Privacy and Composability
(Part 1)

Anupam Datta

Associate Professor
CSD, ECE, CyLab
Carnegie Mellon University
Don’t use age & Don’t use gender

Hiring algo. ; Offer algo.

Implies that

Property holds of system

Don’t use age & Don’t use gender

Hiring algo. ; Offer algo.
Privacy as a right to **restrictions** on personal **information flow**
Noninterference

[Noninterference Program]

High input
Female

Low output
Job ad

Low inputs

Different high input
Male

Same Program

Same low output

Same low inputs

[Goguen and Meseguer, 1982]
Probabilistic Noninterference

Program

Low output distribution

Same low output distribution

Same Program

Different high input

Female

Low inputs

Same high input

Male

Same low inputs
Differential Privacy

About the same low output distribution

High inputs

Program

Low output distribution

Low inputs

Same Program

High inputs

Same low inputs

[Dwork, McSherry, Nissim & Smith, 2006]
A covered entity may disclose an individual’s protected health information (phi) to law-enforcement officials for the purpose of identifying an individual if the individual made a statement admitting participating in a violent crime that the covered entity believes may have caused serious physical harm to the victim.

- **Concepts in privacy policies**
  - **Actions**: send(p1, p2, m)
  - **Roles**: inrole(p2, law-enforcement)
  - **Data attributes**: attr_in(prescription, phi)
  - **Temporal constraints**: in-the-past(state(q, m))
  - **Purposes**: purp_in(u, id-criminal))
  - **Beliefs**: believes-crime-caused-serious-harm(p, q, m)
Reduce Algorithm

\[ \text{reduce} \left( \mathcal{L}, \varphi \right) = \varphi' \]
Privacy as Restrictions on Personal Information Flow

**Purpose & Role based**

- EPAL
- XACML
  - *-access control
- Purpose → Planning

**Temporal**

- FOTLs
  - [Formal Contextual Integrity, Reduce audit algorithm, Basin et al.]

**Interference**

- Jif, FlowCaml, ...
- [Hayati & Abadi]

**Direct**

- Grok + Legalease

**Probabilistic Interference**

- Information Flow Experiments

**Differential Privacy**
Privacy and Composition (Part 2)

Michael Carl Tschantz
International Computer Science Institute
Program 2

Low inputs

Low outputs
High inputs

Low outputs

Program 1

High outputs

Low inputs

Low outputs

Low outputs

Program 2
Failure of Composition

Composite System

Program 1

Program 2

High inputs → High outputs

Low inputs ← Low outputs

High outputs → Low inputs

Low outputs ← Low inputs
Program 1

Low outputs

High outputs

High inputs
High inputs

Program 2

High outputs

High inputs
Failure of Composition

Composite System

Program 1

High outputs

High inputs

Program 2

High outputs

High inputs

Low outputs

High inputs
## Noninterference Compositional and Not

<table>
<thead>
<tr>
<th></th>
<th>Feedback</th>
<th>Cascade (sequential)</th>
<th>Product (parallel)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Not</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td></td>
<td>Not in general</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

[McLean, 1996]
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.
Auditing

- Purpose restriction
- Auditee’s behavior
- Environment Model

- Obeyed
- Inconclusive
- Violated
Record for treatment

Consistent with observed behavior

Consistent with treatment

Solver

Behavior log
Record for treatment

Record for cost reduction

Consistent with treatment

Consistent with observed behavior

Consistent with cost reduction

Behavior log

Solver

Solver
Purpose Compositional and Not

Simultaneous: No
Parallel: Yes
Sequential: Yes

[Tschantz, Datta & Wing 2012; Tschantz 2012]
'We'll be back': Hong Kong protesters chant as camp site dismantled

Reuters | Dec 12, 2014, 08:30 AM IST

HONG KONG: Hong Kong police arrested pro-democracy activists and cleared most of the main protest site on Thursday, marking an end to more than two months of street demonstrations in the Chinese-controlled city, but many chanted: "We will be back".

Most activists chose to leave the Admiralty site, next to the Central business area, peacefully, despite their demands for a free vote not being met. But the overall mood remained defiant.

Hong Kong Federation of Students leader Alex Chow said: "You might have the clearance today but people will come back on to the streets another day."
## Settings for Google ads

Ads enable free web services and content. These settings help control the types of Google ads you see.

### Ads on Google

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Edit Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gender</td>
<td>N/A</td>
<td>Female/Edit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Age</td>
<td>N/A</td>
<td>25-34/Edit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Languages</td>
<td>N/A</td>
<td>English/Edit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Interests</td>
<td>N/A</td>
<td>Air Travel, and 30 more/Edit</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Google ads across the web

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
<th>Edit Options</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Opt-out settings

You've opted out of interest-based ads on Google. **Opt in** to interest-based ads on Google. **Opt out** of interest-based Google ads across the web.
Discrimination

Web browsing → Ad ecosystem → Advertisements

Browse websites related finding a new job

Ad settings

Set the gender bit to female or male

Significant difference ads on news website \((p < 0.000006)\)

[Datta, Tschantz & Datta 2015]
Female Group

Jobs (Hiring Now)
www.jobsinyourarea.co
45 vs. 8

4Runner Parts Service
www.westernpatoyotaservice.com
36 vs. 5

Criminal Justice Program
www3.mc3.edu/Criminal+Justice
29 vs. 1

Male Group

$200k+ Jobs - Execs Only
careerchange.com
311 vs. 1816

Find Next $200k+ Job
careerchange.com
7 vs. 36

Become a Youth Counselor
www.youthcounseling.degreeleap.com
0 vs. 310
Out Bided on Women but Not Men

<table>
<thead>
<tr>
<th>Bids for Females</th>
<th>Bids for Males</th>
</tr>
</thead>
<tbody>
<tr>
<td>$7 Makeup</td>
<td></td>
</tr>
<tr>
<td>$5 Dress</td>
<td></td>
</tr>
<tr>
<td>$4 Job</td>
<td>$4 Job</td>
</tr>
<tr>
<td>$2 Hair Salon</td>
<td></td>
</tr>
<tr>
<td>$1 Car</td>
<td>$1 Car</td>
</tr>
</tbody>
</table>
Who’s to Blame?

• Career coaching service: place same bids for females and males
• Other advertisers: place bids on females for products that cater only to women
• Google: show the highest bid
Backup
Correctness of Reduce

**Theorem 3.2** (Partial correctness of reduce). If $\text{reduce}(\mathcal{L}, \varphi) = \psi$ and $\mathcal{L} \leq \mathcal{L}'$, then (1) $\mathcal{L}' \models \varphi$ iff $\mathcal{L}' \models \psi$ and (2) $\mathcal{L}' \models \overline{\varphi}$ iff $\mathcal{L}' \models \overline{\psi}$.
The Bartlett Group

Other advertisers

Google

Websites

Male users

Female users
The Bartlett Group 

Show to males

Google 

Male users 

Other advertisers 

Websites 

Female users
Female users

Male users

Other advertisers

The Bartlett Group

Show to both

Google

Show to females

Websites

Female users
The Bartlett Group

Other advertisers

Google

Website

Clicking

Male users

Not clicking

Female users
Input

Output

The Bartlett Group

Other advertisers

Websites

Clicking other ads

Male users

Female users

Not clicking other ads

Google
Possible Reasons

1. Google programmed the system to treat genders differently
2. Google's targeting algorithm found and responded to a difference in how males and females were clicking on ads
3. The advertiser targeted the ad differently across genders
4. The advertiser targeted a group correlated with gender
5. The advertiser was out bid on women
6. Some other reason we haven't thought of
7. Some combination of the above