Privacy in the Age of the Internet of Things

Norman Sadeh
Carnegie Mellon University

www.normsadeh.org
usableprivacy.org privacyassistant.org
explore.usableprivacy.org
Quick Show of Hands

• Imagine that you are in the market to purchase a car insurance policy…
How Many of You Would Feel Comfortable Disclosing…

• How many miles you drive per year?

• How fast you drive…
  – Based on GPS…

• Where you go and when…
  – Based on GPS…

• Relevant health data…
  – Such as how many hours you sleep at night…
  – Based on data sensed by your wristwatch…
Internet of Things & Big Data

Increasingly diverse, complex and opaque dataflows

http://www.iamwire.com/2017/01/iot-ai/148265
Information Privacy

• The claim that *certain information should not be collected by government or businesses* – or possibly only under special circumstances – and subject to various rules

  – individuals have some control over the collection and use of information about them
Legal Landscape

• A number of privacy laws around the world:
  – US: State, federal and local laws
    • Federal level: Patchwork of sectoral laws and laws that pertain to data collected by the government
  – EU: General Data Protection Regulation (GDPR)

• All these laws share some commonalities: They set minimum requirements to:
  – Inform users about data collection and use practices
  – Provide users with some type of choice
In practice…

• **Notice and choice is broken**
  – No time to read policies
  – Policies difficult to understand
  – No time or motivation to configure settings

• **91% of people report feeling they have lost control over their information**

Mobile and IoT: A Number of Complicating Factors

- A typical mobile phone user with 50 mobile apps each requesting 3 permissions would have to configure 150 settings

- IoT: Technology is often “invisible”

- Reading policies is even less practical

- Explosion in the number of apps and devices

- Developers often lack the necessary sophistication

What If….

• **Computers understood privacy policies?**
  – Machine-readable policies have been proposed but have not gained traction

• **Computers understood what we care about and what we already know/expect**
Could We Teach Computers to Read Privacy Policies?
1. **First Party Collection/Use**
   - Retention period:
     - All
     - Indefinitely (1)
   - Purpose of retention:
     - All
     - Unspecified (1)

2. **Third Party Sharing/Collection**
   - [More filters](#)

3. **User Choice/Control**

4. **User Access, Edit and Deletion**

5. **Data Retention**
   - [More filters](#)

6. **Data Security**

7. **Policy Change**

8. **Do Not Track**

9. **International and Specific Audiences**

---

**Privacy Policy**

Yahoo News Privacy Policy from Sep 25, 2014. Reading Level: College (Grade 13)

125 privacy practice statements in total

This privacy policy also applies to Flickr, Yahoo Finance, Yahoo News, Yahoo Sports, and Yahoo! Good Morning America.

We reserve the right to send you certain communications relating to the Yahoo service, such as service announcements, administrative messages and the Yahoo Newsletter, that are considered part of your Yahoo account, without offering you the opportunity to opt out of receiving them.

You can delete your [Yahoo account by visiting our Account Deletion page. Please click here to read about information that might possibly remain in our archived records after your account has been deleted.](#)

**CONFIDENTIALITY AND SECURITY**

We limit access to personal information to personnel who we believe reasonably need to come into contact with that information to provide products or services to you or in order to do their jobs.

We have physical, electronic, and procedural safeguards that comply with federal regulations to protect personal information about you.

To learn more about security, including the security steps we have taken and security steps you can take, please read Security at Yahoo.

**CHANGES TO THIS PRIVACY POLICY**

Yahoo may update this policy. We will notify you about significant changes in the way we treat personal information by sending a notice to the primary email address specified in your Yahoo account or by placing a prominent notice on our site.

**QUESTION AND SUGGESTIONS**

If you have questions, suggestions, or wish to make a complaint, please [complete a feedback](#).
A First Task: Segment Annotation

Disclosure of Your Information  Sci-News.com does not sell, trade or rent your personal information to third parties. If we choose to do so in the future, you will be notified by email of our intentions, and have the right to be removed prior to the disclosure.

This policy segment discusses:

- Third Party Sharing/Collection
Another Task: User Choice Instance Extraction

**Choice Instance !!!**
If you do not want us to use personal information that we gather to allow third parties to personalize advertisements we display to you, please adjust your Advertising Preferences.

- User choices often buried deep in the text of long policies
- Is it possible to automatically extract information about such “choice instances” from privacy policies?
- Use Natural Language Toolkit tokenizer to subdivide segments into sentences & build classifiers

---

Annotated 7,000+ policies

https://explore.usableprivacy.org/
Press Coverage – Notice the Irony

You’re Never Going To Read That Privacy Policy. Could AI Help?

This AI trained on legalese acts like a personal translator of confusing, opaque privacy statements.

Screenshot taken on May 31, 2018
Question

• How about helping end users?

• Could we learn people’s privacy expectations and preferences?
  – To selectively notify them about relevant privacy practices
  – To help them configure privacy settings
One Size-Fits-All Defaults Don’t Work

Users’ Average Preferences
- White → comfortable
- Red → uncomfortable

Variance among Users
- Darker yellow → larger variance
Identifying a User’s Privacy Profile

• Using Clustering techniques
• Asking users a small set of questions

Q1 → Q2 → Advanced Users
Q1 → Q3 → The unconcerned
Q1 → Fence-sitters

Q2

Q3
Results with Just 4 Clusters

**Accuracy:**
- One size fits all: 55.8%
- 4 Profiles: 79.4%

**User Burden:**
- One size fits all: 86.8%
- 4 Profiles: 36.5%
Now Available on Google Play (rooted Android Phones 5 and up)

[ROOT] Privacy Assistant
Mobile Commerce Lab @ Carnegie Mellon University  Tools  ★★★★★ 4 0
Everyone

Add to Wishlist  Install

Tell Us About Your Privacy Preferences...

To help the privacy assistant recommend settings, please answer a few quick questions.
(You will be asked up to 5 questions. This shouldn't take more than a couple of minutes.)

Privacy Assistant

In general, do you feel comfortable with Social apps accessing your Camera?

Social apps installed on your phone accessing Camera:

- Google+
- Facebook
- Snapchat

Privacy Assistant

In general, do you feel comfortable with Finance apps accessing your Location?

Finance apps installed on your phone accessing Location:

- PayPal
- Citi Mobile
- Chase

Mostly No  Not Sure  Mostly OK
Mostly No  Not Sure  Mostly OK

Usable Privacy Policy and Personalized Privacy Assistant Projects
What About IoT?
Overall Vision: **Personalized Privacy Assistants**

- Learn models of what users already expect & what they want to be informed about, how to communicate with them (when, how often, how), how to configure their settings
  - Or just allow users to manually configure settings
- **Selectively enter into dialogues** with users and nudge them towards safer practices
- **Extend privacy profiles across many environments:** from your smartphone, to your browser, to your smart home to your social networking account, etc.
Privacy Infrastructure for IoT*

- **Registration** of IoT resources and their privacy policies – **IoT Resource Registry (IRR) & Portal**
  - Policies are in a machine readable format
  - Resources include: sensors (e.g., virtual sensors), applications, and services
  - Series of drop down menus, but also use of templates

- **Discovery of IoT resources and their policies**

- **User notification** via **IoT Assistant implemented as mobile app**

- **Protocols** to securely read and configure privacy settings

*Patent pending
Policy Enforcement Points (PEP)
- Stores resource-specific and user-specific privacy policy settings
- Enforces settings for data collected by IoT resources

Overall Architecture*

- IoT Assistant (IoTA)
- Sensor Databases
- IoT Resource Registries (IRR)
- IRR Directories (by location)
- IRR Portals
- Data Analytics
- Authentication
- IoT Resources (e.g. virtual sensors, apps, services)

The mobile app IoTA is used to discover IoT resources and configure their settings (e.g., opt out)

Templates for IoT Devices (e.g. Nest Cam, Echo, Kinect)

*Patent pending
### Deployment Example

- **Aware of user's location**
- **Aware of user's privacy preferences**
- **Displays relevant information received from IRRs**

<table>
<thead>
<tr>
<th>Resource</th>
<th>User Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>WiFi Location Tracking (Service)</td>
<td>Opt In</td>
</tr>
<tr>
<td>Bluetooth Beacon Location Tracking (Service)</td>
<td>Opt Out</td>
</tr>
<tr>
<td>CMU Friend Finder (App)</td>
<td>Opt In (Location Tracking)</td>
</tr>
<tr>
<td>Facial Recognition (Service)</td>
<td>Opt Out</td>
</tr>
<tr>
<td>Video Obfuscation Demo (App)</td>
<td>Opt Out (Facial Recognition)</td>
</tr>
</tbody>
</table>
### Register a new IoT Resource

#### Control Options

<table>
<thead>
<tr>
<th>Service ID</th>
<th>Subsystem ID</th>
<th>Response URL</th>
</tr>
</thead>
<tbody>
<tr>
<td>concierge</td>
<td>wifi</td>
<td><a href="https://tippersweb.uci.edu/api">https://tippersweb.uci.edu/api</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opt in</th>
<th>Description</th>
<th>Link to additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WIFI Location Tracking is enabled</td>
<td><a href="https://tippersweb.uci.edu/api/opt-in">https://tippersweb.uci.edu/api/opt-in</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Opt out</th>
<th>Description</th>
<th>Link to additional information</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>WIFI Location Tracking is disabled</td>
<td><a href="https://tippersweb.uci.edu/api/opt-out">https://tippersweb.uci.edu/api/opt-out</a></td>
</tr>
</tbody>
</table>
Sample Entries & IoT Device Templates

New resources can be defined using pre-filled fields from templates

Existing Templates:
- Echo
- Honeywell thermostat
- Kinect
- Google Home
- Cujo
- Nest Cam
- Wink Relay
- Zensors

Administrators and resource owners control whether resources are published for others to discover.

Usable Privacy Policy and Personalized Privacy Assistant Projects
Where Do We Start?

- Smart cities (e.g. cameras)
- Malls (e.g., cameras, location tracking)
- University campuses – all sorts of IoT technologies
- Smart buildings (e.g. cameras, location, presence, HVAC)
- Smart homes (e.g. smart speakers)
Privacy-aware Video Streaming

Train Facial Features

Control Opt-in

Live Video Stream

Monitor Class Attendance

Demo: https://goo.gl/gtpbpK
Current Status

- Deployed at UC Irvine
- Deployed at CMU
- First public release coming out this summer
- Includes tools to facilitate adoption
  - Tool to help manage IoT Resource Registries (e.g., administrator portal), tool to enter resources, templates for commercial off-the-shelf IoT resources
  - IoT resource registries hosted at CMU
  - Secure protocols for communicating with user-configurable privacy settings (e.g., opt-in, opt-out)
Concluding Remarks

- Privacy is a fundamental human right and people care about privacy
  - Regulations like COPPA, HIPAA but also GDPR
- Fundamental tension between privacy and usability
- Many IoT data collection processes are invisible/obscure and unexpected
- Notice and Choice in the IoT will require deployment of a Privacy Infrastructure that supports the discovery of IoT resources & their data practices
- First release this summer – subscribe to our mailing list for updates: https://www.privacyassistant.org/contact/
Acknowledgements: Work funded by the National Science Foundation, DARPA and Google

The Usable Privacy Policy Project and the Personalized Privacy Assistant Project both involve a collaborations with a number of individuals. See usableprivacy.org and privacyassistant.org for additional details incl. lists of collaborators and publications

Q&A