A Big-Brother Revolution with Virtual Assistants

Monica Lam
Computer Science Department
Stanford University
lam@cs.stanford.edu

With Giovanni Campagna, Michael Fischer, Mehrad Moradshahi, Rakesh Ramesh, Richard Socher, Silei Xu, Richard Yang
Sponsors: Hitachi, UST Global
Big-Brother Problem

- Consumers: Data Privacy
  - Facebook owns and sells 2-billion people’s personal data
  - Cambridge Analytica incident
  - Big tech backlash

- Unhealthy industrial ecosystem: Platform monopolies/duopolies
  - Google and Apple app stores: 30% revenues
  - Google and Facebook: 60% digital marketing revenues
Biggest Brother: Virtual Assistants

Personal, Linguistic User Interface (LUI)
Sees all personal info
Intermediates all digital services
Controls choice of vendors

Amazon, Facebook, Google combined
## Make Virtual Assistants our Ally

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Open-source decentralized virtual assistants</th>
<th>Almond</th>
</tr>
</thead>
<tbody>
<tr>
<td>Non-Proprietary</td>
<td>Open, crowdsourced skill repository</td>
<td>Thingpedia</td>
</tr>
<tr>
<td>Expressiveness</td>
<td>Open LUI technology &amp; training data</td>
<td>LUInet</td>
</tr>
</tbody>
</table>

Giovanni, Ramesh, Xu, Fischer, Lam, WWW 2017
Example: Asthma Patient

**People**
Dr. Smith: “If Bob’s peak flow-meter drops below 180L/min let me know.”

**Environment**
Dr. Smith: “When the air quality index is above 500 and Bob is running, warn him.”

**Location**
“Let my Dad know if I am at the hospital.”

**Devices**
“When I use my inhaler, record my GPS location in logfile on Box.”
Almond: Open-Source Decentralized Virtual Assistant

- Available as a demo web service/android app
- Decentralized: multiple vendors; personal devices
- Runs complex commands
- Supports sharing with inter-virtual assistant communication
**Thingpedia: Encyclopedia of Things**

- Easy to enter primitive skills in Thingpedia
  - Usable in compound commands
  - API signatures, not just intent dispatches
- Open repository
  - Available to Alexa, Google Assistant, ...

---

**50 devices + 200 functions**

<table>
<thead>
<tr>
<th></th>
<th>Natural Language</th>
<th>Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>WHEN</td>
<td>@Stanford tweets</td>
<td>Monitor (@home_timeline(), ...) author==“Stanford”)</td>
</tr>
<tr>
<td>GET</td>
<td>tweets matching “#Cardinal”</td>
<td>search(...), contains (hashtag, ...)</td>
</tr>
<tr>
<td>DO</td>
<td>tweet “Stanford won!”</td>
<td>post (status)</td>
</tr>
</tbody>
</table>
LUInet: A Neural Network for LUls

- Event-driven program
- Multiple function calls
- Parameter passing
- Filters on values

"When I use my inhaler, get my GPS location, if it is not home, write it to logfile in Box."

```
monitor @Inhaler-use(),
=> @GPS(), location <> "home"
=> @Box-write(file="logfile", data=location)
```

WHEN [FILTERS]
=> GET [FILTERS]
=> DO
ThingTalk Compound Statement

WHEN [FILTERS] → GET [FILTERS] → DO

FILTERS: =, <, >, <=, >=, <>, contains, starts with, ends with

- When I use my inhaler, get my location, save them to Dropbox
- If I get taken to a hospital, let my dad know.
- When the air quality index is above 500, and I am running, send me an SMS.
LUInet

- World of digital interfaces and how they can be composed in NL
  - Consumers:
    long tail of functions, without relying on programmers
  - Corporate: work flows with confidential APIs
- Key technology: semantic parsing with compositionality
  - Feasibility demonstrated by preliminary deep learning models
  - Need usage data and research to improve accuracy
Sharing is Broken Today

• Hard to share
  • Users give up ownership and privacy
  • Limited flexibility of access control
• LUInet + Almond: flexibility and privacy
Fine-Grained Sharing with Privacy

Bob wants to see your photos on Facebook

Owner assistant performs tasks on behalf of requester,

subject to approval of the owner
Access Control: an Extension of ThingTalk

Requester: GET-PREDICATE [FILTERS]

WHEN [FILTERS] → GET [FILTERS] → DO

FILTERS: =, <, >, <=, >=, contains, starts with, ends with

Let Dr. Smith, monitor my peak-flow-meter, if it drops below 180L/min
Let my father, monitor my security camera for motion, only if I’m not home.
Let my accountant get my monthly statements
Let my daughter, from 6-8pm, watch NetFlix
Let my boyfriend, get pictures from my dropbox, taken on Feb 14, and post them on Facebook
### Do Consumers Need Access Control?

<table>
<thead>
<tr>
<th>Role-Based Permission</th>
<th>Attribute-Based Permission</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Teenage daughter</strong> to use credit card</td>
<td>If the package is over $1000</td>
</tr>
<tr>
<td><strong>Amazon courier</strong> to unlock door</td>
<td>If your security camera is on</td>
</tr>
<tr>
<td><strong>Friends</strong> to access cloud drive</td>
<td>Photos with their faces in them</td>
</tr>
<tr>
<td><strong>Parent/kid</strong> to see security cameras</td>
<td>Photos in a specific folder</td>
</tr>
<tr>
<td><strong>10-year-old kid</strong> to use Netflix</td>
<td>If you are not at home</td>
</tr>
<tr>
<td></td>
<td>Cameras facing the front yard/garage</td>
</tr>
</tbody>
</table>

- **Free G or PG rated movies**
- Between 7 PM to 9 PM
- With a $20 budget limit
- For restaurants only

% People comfortable in giving permission (200 person survey)
A Research Agenda Proposal: Open-Source Decentralized Virtual Assistants

<table>
<thead>
<tr>
<th>Privacy</th>
<th>Open-source decentralized infrastructure</th>
<th>Almond</th>
</tr>
</thead>
<tbody>
<tr>
<td>Openness</td>
<td>Non-proprietary, crowdsourced skill repository</td>
<td>Thingpedia</td>
</tr>
<tr>
<td>Expressiveness</td>
<td>LUI technology &amp; dataset in open domain</td>
<td>LUInet</td>
</tr>
</tbody>
</table>

Put Users in the Driver Seat