3,269,456

The Little Black Book of Billionaire Secrets

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did



THE GLOBE AND MAIL

Google broke Canada's privacy laws with targeted health ads, watchdog says

2014

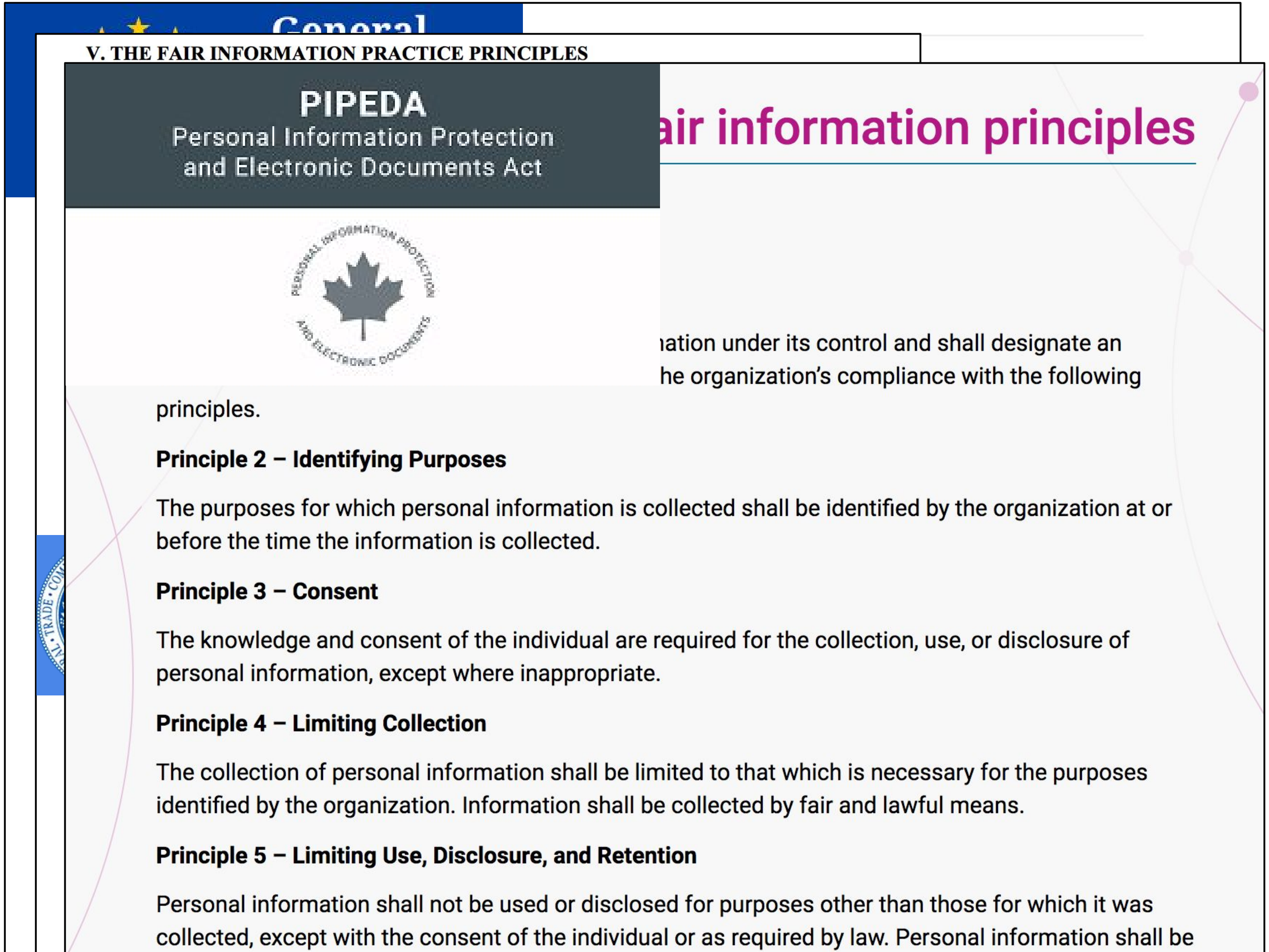
Google broke Canada's privacy laws with targeted health ads, watchdog says

What is *use privacy*?

Can ◉ ***infer*** health information?

Yes

Should ◉ ***use*** health information (for purpose P)?



General

V. THE FAIR INFORMATION PRACTICE PRINCIPLES

PIPEDA
Personal Information Protection
and Electronic Documents Act

air information principles

ation under its control and shall designate an
he organization's compliance with the following
principles.

Principle 2 – Identifying Purposes

The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.

Principle 3 – Consent

The knowledge and consent of the individual are required for the collection, use, or disclosure of personal information, except where inappropriate.

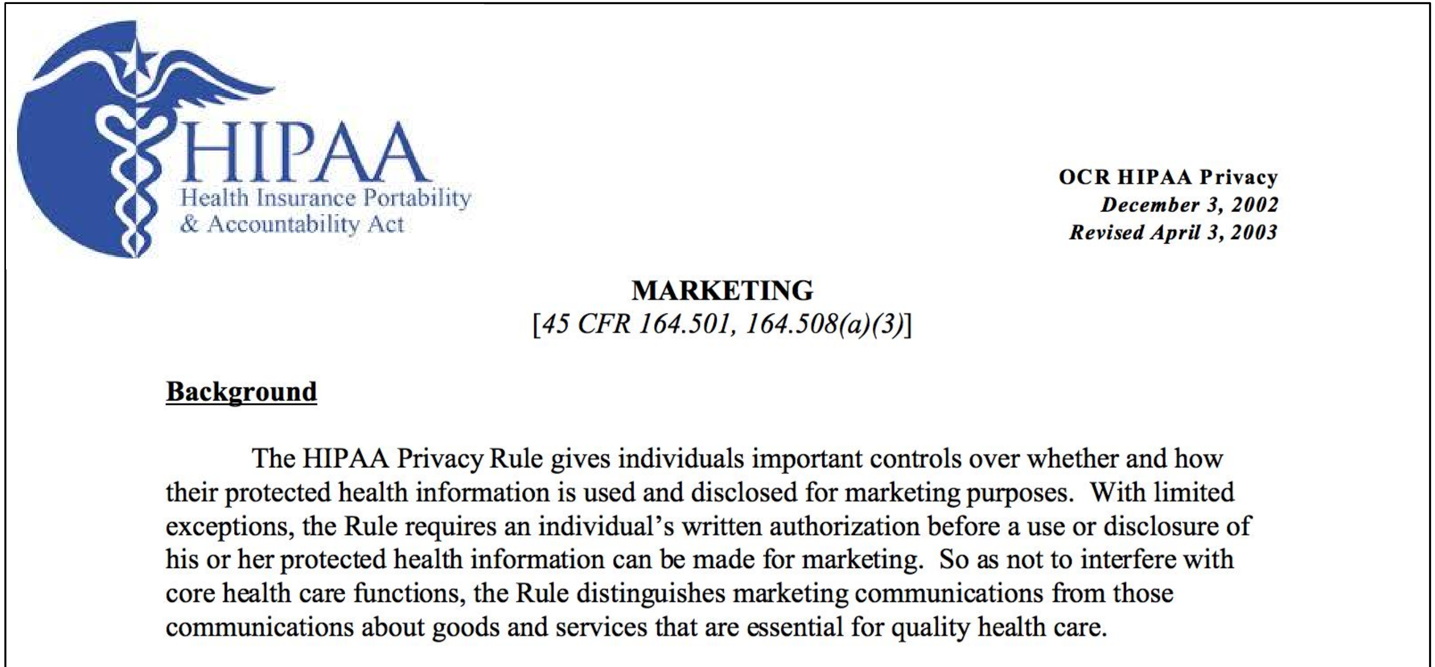
Principle 4 – Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.

Principle 5 – Limiting Use, Disclosure, and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required by law. Personal information shall be

HIPAA: Do not use health information for marketing purposes.



HIPAA
Health Insurance Portability
& Accountability Act

OCR HIPAA Privacy
December 3, 2002
Revised April 3, 2003

MARKETING
[*45 CFR 164.501, 164.508(a)(3)*]

Background

The HIPAA Privacy Rule gives individuals important controls over whether and how their protected health information is used and disclosed for marketing purposes. With limited exceptions, the Rule requires an individual's written authorization before a use or disclosure of his or her protected health information can be made for marketing. So as not to interfere with core health care functions, the Rule distinguishes marketing communications from those communications about goods and services that are essential for quality health care.

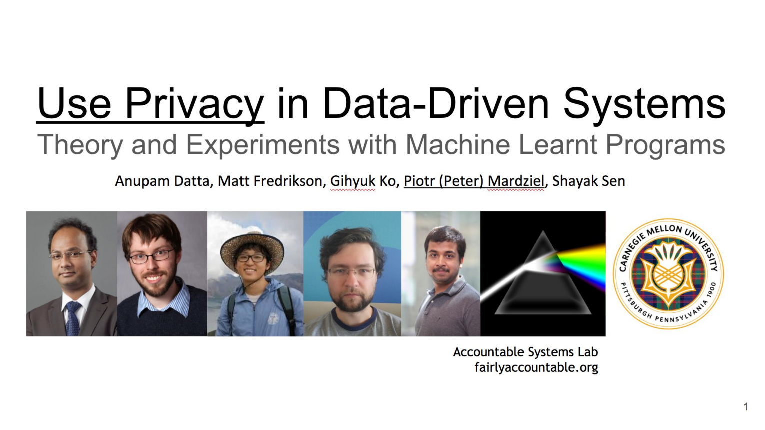
What is *use privacy* protection?

~~Restrict Inference: ***Can*** X ***infer*** private Z?~~ → Difficult ~ Impossible

Should X ***use*** private Z (for purpose P)? ← Legal / Ethical concerns

Restrict Use: ***Does*** X ***use*** private Z? →

Our work: ***Use Privacy***



Use Privacy in Data-Driven Systems

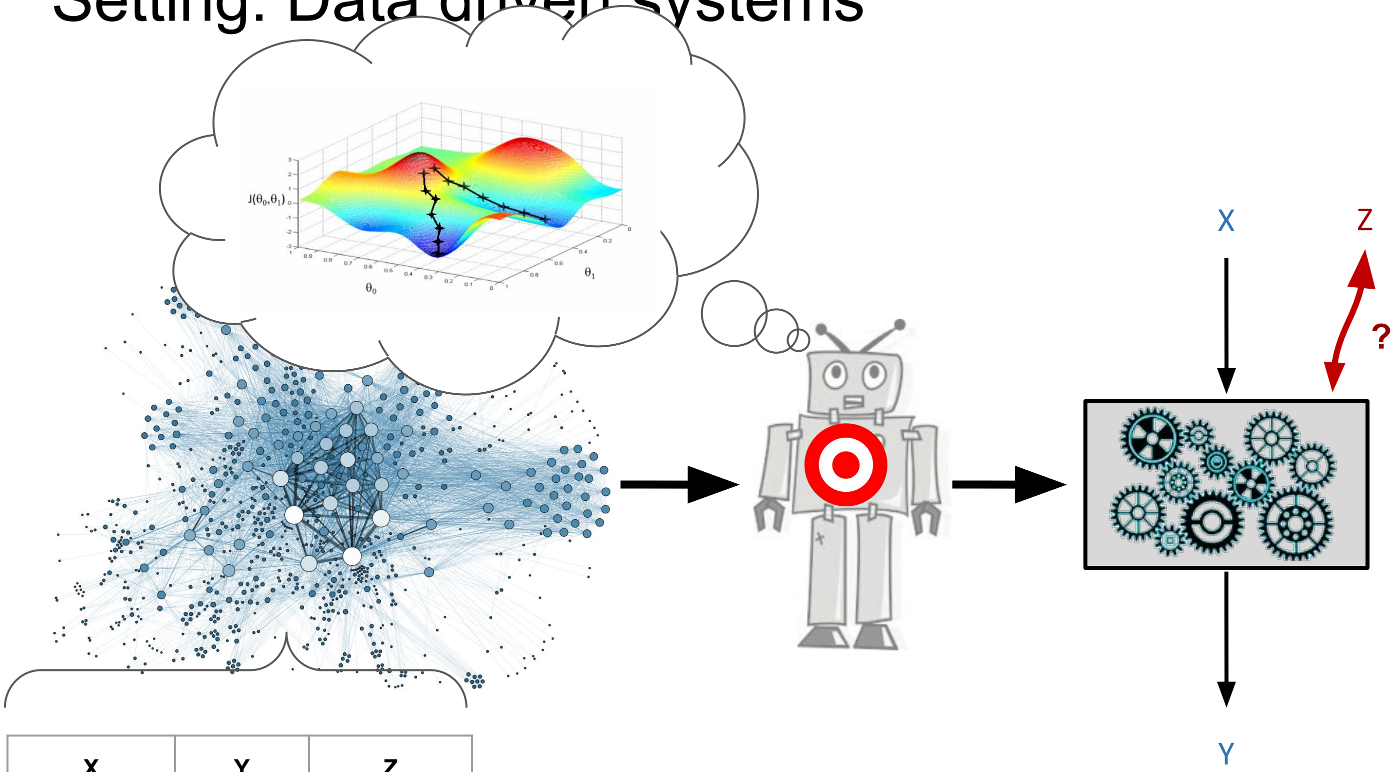
Theory and Experiments with Machine Learnt Programs

Anupam Datta, Matt Fredrikson, Gihyuk Ko, Piotr (Peter) Mardziel, Shayak Sen

Accountable Systems Lab
fairlyaccountable.org

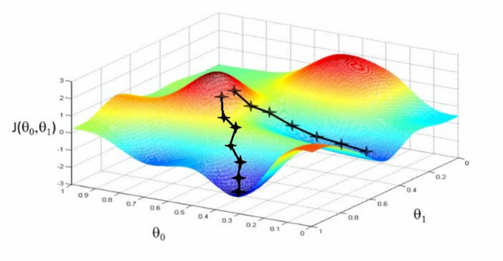
1

Setting: Data driven systems

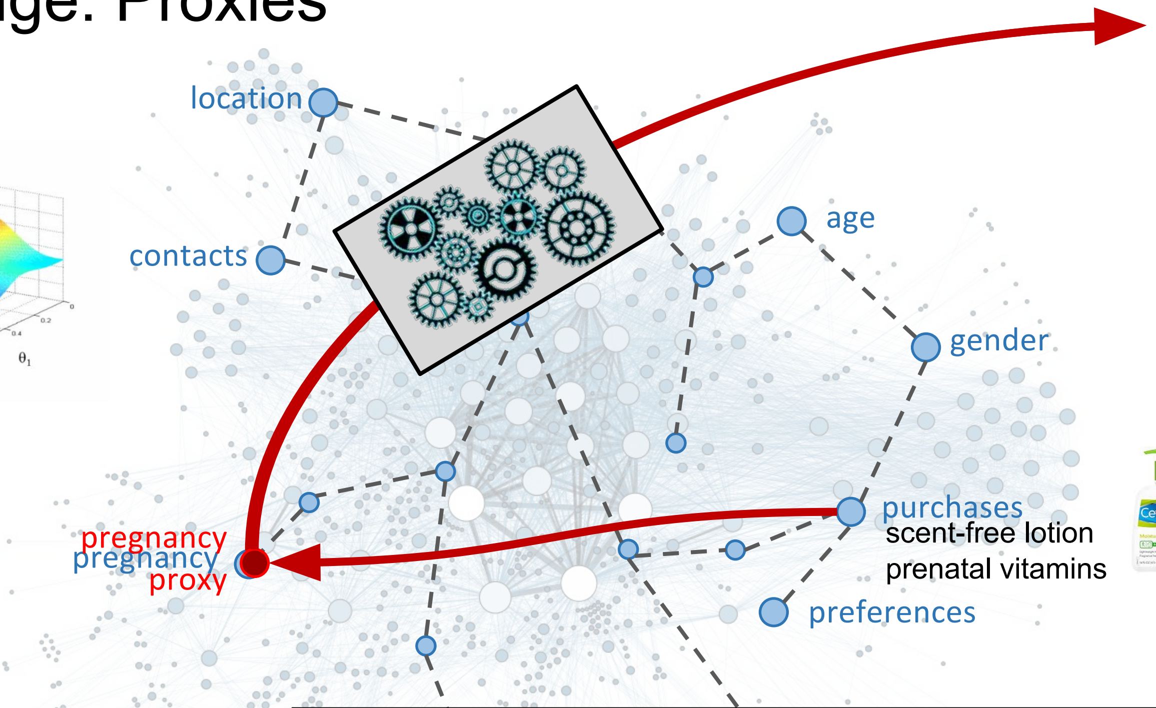


X	Y	Z
…	…	…
…	…	…

The Challenge: Proxies



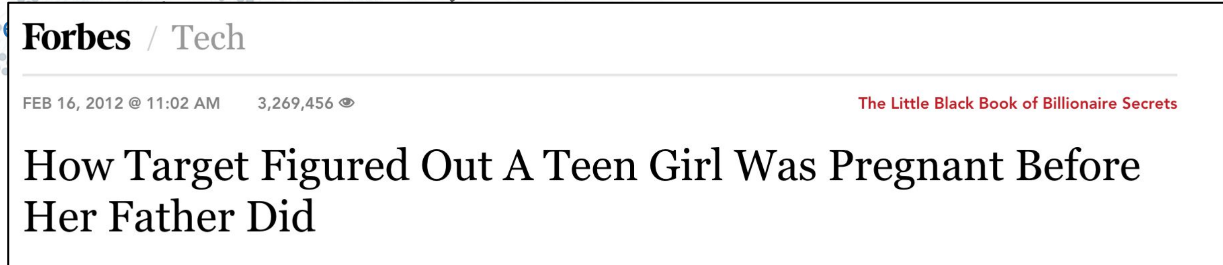
Target.



coupons

scent-free lotion

prenatal vitamins



Forbes / Tech

FEB 16, 2012 @ 11:02 AM 3,269,456

The Little Black Book of Billionaire Secrets

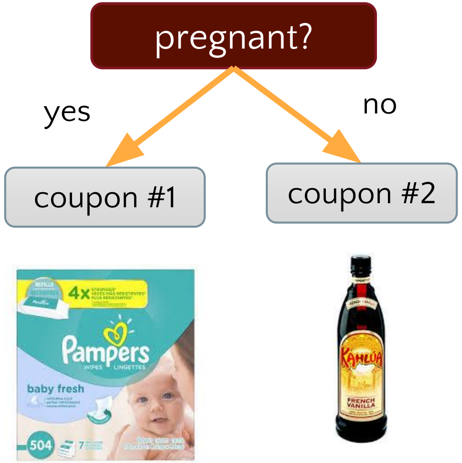
How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Use Privacy in Data-Driven Systems

- Proxy Use: definition of use
- Workflow and examples
- Results
- Summary

Proxy use: Definition by example

1. **explicit use**



pregnant?

yes

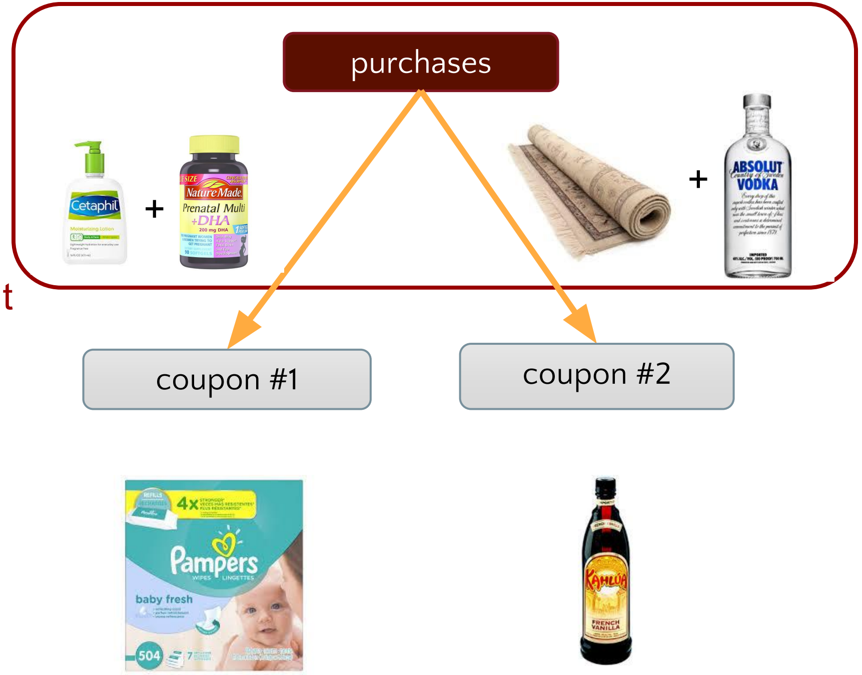
no

coupon #1

coupon #2

Proxy use: Definition by example

1. explicit use
2. **use by proxy**



proxy for pregnant

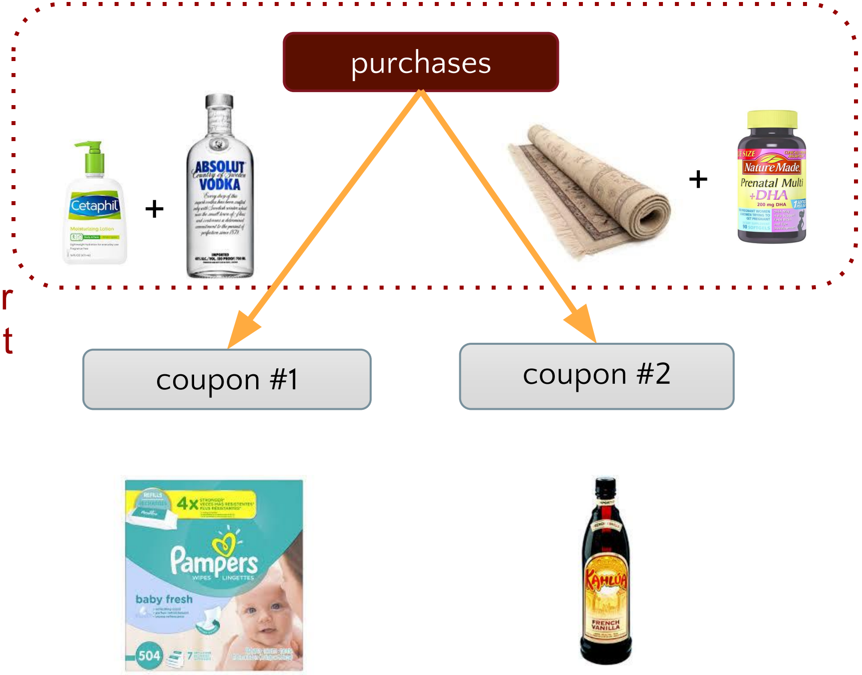
purchases

coupon #1

coupon #2

Proxy use: Definition by example

1. explicit use
2. use by proxy
3. **no use**

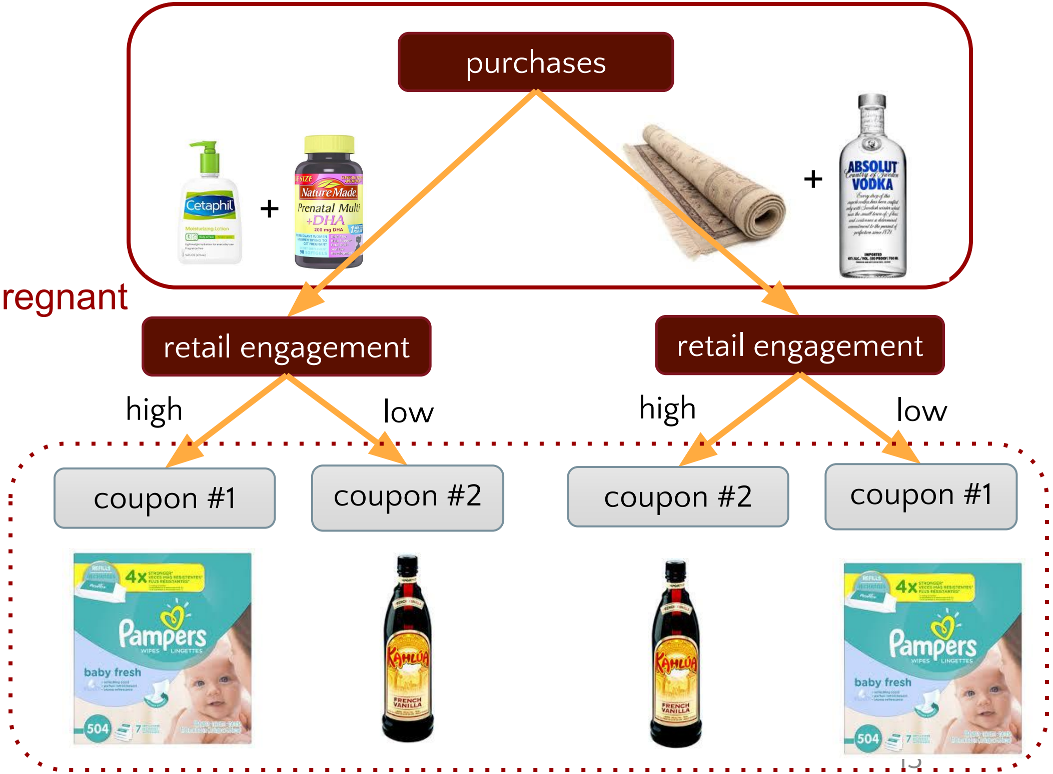


NOT a proxy for pregnant

Proxy use: Definition by example

1. explicit use
2. use by proxy
3. no use
4. **masked use**

proxy for pregnant

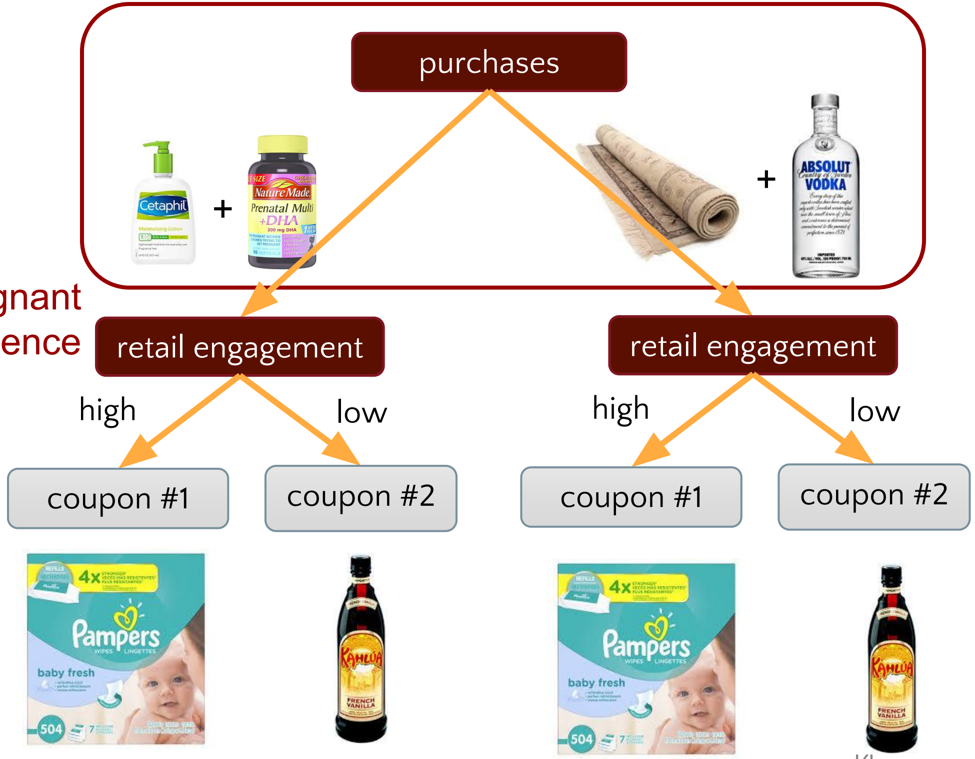


output NOT correlated to pregnant

Proxy use: Definition by example

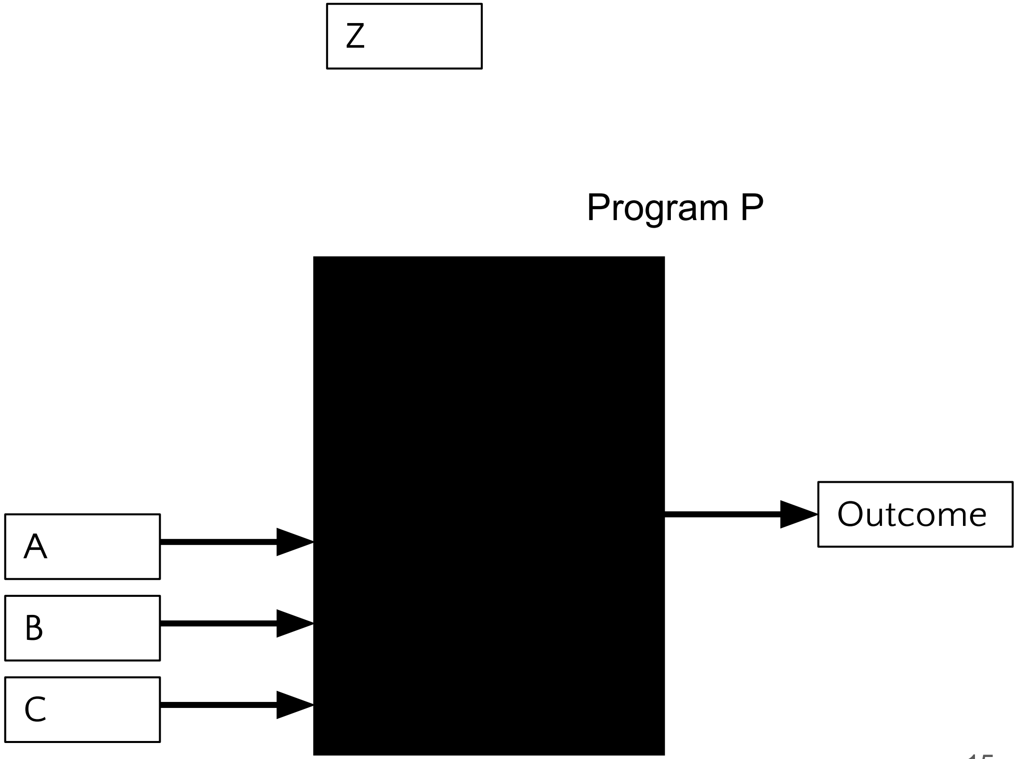
1. explicit use
2. use by proxy
3. no use
4. masked use
5. **influence in use**

proxy for pregnant
but no causal influence



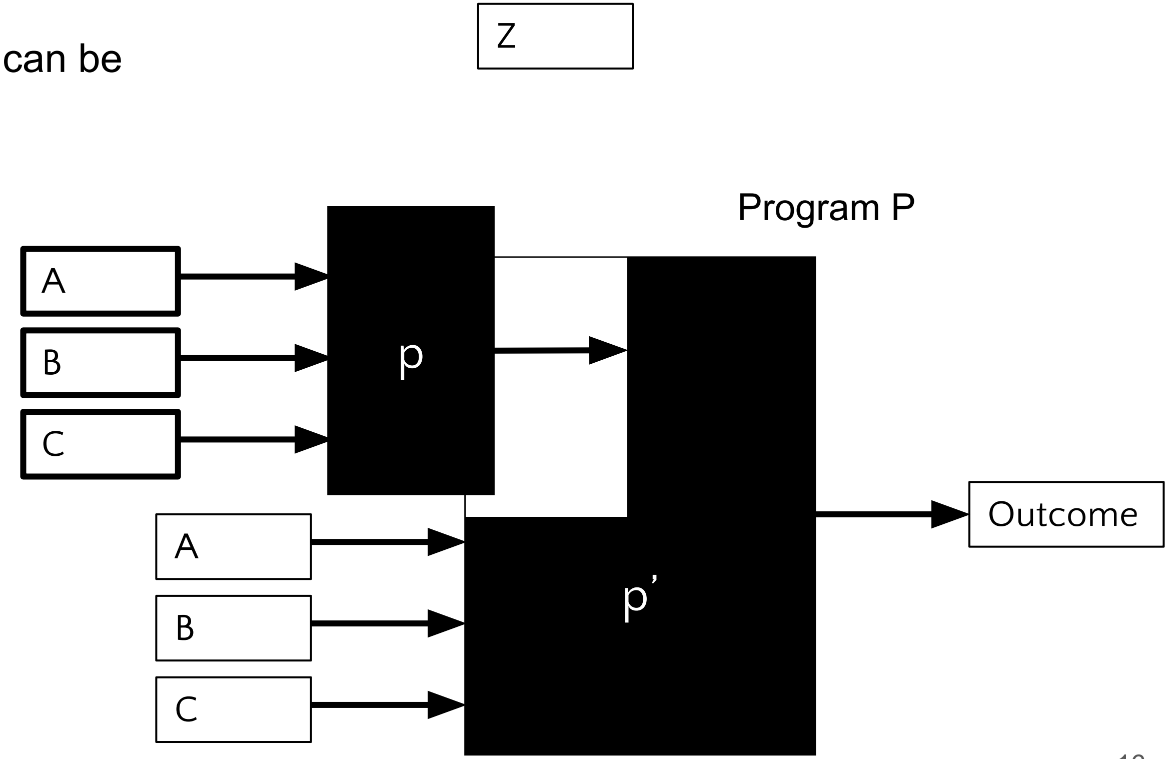
Proxy use: Definition

- ***program P has proxy use of Z*** iff ...



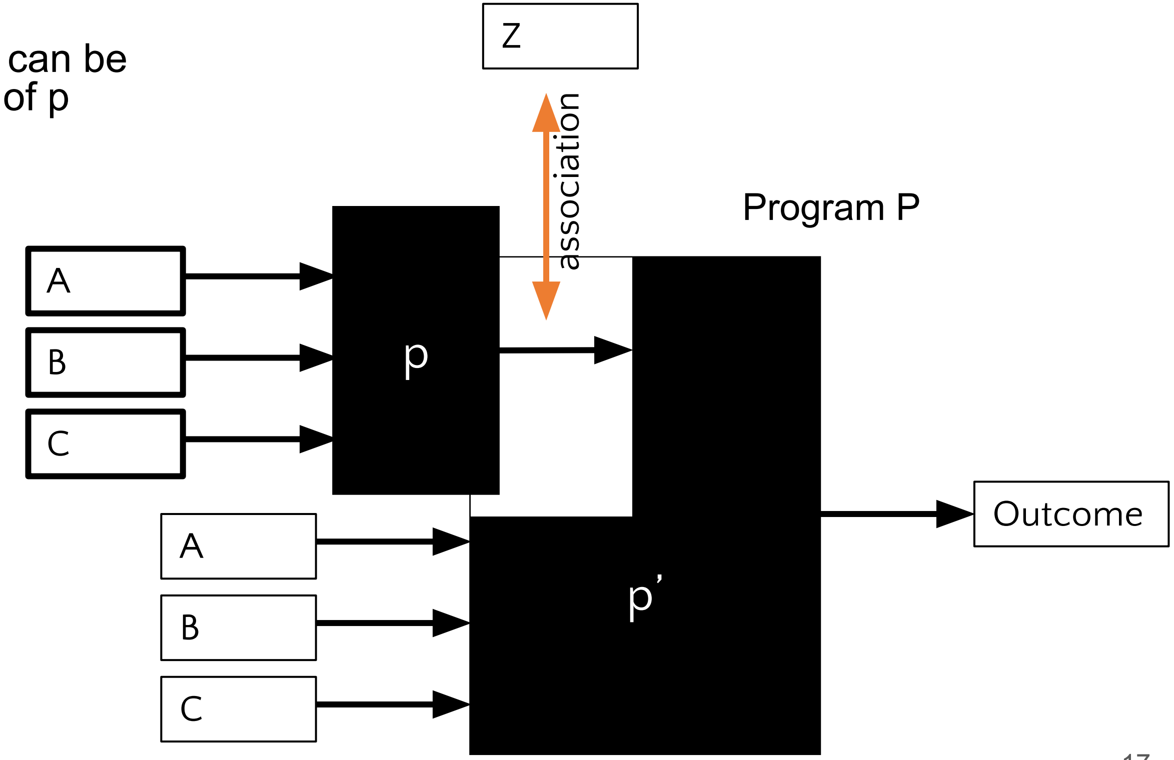
Proxy use: Definition

- ***program P has proxy use of Z*** iff it can be decomposed into p,p’ ...



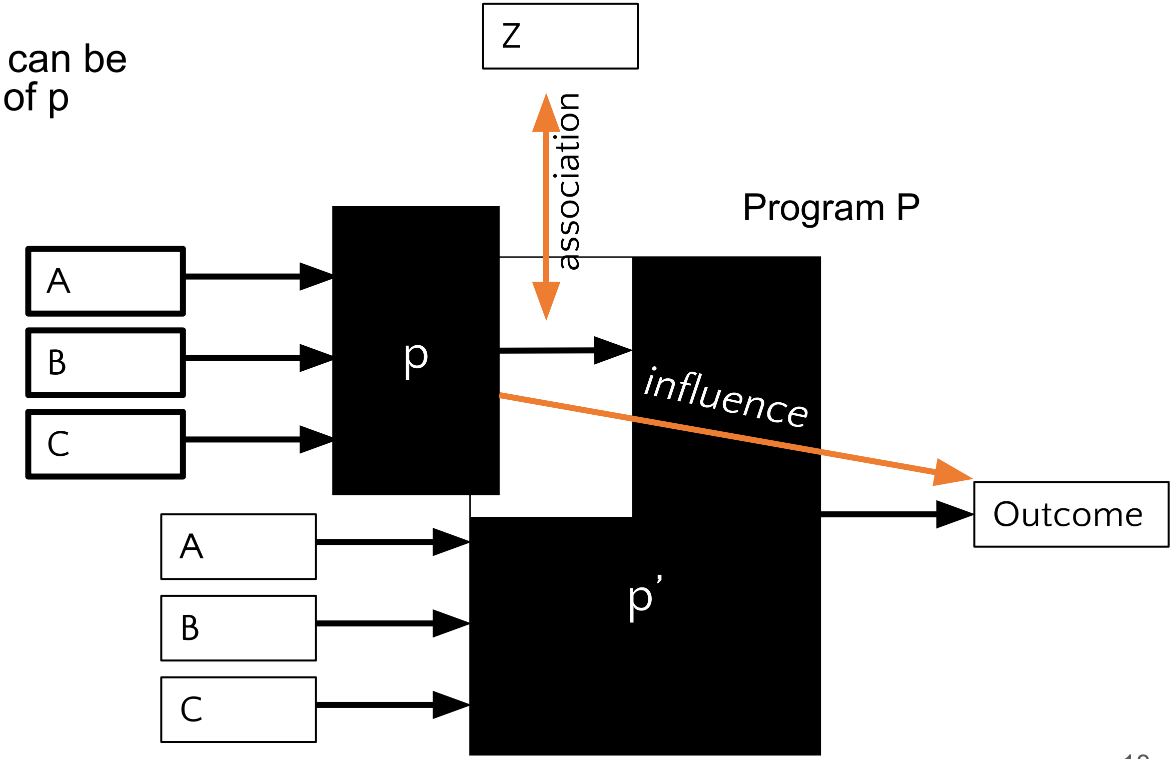
Proxy use: Definition

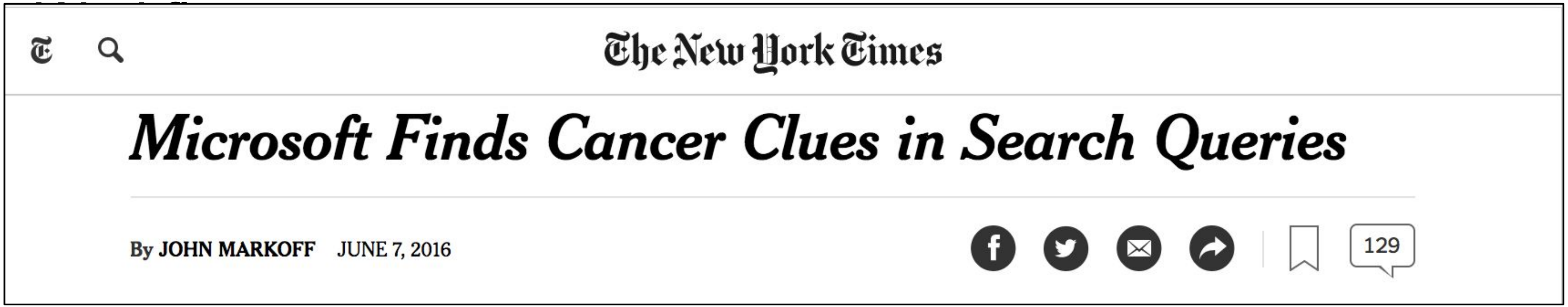
- ***program P has proxy use of Z*** iff it can be decomposed into p,p’ s.t. the output of p
    - is a ***proxy*** of Z (associated) and



Proxy use: Definition

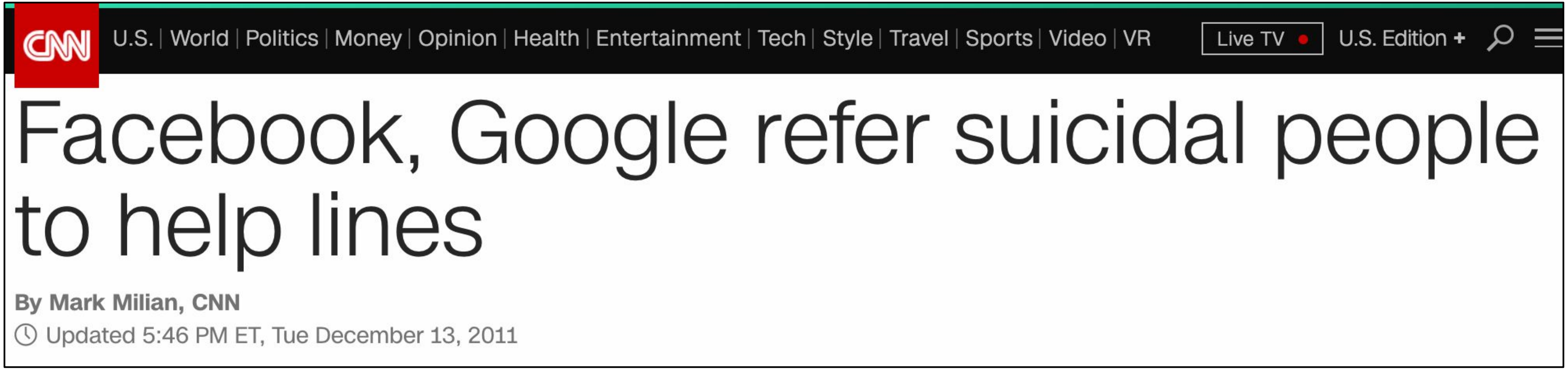
- ***program P has proxy use of Z*** iff it can be decomposed into p,p’ s.t. the output of p
  - is a ***proxy*** of Z (associated) and
  - is ***used*** (causal influence).





Microsoft Finds Cancer Clues in Search Queries

By JOHN MARKOFF JUNE 7, 2016

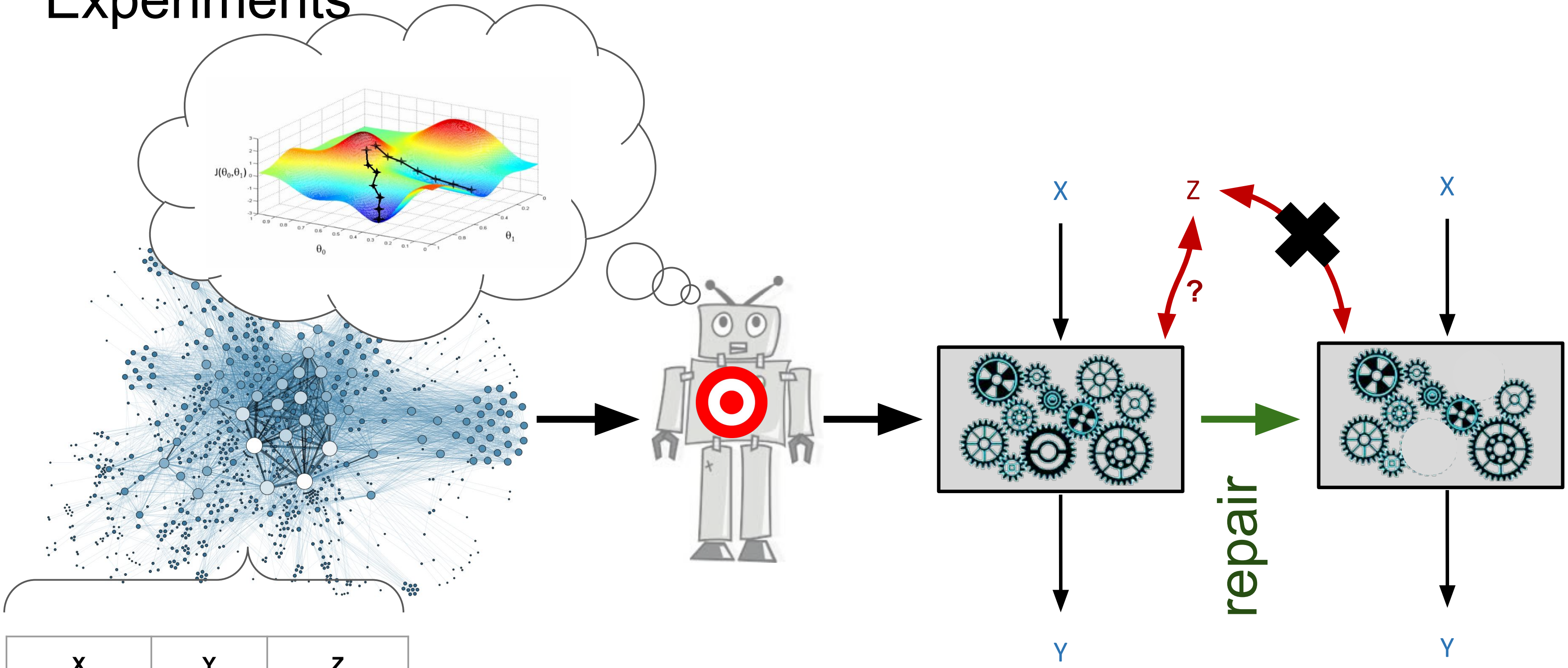

CNN
U.S. | World | Politics | Money | Opinion | Health | Entertainment | Tech | Style | Travel | Sports | Video | VR
Live TV
U.S. Edition +

Facebook, Google refer suicidal people to help lines

By Mark Milian, CNN

Updated 5:46 PM ET, Tue December 13, 2011

Experiments

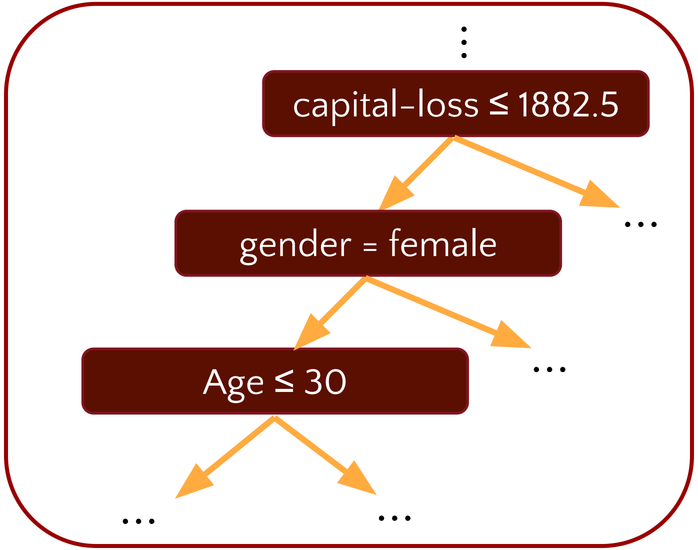


X	Y	Z
…	…	…
…	…	…

Example: Income

Income prediction using census data

- Gender, Education, Age, Capital Gains, Ethnicity, others
- **Marital status:** Married-civ-spouse, Divorced, Never-married, Separated, …
- Classification: Income <50k,>= 50K
- ~30,000 individuals



~ Marital status

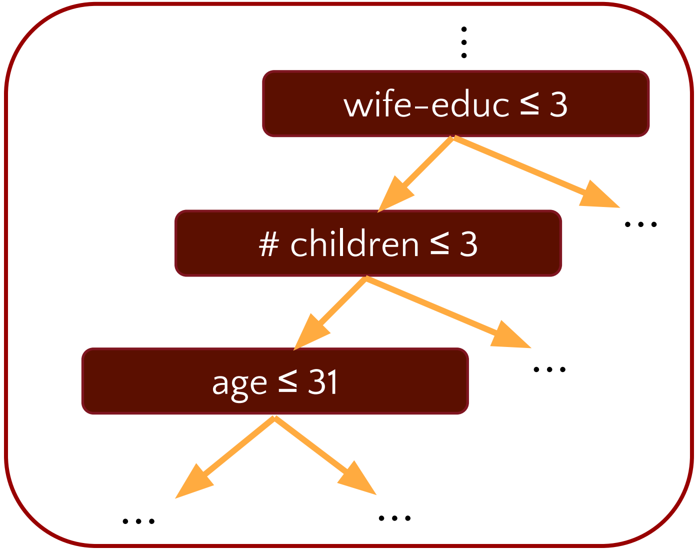
model accuracy
83.6 %

after repair
81.7 %

Example: Indonesian contraception

Contraception method of married women predicted from family information.

- wife's age, husband's education, # children, wife's occupation, husband's occupation, standard-of-living index, media exposure
- Wife's education 1=low, 2, 3, 4=high
- **Wife's religion** 0=Non-Islam, 1=Islam
- Classification: Contraceptive method used 1=No-use 2=Long-term 3=Short-term
- 1473 individuals



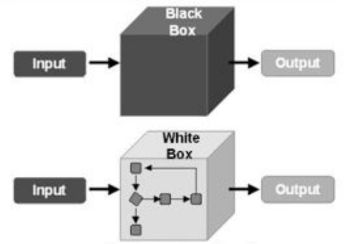
~ Wife's religion

model accuracy
61.2%

after repair
52.1%

See paper for

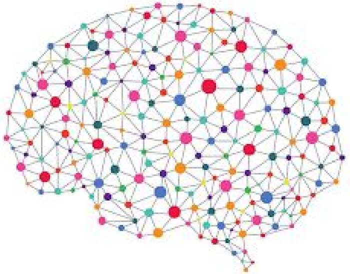
- Why white-box?
  - Semantic Impossibility Result
- Quantitative parameterization
  - Quantify proxy-ness and use
- Algorithms
  - Detection and utility-sensitive repair
- More experiments
  - More data
  - More models

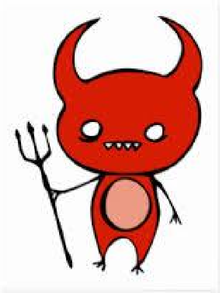


(ε,δ)

Ongoing work / open problems

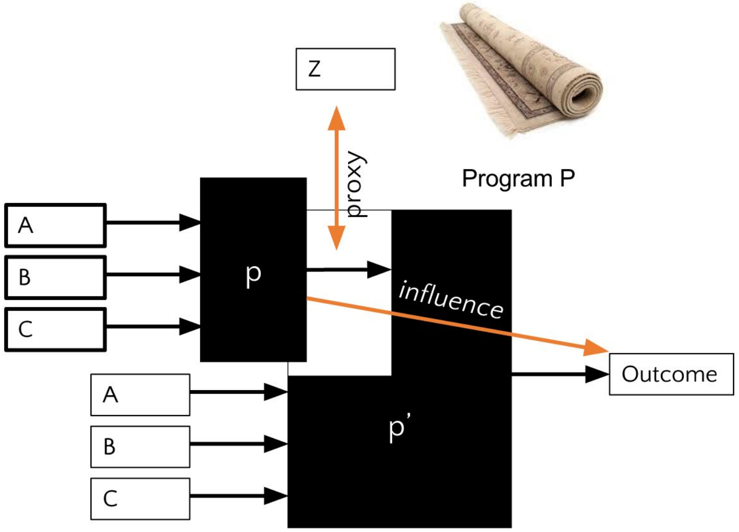
- Practical/scalable tools for data scientists
- Support for more complex models
- “Adversarial” settings: tools for auditors, end-users





TL;DW: *Use Privacy* in Data-Driven Systems

- **Use restrictions** are important privacy requirements
- **Challenge: proxies** make enforcing use restrictions difficult
- Our contribution: a **definition** and **enforcement workflow** for *use privacy*


Z
proxy
Program P
A
B
C
p
influence
Outcome
A
B
C
p'