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
Starting November 5, class will be held out of CIC 4101!
Midsemester Rubric and Comments

- Few students did poorly on both homeworks
  - Eventual lowest homework drop will help many, but be sure those are good!
  - Office hours can help
- Significant improvement on people’s project proposal scores!
- Quizzes pretty good
- Class activity quite correlated with overall performance

<p>| | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Homeworks</strong></td>
<td>15 points each</td>
<td><strong>Highest quizzes:</strong> 2</td>
</tr>
<tr>
<td><strong>Class participation</strong></td>
<td>5 points</td>
<td><strong>FIPPs Piazza:</strong> 1</td>
</tr>
<tr>
<td><strong>Activity:</strong></td>
<td>2</td>
<td><strong>Activity:</strong> 2</td>
</tr>
<tr>
<td><strong>Class project</strong></td>
<td>6 points</td>
<td><strong>Project proposal</strong></td>
</tr>
</tbody>
</table>
Engagement is good for you

Midsemester grade

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

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)?
You’ve seen use privacy before

_Cylabrador Medical Privacy Law v. 3:

_Doctors must have a patient’s consent to share their diagnosis information with anyone except for the purpose of medical care._

Dear Cylabrador Times-Dispatch,

I am writing to you to inform you that my patient, Gordon, who is in a coma, suffers from Embarrassing Smell Disorder. His family refused to meet my very reasonable blackmail demands, so I’d like you all to share his diagnosis with the world.

Regards,
Dr. Strangelove
V. THE FAIR INFORMATION PRACTICE PRINCIPLES

**PIPEDA**
Personal Information Protection and Electronic Documents Act

---

The organization under its control and shall designate an officer to oversee the 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 retained only as long as it is necessary for the fulfillment of the purposes for which it was collected.
HIPAA: Do not use health information for marketing purposes.

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)?

Restrict Use: *Does X use* private Z?  
← Legal / Ethical concerns

Our work: *Use Privacy*

---

Use Privacy in Data-Driven Systems
Theory and Experiments with Machine Learnt Programs

Anupam Datta, Matt Fredrikson, Gilhyuk Ko, Piotr (Pawel) Maidal, Shayak Sen

Accountable Systems Lab
fairlyaccountable.org
Setting: Data driven systems

<table>
<thead>
<tr>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>
| ...| ...| ...
The Challenge: Proxies

pregnancy  proxy

location
contacts

age  gender  purchases
scent-free lotion
prenatal vitamins
preferences

 coupons

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

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
Proxy use: Definition by example

1. explicit use
2. use by proxy
Proxy use: Definition by example

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

- NOT a proxy for pregnant

- purchases

- coupon #1
- coupon #2
Proxy use: Definition by example

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

output NOT correlated to pregnant

Proxy use: Definition by example

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

output NOT correlated to pregnant
Proxy use: Definition by example

1. explicit use
2. use by proxy
3. no use
4. masked use
5. proxy without use
Proxy use: Definition

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

![Diagram showing Program P with inputs A, B, C, and output Outcome]
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).

![Diagram showing program P, Z, p, p', influence, association, and proxy use definition.]

A, B, C inputs to \( p \), \( p' \), with arrows indicating influence and association to Z, leading to the outcome.
Experiments

<table>
<thead>
<tr>
<th>X</th>
<th>Y</th>
<th>Z</th>
</tr>
</thead>
<tbody>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
<tr>
<td>...</td>
<td>...</td>
<td>...</td>
</tr>
</tbody>
</table>

repair
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

![Diagram showing decision tree for income prediction]

- Model accuracy: 83.6% after repair
- ...
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

Model accuracy
- 61.2%
- after repair 52.1%
## Example model digest

<table>
<thead>
<tr>
<th>Purpose of model</th>
<th>Allowed information</th>
<th>Proxied term</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send out coupons to Target that people will use</td>
<td>People’s past purchases</td>
<td>Pregnancy status</td>
</tr>
<tr>
<td>Predict people’s income from their census data</td>
<td>Census data EXCEPT marital status</td>
<td>Marital status</td>
</tr>
<tr>
<td>Predict contraception method of married women</td>
<td>Wife’s age, husband's education, # children, wife's occupation, husband's occupation, standard-of-living index, media exposure (not Religion)</td>
<td>Religion</td>
</tr>
</tbody>
</table>
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

\[(\varepsilon, \delta)\]
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*

![Diagram](www.fairlyaccountable.org)