Scaling Privacy in the Age of the Internet of Things: Could AI Hold the Solution?

Norman Sadeh
Carnegie Mellon University
Outline

• Privacy in the age of IoT
• Notice and Choice is Broken
• The Usable Privacy Policy Project
• Can We Crowdsourcing Policy Annotations?
• How Can Machine Learning and Natural Language Processing Help?
• Nudging Users to Review their Privacy Settings
• Next Steps
The Internet of Things

<table>
<thead>
<tr>
<th>World Population</th>
<th>6.3 Billion</th>
<th>6.8 Billion</th>
<th>7.2 Billion</th>
<th>7.6 Billion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connected Devices</td>
<td>500 Million</td>
<td>12.5 Billion</td>
<td>25 Billion</td>
<td>50 Billion</td>
</tr>
</tbody>
</table>

- 2003: 0.08 More connected devices than people
- 2010: 1.84
- 2015: 3.47
- 2020: 6.58

Source: Cisco IBSG, April 2011
Privacy Implications

• As we go about our daily lives, we interact with a number of devices, applications and services

• Many of these devices applications and services may collect, share and mine data about us
  – Many potential benefits
  – …but also many potential risks
Benefits …and Risks

• Your home thermostat accesses your calendar to start the AC or furnace in time for when you return from work

• Your smartwatch shares your heart rate with your doctor

• …But would you want…
  – your phone to also report your driving habits to your car insurance provider?
  – your blood pressure to be sent to your health insurance provider?
“Notice and Choice”

• Not everyone feels the same way about these potential privacy risks

• “Notice and Choice” is intended to support informed consent
  – Enshrined in many legal documents
    • Including Hong Kong’s Personal Data (Privacy) Ordinance
Notice and Choice in Practice

- Privacy policies
  - Websites, mobile apps,
- Privacy settings
  - Smartphones, browsers, facebook
A First Quick Question

• How many of you have read a privacy policy over the past month?
People Are Feeling Helpless

• Reading a privacy policy takes about 10 minutes…or about 200 hours/year for an average Internet user… (McDonald & Cranor 2009)

• A typical mobile phone user with 40 mobile apps each requesting 3 permissions would have to configure 120 settings (Lin, Liu, Sadeh, Hong 2014)
The Usable Privacy Policy Project

- Annotate natural language website privacy policies to capture key policy considerations – those that matter to users

- Develop concise, intuitive and effective UIs to convey key information to users
  - Ultimately in a personalized fashion
Approach

• Combining **machine learning, natural language processing** and **crowdsourcing** to scale policy annotation

• **Modeling people’s privacy preferences** to focus on those questions users care about

• **Effective UIs** – browser plug-in(s)

• **Analysis** of website privacy policies
  – Ambiguity, compliance, stated practices
  – Across sectors, within sectors
  – Language addressing specific issues
Tightly Interconnected Threads

Natural Language Privacy Policies of Websites

Semi-Automated Extraction of Privacy Policy Features

Simplified Privacy Policy Models

Policy Analysis

Inform Public Policy

User Privacy Preference Modeling

Key Features of Privacy Policies

User Privacy Profiles

Effective User Interfaces for Privacy Notices

Inform Internet Users

Features for which to elicit user preferences

Identification and generation

Support personalization

Iterative design

Formal models

Semantic features

Features for which policy features to be extracted

Privacy practices to be presented to user

Usable Privacy Policy Project
Initial Focus on 9 Questions

• Collection of contact, location, health, financial data

• Sharing of contact, location, health, financial data
  – Distinguishing between different options (e.g. sharing to support core service vs. sharing for a secondary purpose)

• Deletion of personal data

• Including “Not clear” and “not addressed” options
Crowdsourcing Answers to 9 Questions

Answer the following questions

Question:
Does the policy state that the website might **collect current location** of a user when he/she is using their service?

- [ ] No - the policy states that the website will not collect **current location** information of its user.
- [ ] Yes - the policy states that the website might collect current location information of its user.
- [ ] Unclear - the policy makes statements that could mean the website might collect current location but is not clear about it.
- [ ] Not applicable - the policy does not appear to address the question.

Click here to view the instructions again

Find the answer in the document, highlight the sentences containing the answer, and click the blue button above to paste the text here

Previous

Your Progress: 11%
Initial Work – Amazon Mechanical Turk

**Mechanical Turk** is a marketplace for work.
We give businesses and developers access to an on-demand, scalable workforce.
Workers select from thousands of tasks and work whenever it’s convenient.

**301,177 HITs** available. [View them now.](#)

---

**Make Money**
by working on HITs

HITs - *Human Intelligence Tasks* - are individual tasks that you work on. [Find HITs now.](#)

**As a Mechanical Turk Worker you:**
- Can work from home
- Choose your own work hours
- Get paid for doing good work

---

**Get Results**
from Mechanical Turk Workers

Ask workers to complete HITs - *Human Intelligence Tasks* - and get results using Mechanical Turk. [Get Started.](#)

**As a Mechanical Turk Requester you:**
- Have access to a global, on-demand, 24 x 7 workforce
- Get thousands of HITs completed in minutes
- Pay only when you're satisfied with the results

---

[Usable Privacy Policy Project](#)
Does Crowdsourcing Even Work?

Questions:

• Do Turkers converge (80%) on the correct answer?

• Gold standard obtained from skilled annotators with experience reading privacy policies

• 26 policies, 9 questions, 10 turkers per policy-question pair

<table>
<thead>
<tr>
<th># policy-question pairs with gold standard</th>
<th>80% turkers agree (same answer)</th>
<th>80% turkers agree (different answer)</th>
<th>Turker agreement below 80%</th>
</tr>
</thead>
<tbody>
<tr>
<td>198</td>
<td>36 (75%)</td>
<td>1 (2%)</td>
<td>11 (23%)</td>
</tr>
</tbody>
</table>
Crowdsourcing Does Work…But…

• A single user will often make mistakes…but collectively crowdworkers are able to accurately annotate 75% of policy-question pairs
  – And they rarely seem to converge on erroneous annotations

• …But the process is time consuming: around 20 minutes per policy…
Alternatively Could we Fully Automate?

<table>
<thead>
<tr>
<th>Question Category</th>
<th>Avg. Accuracy</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information collected or inferred</td>
<td>73%</td>
</tr>
<tr>
<td>Entities with which info may be shared</td>
<td>63%</td>
</tr>
<tr>
<td>Retention and Access</td>
<td>64%</td>
</tr>
<tr>
<td>Purposes</td>
<td>59%</td>
</tr>
<tr>
<td>Consent Model (Can users limit?)</td>
<td>68%</td>
</tr>
<tr>
<td>Choice method</td>
<td>74%</td>
</tr>
<tr>
<td>Security and other practices</td>
<td>75%</td>
</tr>
</tbody>
</table>
Our Approach

• Combine crowdsourcing with machine learning and natural language processing

• Find ways of decomposing the problem
  – Reduce the number and complexity of the tasks assigned to crowdworkers
Paragraph Sequencing

• Could we automatically organize paragraphs based on the privacy issues they discuss?

• And use this as a basis for simplifying the work of crowdworkers
Example of 2 paragraphs discussing cookies:

**What About Cookies?**
Cookies are unique identifiers that we transfer to your device to enable our systems to recognize your device and to provide features such as 1-Click purchasing, Recommended for You, personalized advertisements on other Web sites...

...Because cookies allow you to take advantage of some of Amazon.com’s essential features, we recommend that you leave them turned on. For instance, if you block or otherwise reject our cookies, you will not be able to add items to your Shopping Cart, proceed to Checkout, or use any Amazon.com products and services that require you to Sign in...
Instructions:

- Your task is to read **two text descriptions** extracted from **website privacy policies**. Example privacy policies include: Amazon Privacy Notice, Ebay Privacy Policy.
- You will **select 1-3 keywords** for each description, and **check "yes" or "no"** to decide if the two descriptions are discussing the same **privacy issue** or not.
- **Example privacy issues** may include: collection of personal information, sharing information with third parties, cookies and other tracking techniques, data security, policies for children, contact of the merchant, etc.

Example:

**Description 1:**
Choice/Opt-out. If we ever send you information by email concerning new products, services or information that you did not expressly request, we will provide you with an email address by which you may request no further notices.

**Keywords:** choice, opt-out

**Description 2:**
You may also opt-out of your participation in most of the ABC's digital services. Information about how to opt-out will be provided in the particular service. However, you should be aware that the ABC may continue to store personal information provided by you prior to you opting-out.

**Keywords:** opt-out

**Are they discussing the same privacy issue? Yes.** Both of the descriptions are discussing the "opt-out" options provided to the website users, although the detailed terms may be different.
Privacy Policy Dataset

1010 privacy policies collected during December 2013 to January 2014, ranging over 15 website categories

<table>
<thead>
<tr>
<th>Arts</th>
<th>Business</th>
<th>Computers</th>
<th>Games</th>
<th>Health</th>
</tr>
</thead>
<tbody>
<tr>
<td>Home</td>
<td>Kids and Teens</td>
<td>News</td>
<td>Recreation</td>
<td>Reference</td>
</tr>
<tr>
<td>Regional</td>
<td>Science</td>
<td>Shopping</td>
<td>Society</td>
<td>Sports</td>
</tr>
</tbody>
</table>

Paragraph Sequencing – Approach

- Hidden Markov model representation
  - Each hidden state represents a privacy issue
  - Each observation represents a text segment

We will not sell, rent or lease your personal information to others except as described in this statement...
Paragraph Sequencing – Algorithms

• Hidden Markov model representation
  – Each hidden state represents a privacy issue
  – Each observation represents a text segment

• System comparison
  – CLUTO: a greedy dividing clustering algorithm
  – EM-HMM: expectation maximization
  – VB-HMM: variational Bayesian inference
Paragraph Sequencing – Evaluation

• Gold-standard: human-labeled paragraph pairs

true positive

false positive

true negative

e tc.
Paragraph Sequencing – Results

- Gold-standard: human-labeled paragraph pairs
- System results
  - HMMs outperform clustering when $K$ is in the range of $[5, 15)$, best performance achieved by HMMs at 87% f-score
  - Using two levels of text granularities (paragraphs and sections), systems achieve similar results on f-scores
Highlighting Technique

• For each of the 9 questions:
  – Look for the presence of key combinations of terms in text highlighted by skilled annotators in answering these questions
  – Learn models that can be used to highlight relevant paragraphs in crowdworker UI
The Information We Collect

At some Turner Network sites, you can order products, enter contests, vote in polls or otherwise express an opinion, subscribe to one of our services such as our online newsletters, or participate in one of our online forums or communities. In the course of these various offerings, we often seek to collect from you various forms of personal information. Examples of the types of personally identifiable information that may be collected at these pages include: name, address, e-mail address, telephone number, fax number, credit card information, and information about your interests in the use of various products, programs, and services.

At some Turner Network sites, you may also be able to submit information about other people. For example, you might submit a person’s name and e-mail address to send an electronic greeting card and if you order a gift online and want it sent directly to the recipient, you might submit the recipient’s name and address. Examples of the types of personally identifiable information that may be collected about other people at these pages include: recipient’s name, address, e-mail address, and telephone number.

At certain parts of some of our sites, only persons who provide us with the requested personally identifiable information will be able to order products, programs, and services or otherwise participate in the site’s activities and offerings.

We, our third party service providers, advertisers, advertising networks and platforms, agencies, and partners may collect various types of non-personally identifiable information when you visit any of our sites. A

Answer the following questions

Click here to view the instructions again

Question 3:
Does the policy state that the website might collect current location about its users?

Select sentence from policy and click

Find the answer in the document, highlight the sentences containing the answer, and click the blue button above to paste the text here

- No - the policy explicitly states that the website will not collect current location information.
- Yes - the policy explicitly states that the website might collect current location information.
- Unclear - the policy does not explicitly state whether the website might collect current location information or not, but the selected sentences could mean that the current location information might be collected.
- Not applicable - this question is not addressed by this policy.
## Impact on Accuracy

<table>
<thead>
<tr>
<th>Condition</th>
<th>Correct</th>
<th>Wrong</th>
<th>No Convergence</th>
</tr>
</thead>
<tbody>
<tr>
<td>NOHIGH</td>
<td>76 (84.4%)</td>
<td>4 (4.4%)</td>
<td>10 (11.1%)</td>
</tr>
<tr>
<td>TOP05</td>
<td>74 (82.2%)</td>
<td>9 (10%)</td>
<td>7 (7.8%)</td>
</tr>
<tr>
<td>TOP10</td>
<td>81 (90.0%)</td>
<td>3 (3.3%)</td>
<td>6 (6.7%)</td>
</tr>
</tbody>
</table>

Performance on 90 policy-question pairs

NOHIGH = No Highlights
TOP 05 = 5 Highlighted Paragraphs
TOP 10 = 10 Highlighted Paragraphs

Note: on average a policy has a little over 40 paragraphs

Suggests possible improvements in both accuracy and productivity
Next Steps

• Adaptive Crowdsourcing:
  – Dynamically adjust number of crowdworkers
  – Distinguish between crowdworkers & optimize the allocation of crowdworkers to tasks

• More organic annotation process
  – Annotate finer grain issues

• Public crowdsourcing site: Q1 2016
Simple Browser Plug-In

Example of Privacy Nutrition Label

<table>
<thead>
<tr>
<th>Acme</th>
<th>ways we use your information</th>
<th>information sharing</th>
</tr>
</thead>
<tbody>
<tr>
<td>information we collect</td>
<td>provide service and maintain site</td>
<td>other companies</td>
</tr>
<tr>
<td>contact information</td>
<td>marketing</td>
<td>opt out</td>
</tr>
<tr>
<td></td>
<td>telemarketing</td>
<td>opt out</td>
</tr>
<tr>
<td>cookies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>demographic information</td>
<td></td>
<td>opt out</td>
</tr>
<tr>
<td>financial information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>health information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>preferences</td>
<td></td>
<td>opt out</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>purchasing information</td>
<td></td>
<td>opt out</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>social security number &amp; govt ID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>your activity on this site</td>
<td></td>
<td>opt out</td>
</tr>
<tr>
<td>your location</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Access to your information
This site gives you access to your contact data and some of its other data identified with you.
How to resolve privacy-related disputes with this site
Please email our customer service department

acme.com
5000 Forbes Avenue
Pittsburgh, PA 15213
United States
Phone: 800-555-5555
help@acme.com

Informed by Mental Models

Key Insight: Highlight What Users Do Not Expect

User data collection & sharing expectations for 3 categories of websites: financial, health and dictionary
But Simple UI’s Many Not Be Enough

….How do we motivate users to pay attention?
Helping Users Manage Privacy Settings: Explosion of Settings
Another Quick Question

• How many of you know what mobile apps are currently running on their smartphones and what information they collect?
People’s Response When They Find Out...

Percentages of people surprised by an App’s Permission Requests

- Location
- Device ID
- Contact List

Facebook (rank 1)

- 60% Location
- 60% Device ID
- 0% Contact List

Angry Bird (rank 3)

- 40% Location
- 80% Device ID
- 0% Contact List

Pandora (rank 4)

- 40% Location
- 80% Device ID
- 0% Contact List

Brightest Flashlight (rank 78)

- 95% Location
- 95% Device ID
- 0% Contact List

Helping Users Manage Privacy Settings

- ...Beyond understanding privacy policies...
- Do permission managers help users (e.g. iOS, Android App Ops)?
- Could nudges help increase user awareness and motivate users to take a closer look at their settings?
Field Study

• 22-day study with 23 participants using their regular Android phone

• **Week 1:** baseline

• **Week 2:** App Ops permission manager

• **Final 8 days:** App Ops + one daily nudge focused on one permission

• Collected detailed logs of all permission changes + pre- and post-surveys
Your location has been shared 5398 times with Facebook, Groupon, GO Launcher EX, and 7 other apps for the past 14 days.

<table>
<thead>
<tr>
<th>Number of times your location has been shared with each app for the past 14 days.</th>
<th>Let me change my settings</th>
<th>keep sharing my location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Google Play services</td>
<td>1603</td>
<td>Let me change my settings</td>
</tr>
<tr>
<td>Android System</td>
<td>1602</td>
<td>keep sharing my location</td>
</tr>
<tr>
<td>Groupon</td>
<td>1602</td>
<td>Let me change my settings</td>
</tr>
<tr>
<td>Weather &amp; Clock Widget</td>
<td>296</td>
<td>keep sharing my location</td>
</tr>
<tr>
<td>GO Launcher EX</td>
<td>255</td>
<td>Let me change my settings</td>
</tr>
<tr>
<td>Maps</td>
<td>18</td>
<td>keep sharing my location</td>
</tr>
<tr>
<td>Viber</td>
<td>11</td>
<td>Let me change my settings</td>
</tr>
<tr>
<td>Facebook</td>
<td>5</td>
<td>keep sharing my location</td>
</tr>
<tr>
<td>Google Search</td>
<td>3</td>
<td>Let me change my settings</td>
</tr>
<tr>
<td>MyFoodCoach Study</td>
<td>3</td>
<td>keep sharing my location</td>
</tr>
</tbody>
</table>

Notification provided by AppOps.
Implementation of Study App

• Developed & installed an Android app that was used:
  – To launch AppOps
  – Collect detailed AppOps logs
    • What permissions apps are allowed to access
      – Including changes to settings made by user, when and through which interface (e.g. from the nudge or directly via AppOps)
    • For each app-permission pair:
      – Last time the app tried to access the permission
      – Each app request & whether it was granted/denied
      – Whether the app is currently using the permission and for how long (e.g. camera, recording audio)
Demographics & Additional Details

- **23 participants** (65% female; ages 18–44, median=23)
  - 21 owned Samsung devices and 2 owned an HTC One.
- On average, 89 apps installed (SD=22), including services and pre-installed apps.
- **21 (91%) reported never using AppOps before**
  - 1 had used AppOps, and 1 was unsure.
- **Phase 1 users could not access App Ops**
  - *We checked that no other App Ops launcher was installed on their phones and our App did not allow them during that week to access App Ops.*
## Permission Managers Are Not Enough

- Nudges can make a big difference

### Week 2: Permission Manager Only

### Week 3: Daily Nudges
Permission Manager w/o Privacy Nudges

• In phase 2, participants reviewed their app permissions **51 times**, restricted **76 distinct apps** from accessing a total of **272 permissions**

• Only one interaction where a user opened access to one permission.
Reviewing of App Permissions During Phase 2

- 22 participants (95.6%) reviewed their app permissions at least once.
  - 12 reviewed their app permissions multiple times.
- One did not review his permissions in phase 2.
Adjusting App Permissions

- 15 (65%) participants restricted 272 app-permission pairs from 76 distinct apps, including both participant-installed and pre-installed apps.

- Participants restricted apps’ access to:
  - Location: 74 (27%)
  - Contacts: 57 (21%)
  - Calendar: 10 (4%)
  - Call logs: 9 (3%).
  - Others included: Camera: 42 (9%), SMS: 21 (8%), Post notification: 19 (7%), Recording audio: 15 (6%).

- Only one participant opened back a permission to the Weather Channel app - to send notifications.
Why did participants restrict apps’ access to permissions?

• Participants restricted unused apps, especially pre-installed apps.
  – P10 stated: “I also blocked [a] bunch of AT&T bloatware from accessing any information. I don’t use them anyways.”

• Participants restricted permissions required for unused functionality.
  – P13 restricted iHeartRadio access to location, explaining: “I know what stations I want to listen to no matter where I am so I turn off the location.”
Why did participants restrict apps’ access to permissions? (continued)

• Participants restricted apps when the purpose to access their personal information was unclear.
  – P4 stated: “[I turned it off] because I can’t think of a reason why Inkpad needs my location.”
Adding Privacy Nudges – Final 8 days

• Do nudges further change user behavior and how do they feel about them?
Effectiveness of Privacy Nudges – Final 8 days

• In phase 3, participants reviewed their app permission 69 times, restricted 47 distinct apps from accessing 122 permissions, and permitted six apps access to six permissions.

• …this is after a week with access to App Ops.
Reviewing App Permissions

- Participants could review their app permissions either by
  1. Opening AppOps directly (same as in phase 2)
  2. Opening AppOps in response to a nudge.
Reviewing App Permissions

• 22 participants (95.6%) reviewed their app permissions at least once in phase 3.
  – 21 participants reviewed their apps’ permissions in response to nudges:
    • 53 times (78% of the time) in response to a nudge
    • 15 times (22%) by directly opening AppOps.
  – 1 participant reviewed her apps’ permissions only once and only by directly opening AppOps.

• The privacy nudges were the primary trigger for participants to review their app permissions.
Adjusting App Permissions

• Participants restricted 122 permissions - breakdown:
  – **Location**: 30 (25%)
  – **Contacts**: 25 (20%)
  – **Calendar**: 8 (7%)
  – **Call logs**: 6 (5%).
  – Other restricted permissions included:
    • Post notification: 10 (8%), SMS: 9 (7%), camera: 7 (6%), record audio: 7 (6%).

• Only three participants made *permissive adjustments due to loss of app functionality*.
  – In the interview, P10 noted that he restricted and later permitted Facebook’s access to the clipboard, because he was unable to copy & paste in Facebook.
Concluding Remarks - I

• “Notice and Choice” is the de facto approach to privacy on the Web
• Even on the fixed Web, this approach does not work
• On smartphones and with the emerging Internet of Things, this framework (in its current form) simply does not scale
Concluding Remarks - II

- **Usability research** is key to understanding what users can realistically be expected to do and can inform the design of more realistic implementations of Notice and Choice.

- **Artificial Intelligence**, which is often blamed for many of the privacy risks we face in the Internet of Things, may also hold part of the solution to scaling Notice and Choice.
  - Machine Learning & NLP to **annotate privacy policies**
  - Personalized Privacy Assistants for **personalized summaries of policies**, learning our privacy **preferences** and **nudging** us to examine our privacy settings.
Apps Snoop on Your Location Way More Than You Think

But Professor **Norman Sadeh**, a member of the research team that conducted the research, says the volume of location-harvesting isn't the ... What do your mobile apps tell third parties?

Carnegie Mellon study: your apps are tracking you more than you ...

How Often Does an App Share Your Location? You May Be Surprised

You'll Be Freaked Out to Learn How Often Your Apps Share Your ...

Where Were You 3 Minutes Ago? Your Apps Know

**Explore in depth** (37 more articles)

Does Your Cellphone Know Too Much?

... private information, they tried to limit future sharing, according to **Norman Sadeh**, a Carnegie Mellon University computer science professor.

Your location has been shared 5398 times .... 'Are you kidding me?'

“The vast majority of people have no clue about what's going on,” said **Norman Sadeh**, a professor in the School of Computer Science's
Acknowledgements: Work funded by the National Science Foundation, Google and Samsung

The Usable Privacy Policy Project involves a collaboration with a number of individuals. See usableprivacy.org for additional details

Q&A