

**Carnegie  
Mellon  
University**

CyLab

# Privacy, Law, and Smartphones

Rebecca Balebako

Oct. 29, 2015

**Engineering &  
Public Policy**



# Agenda

- Quiz
- Reading discussion
- Permission notices on major platforms
- Policy on smartphone privacy
- Research on smartphone privacy

# By the end of class....

- Understand privacy concerns around smartphones
- Understand how privacy notices on smartphones are evolving
- Identify the research questions in several smartphone privacy research projects
- Recognize several methods for addressing the research questions

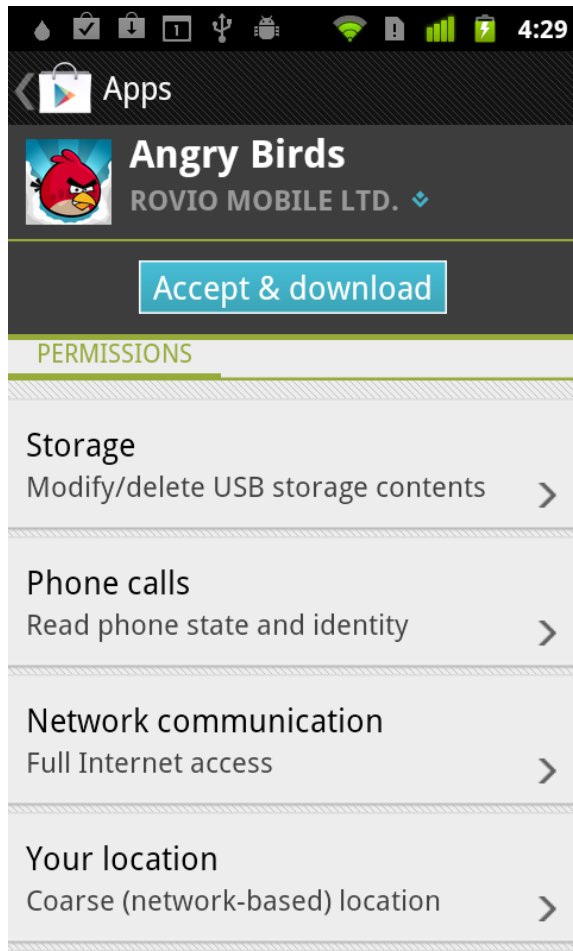
# Smartphones allow data sharing



# Privacy and security concerns

- Immature technology
- Phones always with user and always on
- Data sharing might be unknown to user
  - Sensors (GPS location, camera, accelerometer, gyroscope)
- Inferences can be made

# Permissions warnings differ on time and content



Android 2012



iOS 2012








# Android Permission Manager (AppOps)








- Introduced in Android 4.3, albeit hidden by default.
  - need a launcher app.
- Made in completely inaccessible in Android 4.4.2.
- Next version of Android will have just-in-time permissions

# Research questions

- Would AppOps provide any benefit to smartphone users?
- Would additional notices or nudges benefit users?



App ops		
LOCATION	PERSONAL	
	<b>Google Play services</b> wi-fi scan, cell scan, fine location, GPS, coarse location	0 mins ago
	<b>Android System</b> fine location, coarse location	1 min ago
	<b>The Weather Channel</b> fine location, coarse location	2 mins ago
	<b>Facebook</b> cell scan, fine location, GPS, coarse location, wi-fi scan	17 mins ago
	<b>GO SMS Pro Theme Butterfly</b> fine location, coarse location	August 28
	<b>Settings</b> wi-fi scan, coarse location, fine location	June 16
	<b>Piano Tiles</b> wi-fi scan, coarse location	May 5

App ops		
LOCATION	PERSONAL	MESSAGING
	<b>Messaging</b> read contacts	2 mins ago
	<b>Google Search</b> read contacts, read calendar	3 mins ago
	<b>Calendar Storage</b> read calendar, modify calendar	3 mins ago
	<b>Viber</b> read contacts, modify contacts, read call log	6 mins ago
	<b>Google Keyboard</b> read contacts	6 mins ago
	<b>GO SMS Pro</b> read contacts, read call log	6 mins ago
	<b>Facebook</b> read contacts	7 mins ago

# Privacy Nudge

# Detailed Report

Your location shared with 10 apps

**Did you know?**  
Your **location** has been shared **5398** times with Facebook, Groupon, GO Launcher EX, and 7 other apps for the past **14** days.

[Let me change my settings](#)

[Show me more before I make changes](#)

[Keep sharing my location](#)

Notification provided by AppOps.

Your location shared with 10 apps

Number of times your **location** has been shared with each app for the past 14 days.

Google Play services	1603
Android System	1602
Groupon	1602
Weather & Clock Widget	296
GO Launcher EX	255

[Let me change my settings](#)

[keep sharing my location](#)

Your location shared with 10 apps

Number of times your **location** has been shared with each app for the past 14 days.

Maps	18
Viber	11
Facebook	5
Google Search	3
MyFoodCoach Study	3

[Let me change my settings](#)

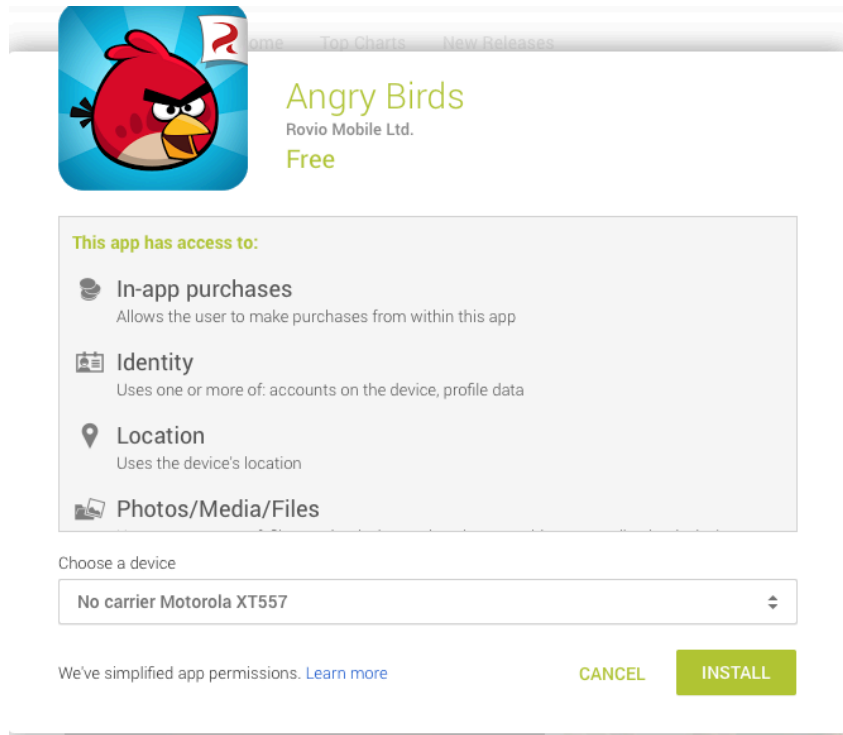
[keep sharing my location](#)

[Your Location has been Shared 5,398 Times! A Field Study on Mobile App Privacy Nudging](#)

H Almuhimedi, F Schaub, N Sadeh, I Adjerid, A Acquisti, J Gluck, ...

CHI '15: ACM CHI Conference on Human Factors in Computing Systems

# 2014: Android layered the permissions



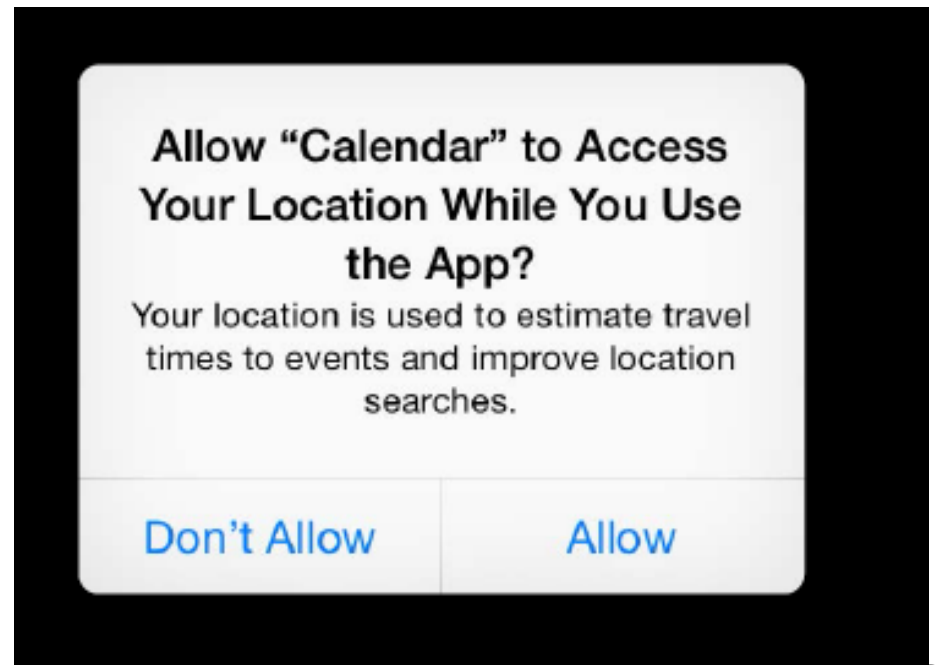
- Location now represents all types of location
- “Network” permissions no longer on top layer

Google Play Store, Oct 19, 2014

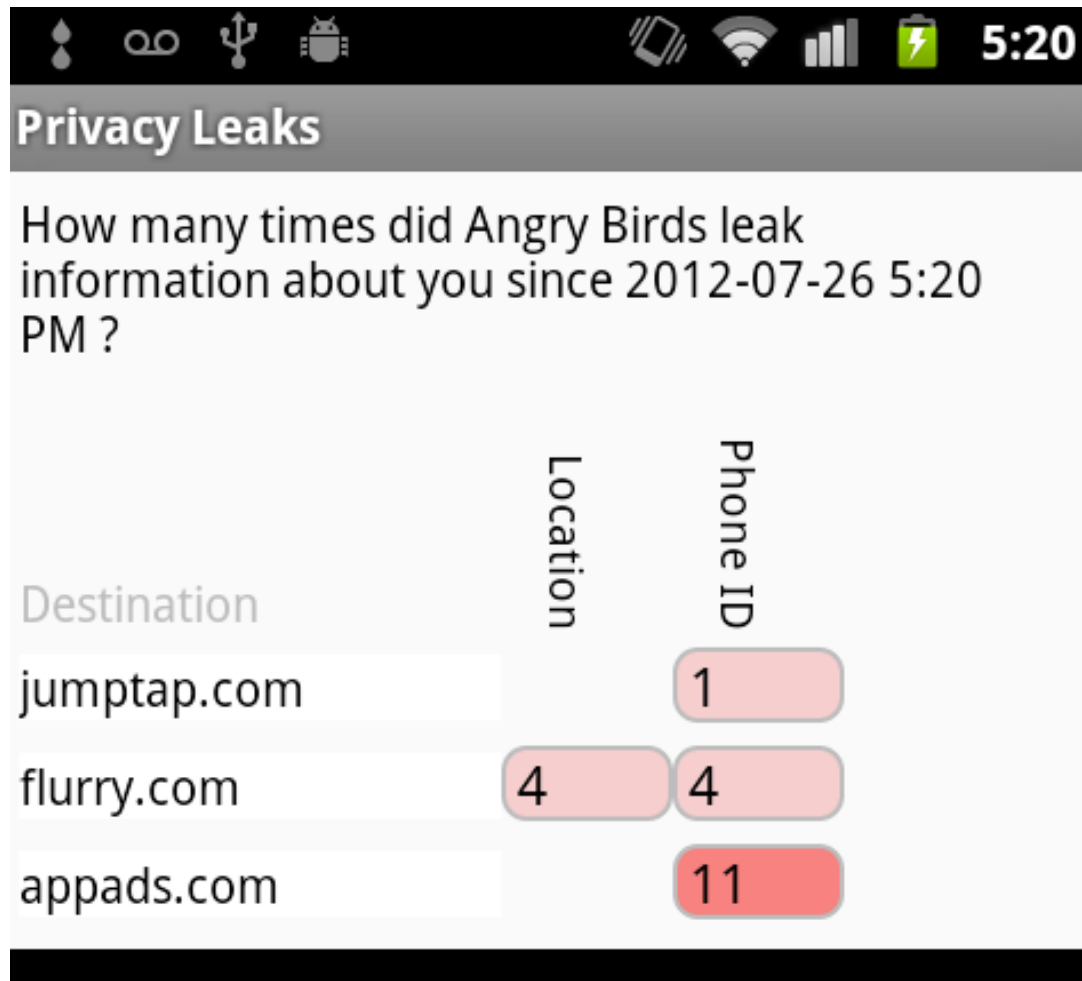
[https://support.google.com/googleplay/answer/6014972?p=app\\_permissions&rd=1](https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1)

# iOS8 privacy settings

- Limit Ad tracking
- Developers required to include a purpose string
- More “data classes”:
  - Location
  - Contacts
  - Calendar
  - Reminders
  - Photos
  - Camera
  - Microphone
  - Health Kit
  - Motion Activity
  - Social



# A large chunk of the data-sharing ecosystem is invisible



# Recent Policy: FTC Staff Report



## **Mobile Privacy Disclosures**

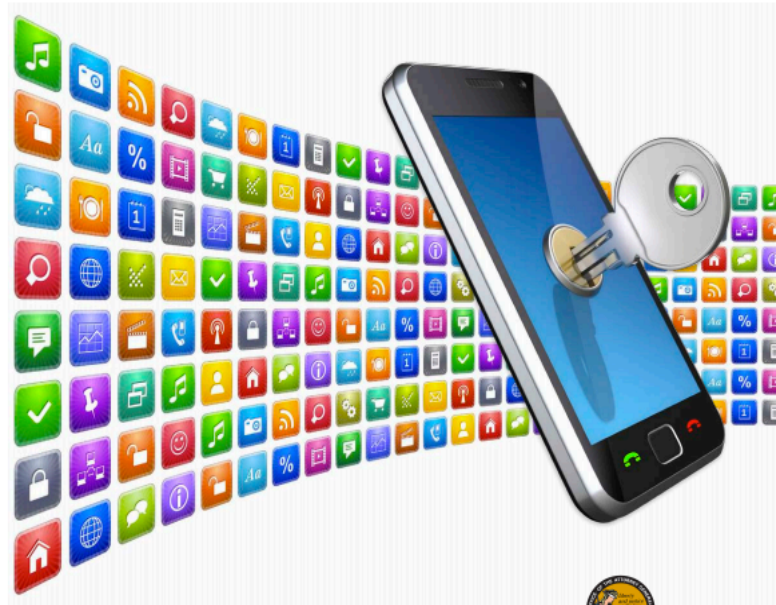
Building Trust Through Transparency

# California Attorney General

## PRIVACY ON THE GO

RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM

January 2013



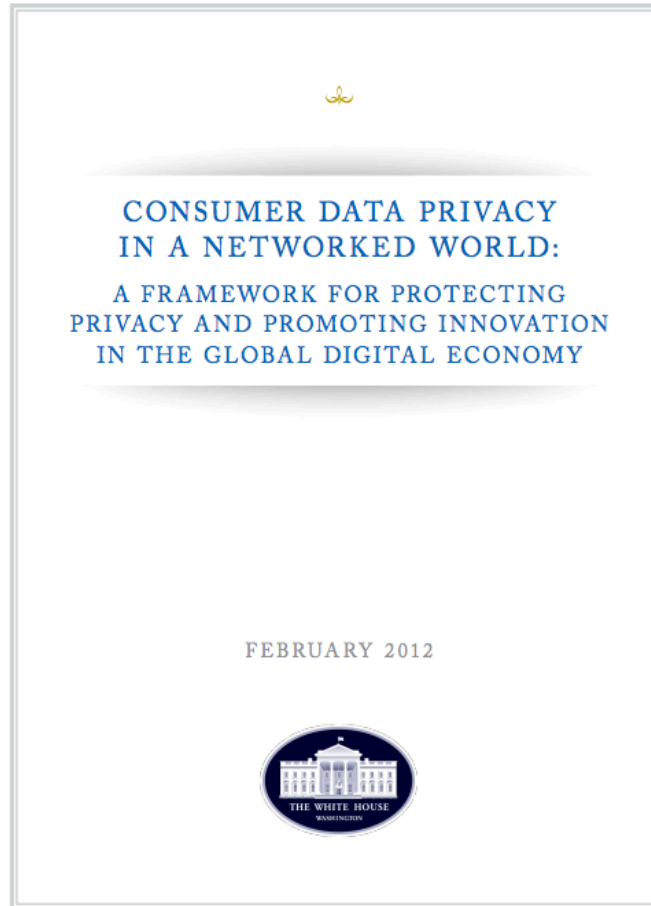
Kamala D. Harris, Attorney General  
California Department of Justice

# App Developers Should...

- Data checklist for PII
- Avoid or limit PII
- Develop a privacy policy
- Limit data collection
- Limit data retention
- Special notices for unexpected data practices “to enable meaningful practices”
- Give users access



# White House Consumer Privacy Bill of Rights



# Developing Policy: NTIA MSHP



**NTIA** National Telecommunications & Information Administration  
United States Department of Commerce

**TOPICS** **NEWSROOM** **PUBLICATIONS** **BLOG** **OFFICES** **ABOUT**

[Spectrum Management](#)  
[Broadband](#)  
[Internet Policy](#)  
[Domain Name System](#)  
[Public Safety](#)  
[Grants](#)  
[Institute for Telecommunication Sciences](#)

[Home](#) » [Publications](#) » [Other Publications](#) » [2013](#)

## Privacy Multistakeholder Process: Mobile Application Transparency

**Topics/Subtopics:**  
[Internet Policy Task Force](#) [Privacy](#) [Internet Policy](#)

**Date:**  
February 21, 2013

 [Printer-friendly version](#)

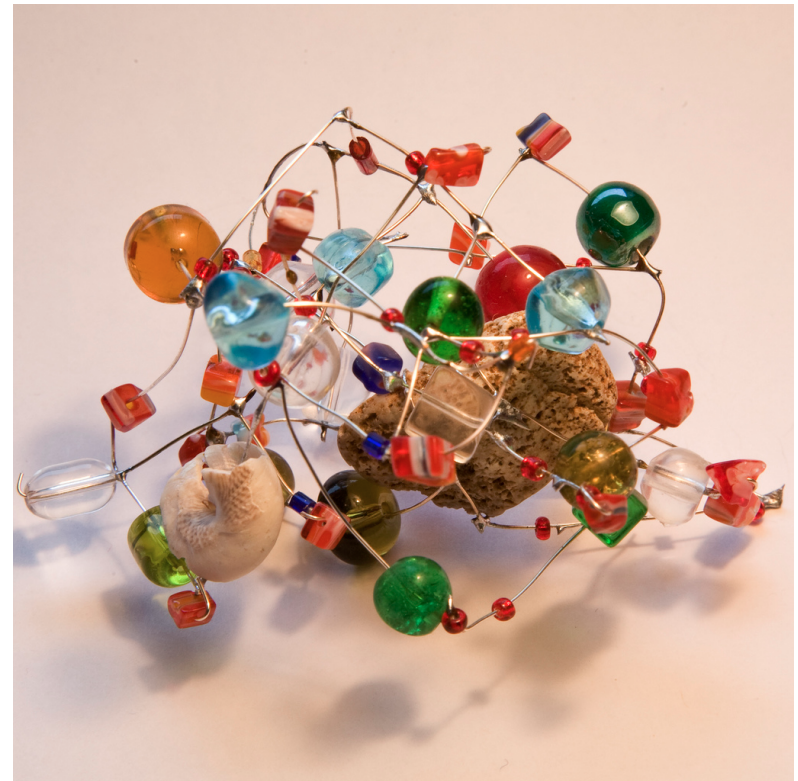
This web page provides details on the NTIA-convened privacy multistakeholder process regarding mobile application transparency. On June 15, 2012, NTIA announced that the goal of the first multistakeholder process is to develop a code of conduct to provide transparency in how companies providing applications and interactive services for mobile devices handle personal data.

# Multi-stakeholder process (MSHP)

- Open meetings
- MSHP vs. self-regulation

# NTIA MSHP vs W3C

- Communication (email, in-person, etc.)
- Goal (Code of Conduct vs. tech standard)
- Novelty of MSHP



Credits – Michael Heiss / Flickr

# NTIA Code of Conduct: Data Types

- Biometrics (information about your body, including fingerprints, facial recognition, signatures and/or voice print.)
- Browser History and Phone or Text Log (A list of websites visited, or the calls or texts made or received.)
- Contacts (including list of contacts, social networking connections or their phone numbers, postal, email and text addresses.)
- Financial Information (Includes credit, bank and consumer-specific financial information such as transaction data.)
- Health, Medical or Therapy Information (including health claims and information used to measure health or wellness.)
- Location (precise past or current location and history of where a user has gone.)
- User Files (files stored on the device that contain your content, such as calendar, photos, text, or video.)

# NTIA Code of Conduct: Third-Party Entities

- Ad Networks (Companies that display ads to you through apps.)
- Carriers (Companies that provide mobile connections.)
- Consumer Data Resellers (Companies that sell consumer information to other companies for multiple purposes including offering products and services that may interest you.)
- Data Analytics Providers (Companies that collect and analyze your data.)
- Government Entities (Any sharing with the government except where required or expressly permitted by law.)
- Operating Systems and Platforms (Software companies that power your device, app stores, and companies that provide common tools and information for apps about app consumers.)
- Other Apps (Other apps of companies that the consumer may not have a relationship with)
- Social Networks (Companies that connect individuals around common interests and facilitate sharing.)

# What is the research question?

- Can users understand the terms used in the NTIA short form policy?
- How can we find the answer?

# A Case Study on the Role of Usability Studies in Developing Public Policy : Web Survey

- 791 participants from Amazon mturk
  - 51% female
  - Age 18-73 years (mean 33, std 11)
- Asked to categorize realistic app-sharing scenarios



# Scenario example

The SuperTax app lets you fill out and submit your tax forms quickly and easily.

SuperTax will take a picture of your W-2. It will answer questions about your financial information, including salary and interest income.

It will then submit your return to state and federal agencies.

The scenarios describe the data collection and sharing completely, so **you do not need to guess anything outside of what is described.**

16. For each data collected by the app, what type of data is it?

	Biometrics	Browser History and Phone or Text Log	Contacts	Financial Information	Health, Medical or Therapy Information	Location	User Files	None of the Above	Not Sure
Photo of W-2	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Salary	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Interest Income	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

# Parenthetical condition

The different types of entities with which data can be shared are defined as follows:

- Ad Networks (Companies that display ads to you through apps.)
- Carriers (Companies that provide mobile connections.)
- Consumer Data Resellers (Companies that buy and/or sell consumer information to other companies for multiple purposes including offering products and services that may interest you.)
- Data Analytics Providers (Companies that collect and analyze your data.)
- Government Entities (Any sharing with the government except where required or expressly permitted by law.)
- Operating Systems and Platforms (Software companies that power your device, app stores, and companies that provide common tools and information for apps about app consumers.)
- Other Apps (Other apps of companies that the consumer may not have a relationship with)
- Social Networks (Companies that connect individuals around common interests and facilitate sharing.)

**27. Apps can share data with different categories of entities. For each of the entities with which this app shares data, what category would best describe the entity?**

	Ad Networks	Carriers	Consumer Data Resellers	Data Analytics Providers	Government Entities	Operating Systems and Platforms	Other Apps	Social Networks	None of the Above	Not Sure
State Agency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Federal Agency	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

# Users struggled to understand the terms

- Participants had high common understanding of:
  - Facebook = Social Network
  - Government Entities
  - Carriers
- Participants had low common understanding of:
  - Consumer Data Reseller
  - Data Analytics Providers
  - Ad Networks

Is Your Inseam a Biometric? A Case Study on the Role of Usability Studies in Developing Public Policy

Balebako, R., Shay, R., Cranor, L. In USEC 2014

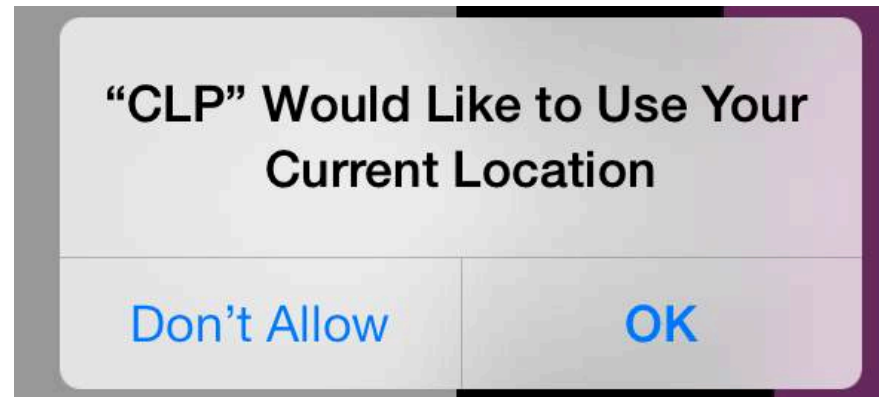
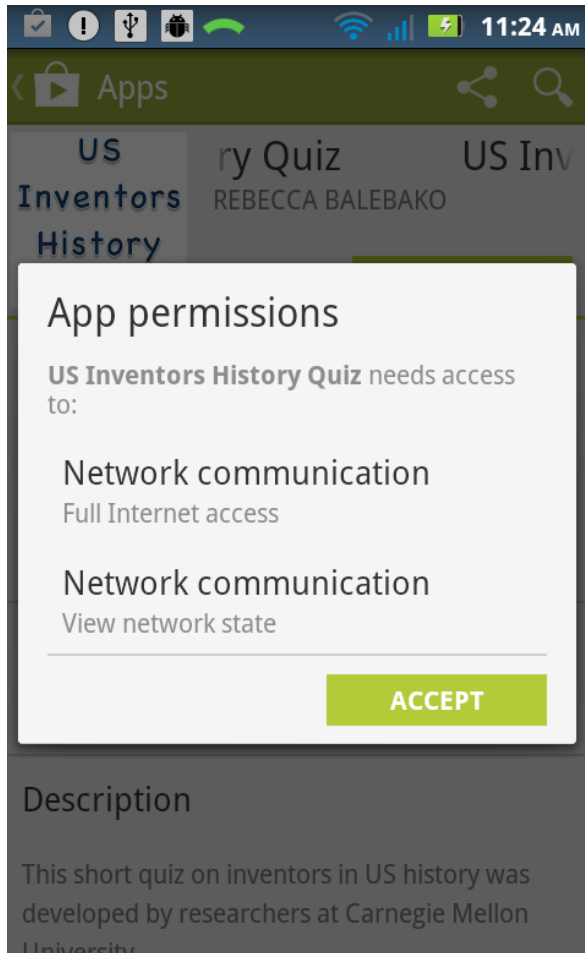
# Why was the result of the NTIA MSHP so bad?

- Process Fatigue
- What is usability?
- Cost of usability tests
- Process issues

# Different Study



# Current permissions requests are not sufficient for informed choice



# What is the research question?

- Does timing impact whether privacy notices are effective?
- What do we mean by effective?
- What do we mean by timing?

# What makes a privacy notice effective?

- The notice should have information people care about.
- A privacy notice should be salient; people should notice it.
  - Recall is a measure of salience



# Contributions from this paper

- Salience of smartphone privacy notices can be improved through timing
- We provide recommendations on how to integrate privacy notices into apps for improved recall
- We provide design guidelines for improving privacy notices in the app store

# Does timing matter? Which option is best?

- Smartphone apps can display privacy notices at many points

- In the app store

- During install

- Before use

- During use

- After use

Before app is on the phone


App is on the phone and in use

# Method to measure impact of timing on recall

1. Participants completed consent form and demographic questions
2. Installed and played the app
3. Experienced a distractor or delay
4. Answered recall questions
5. Evaluated the notice

# Simple app quiz on American inventors

**Question 10 of 11**



Madame C. J. Walker (1867-1919) was the first African-American female millionaire. Her business included products she invented such as:

bifocals

the parachute

**the lightening rod**

hair-growing lotion

Oops!! The correct answer is "hair-growing lotion"


NEXT

# The privacy notice

US Inventors History Quiz


## Privacy Notice

### What do we collect?

  
Browser History

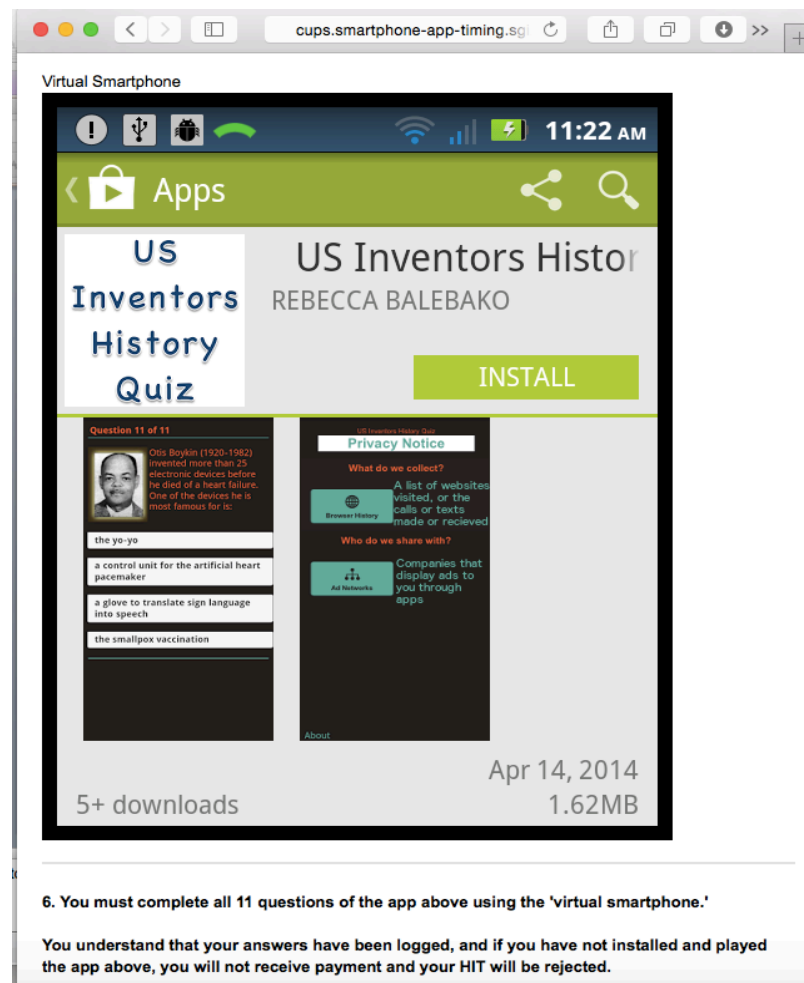
A list of websites visited, or the calls or texts made or received.

### Who do we share with?

  
Ad Networks

Companies that display ads to you through apps.

# Web survey used iFrame to mimic smartphone



The screenshot shows a browser window with the URL `cups.smartphone-app-timing.cgi`. The browser title is "Virtual Smartphone". The page content is a mobile app listing for "US Inventors History Quiz" by REBECCA BALEBAKO. The app card includes an "INSTALL" button, a "5+ downloads" badge, and a date of "Apr 14, 2014" with a size of "1.62MB". Below the app card, there is a "Privacy Notice" section with two sub-sections: "What do we collect?" and "Who do we share with?". The "What do we collect?" section lists "Browser History" and "Ad Networks". The "Who do we share with?" section lists "Companies that display ads to you through apps".

6. You must complete all 11 questions of the app above using the 'virtual smartphone.'

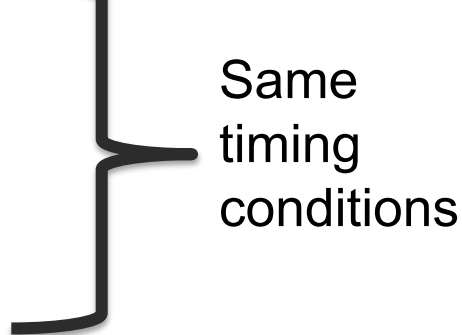
You understand that your answers have been logged, and if you have not installed and played the app above, you will not receive payment and your HIT will be rejected.

# Participants were assigned to a timing condition

- Not Shown
- App Store
- Before use
- During use
- After use



# We approached this problem using<sup>40</sup> both web surveys and a field experiment

- Web Survey (277 Mturk participants)
    - Participants played a virtual app online
  - Field Experiment (126 participants)
    - Participants downloaded and played an app quiz
- 
- Same  
timing  
conditions



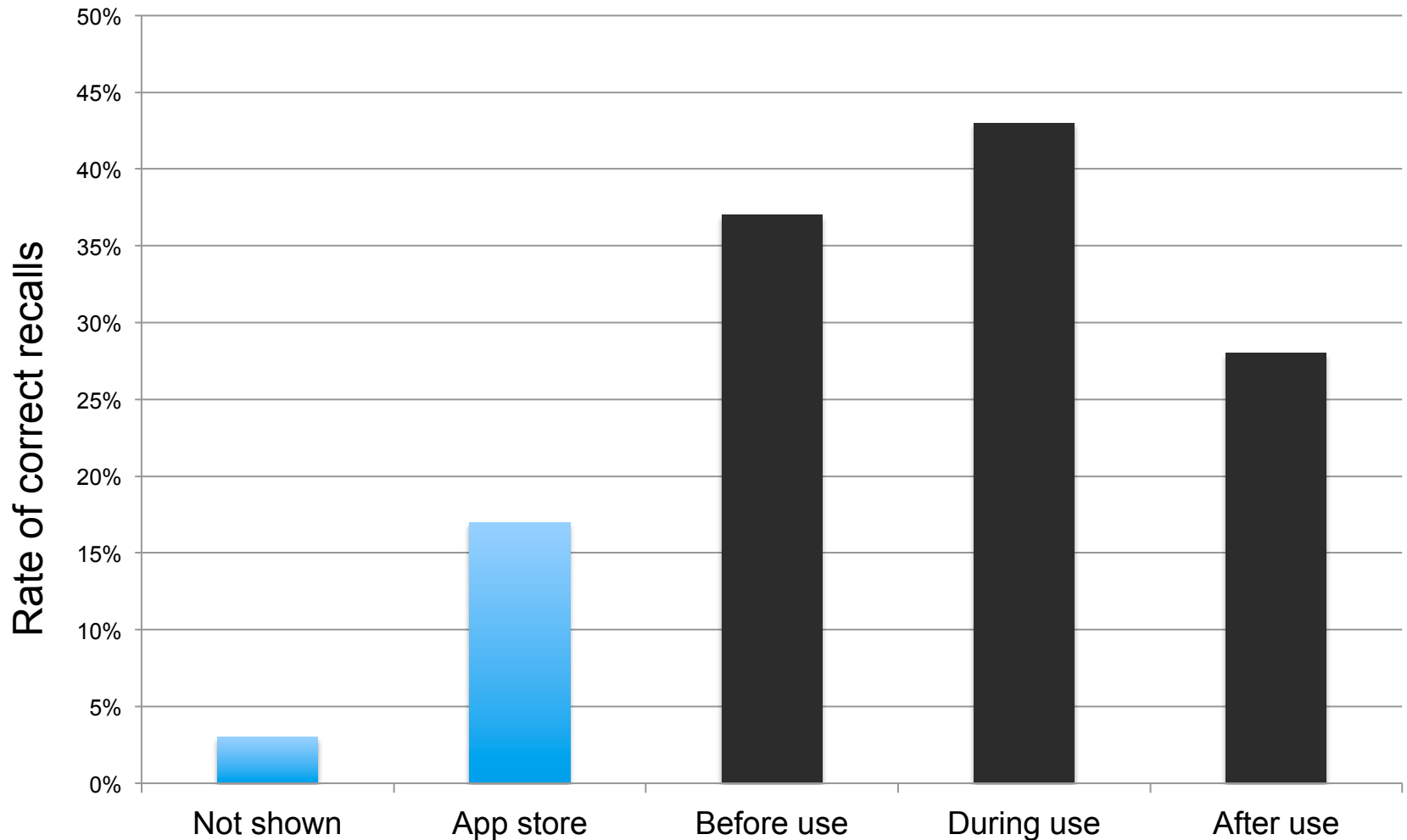
# A Follow-up web survey used new conditions

- Web Survey (277 Mturk participants)
    - Participants played a virtual app online
  - Field Experiment (126 participants)
    - Participants downloaded and played an app quiz
  - Follow-up Web Survey (326 participants)
    - Participants played a virtual app online
- 
- Same timing conditions
- New timing conditions

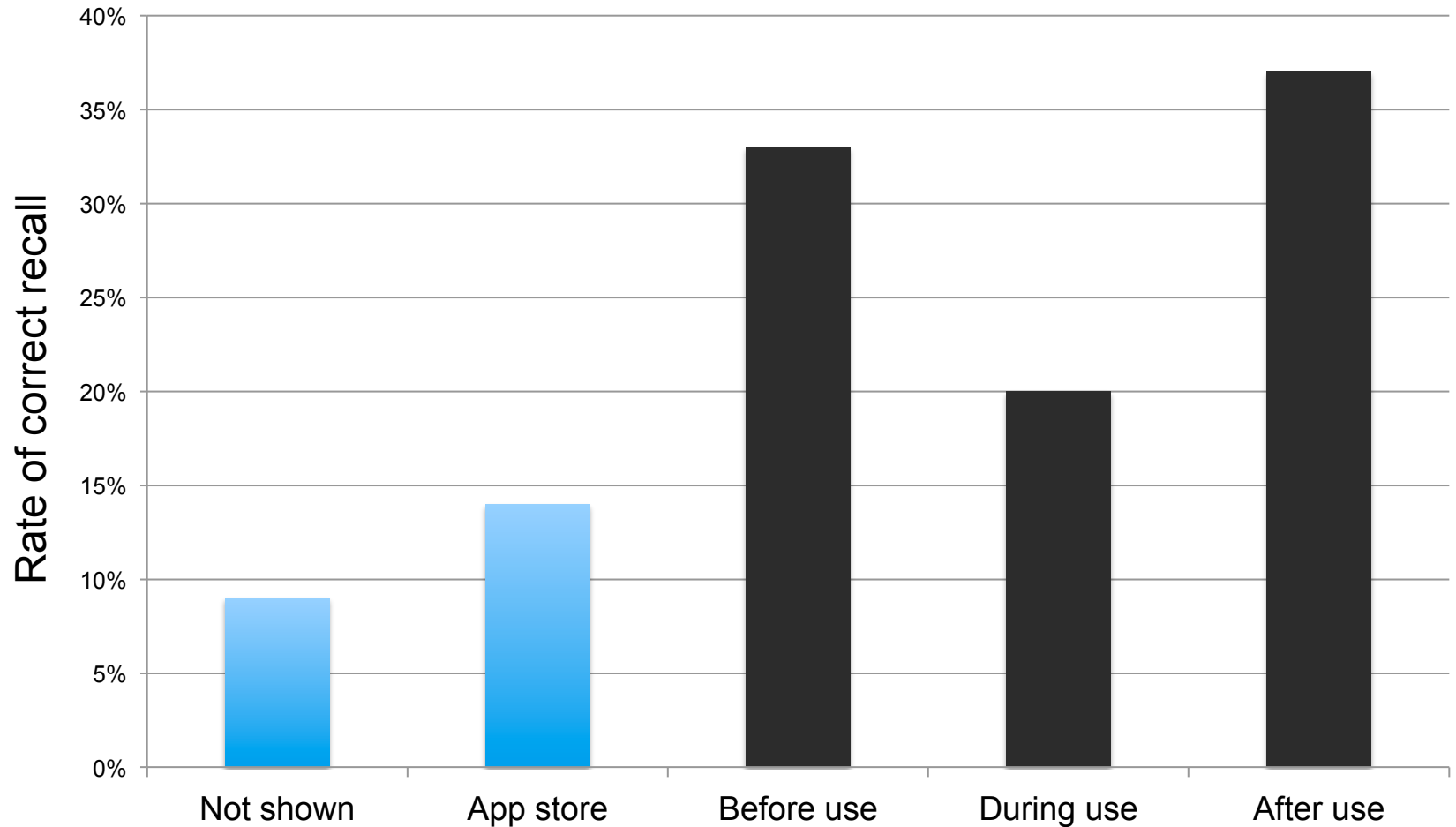
# All participants completed following steps

1. Completed consent form and demographic questions
2. Installed and played the app
3. Experienced a distractor or delay
  - Web survey: questions about privacy preferences
  - Field experiment: 24 hours
4. Answered recall questions
5. Evaluated the notice

# Rate of Recall for Notice – Web Survey



# Rate of Recall for Notice – Field Study



# Participants wanted to remember what was in notice

I would want notifications like this when I download or use an app

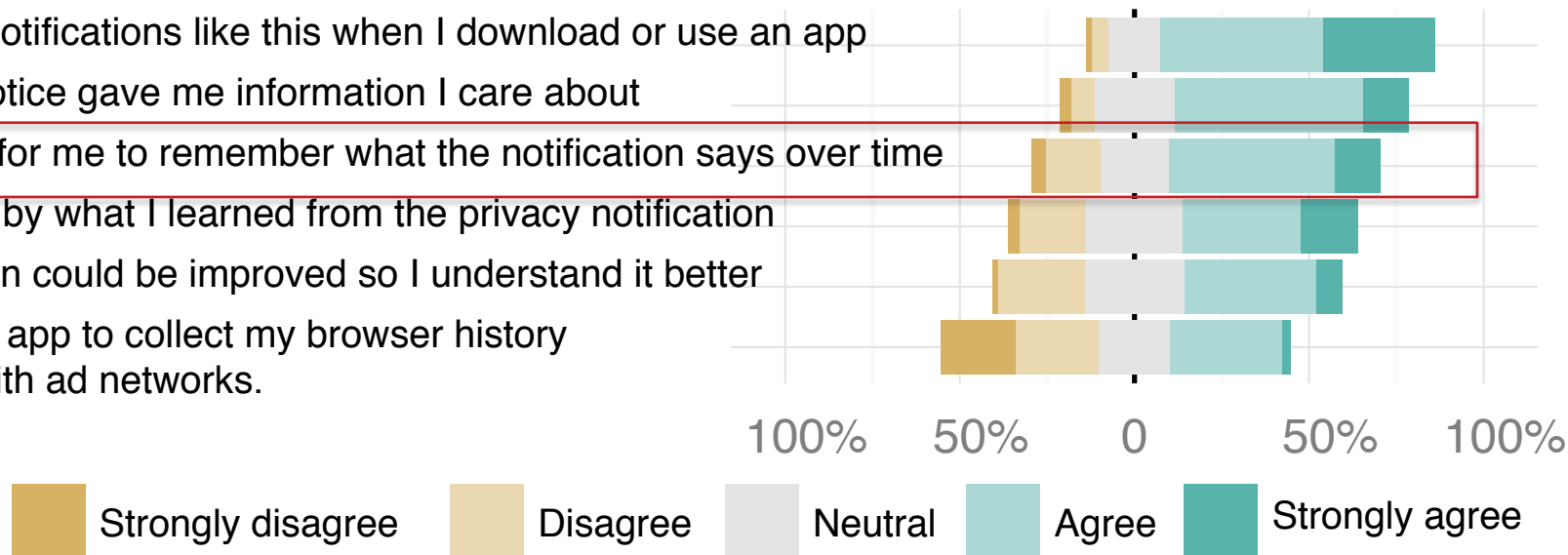
The privacy notice gave me information I care about

It is important for me to remember what the notification says over time

I was surprise by what I learned from the privacy notification

This notification could be improved so I understand it better

I expected the app to collect my browser history and share it with ad networks.



# Why did app store perform so poorly?

US Inventors History Quiz

REBECCA BALEBAKO

INSTALL

Question 11 of 11

Otis Boykin (1920-1982) invented more than 25 electronic devices before he died of a heart failure. One of the devices he is most famous for is:

the yo-yo

a control unit for the artificial heart pacemaker

a glove to translate sign language into speech

the smallpox vaccination

Privacy Notice

What do we collect?

A list of websites visited, or the calls or texts made or received.

Who do we share with?

Companies that display ads to you through apps.

Apr 14, 2014

5+ downloads

1.62MB

Be the first to +1 this.

Rate this app

US Inventors History Quiz

INSTALL

US Inventors History Quiz

Privacy Notice

What do we collect?

A list of websites visited, or the calls or texts made or received.

Browser History

Who do we share with?

Companies that display ads to you through apps.

Ad Networks

US Inventors History Quiz

INSTALL

US Inventors History Quiz

Privacy Notice

What do we collect?

A list of websites visited, or the calls or texts made or received.

Browser History

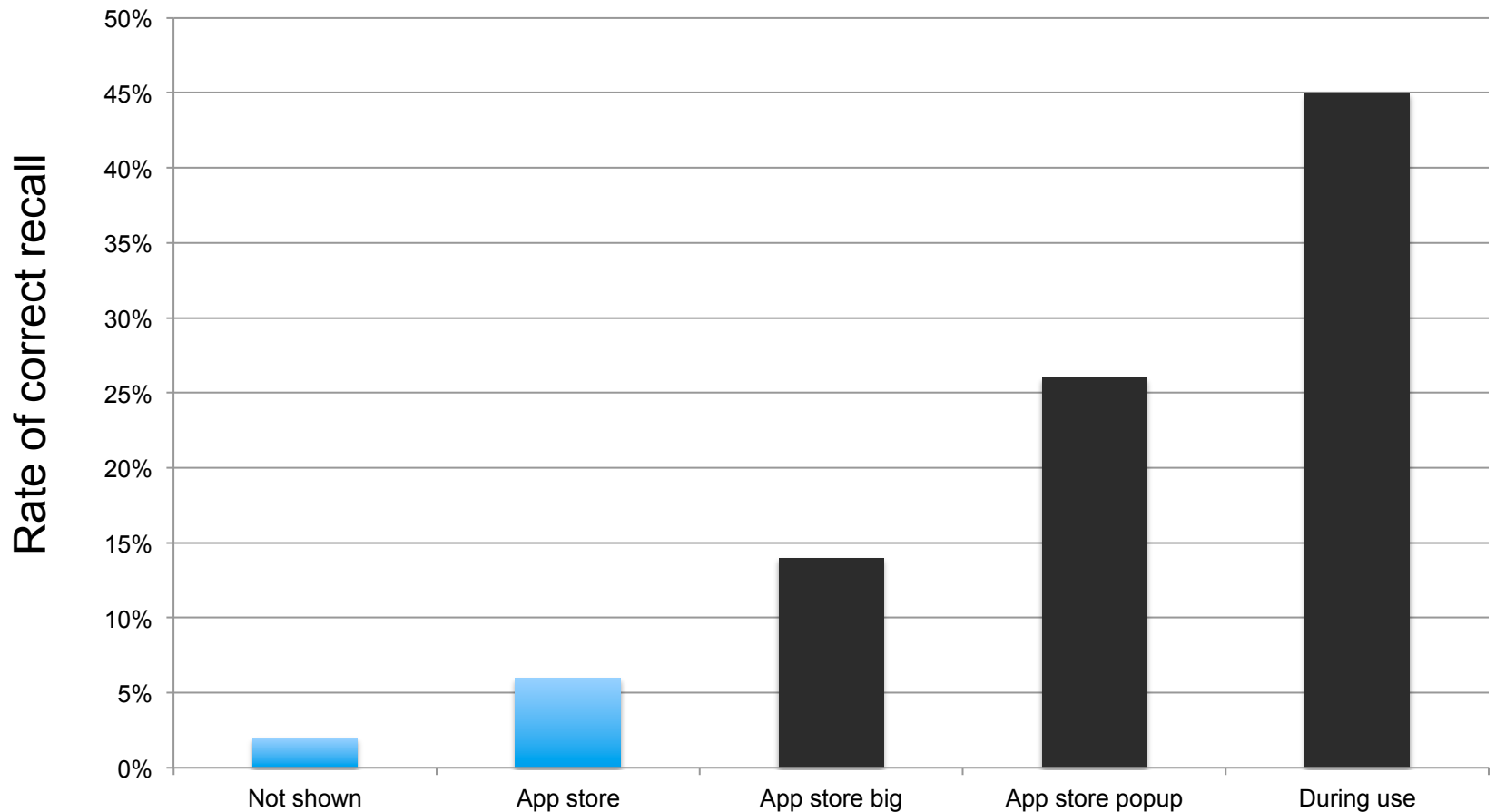
Who do we share with?

Companies that display ads to you through apps.

Ad Networks

ACCEPT

# New notices better, but not as good as during use



# Design recommendations

- Participants remembered notices shown during app use
- Participants did not like the notices shown after app use
- Making the notice more prominent in the app store can improve recall
- Show privacy notices during app use, in context.

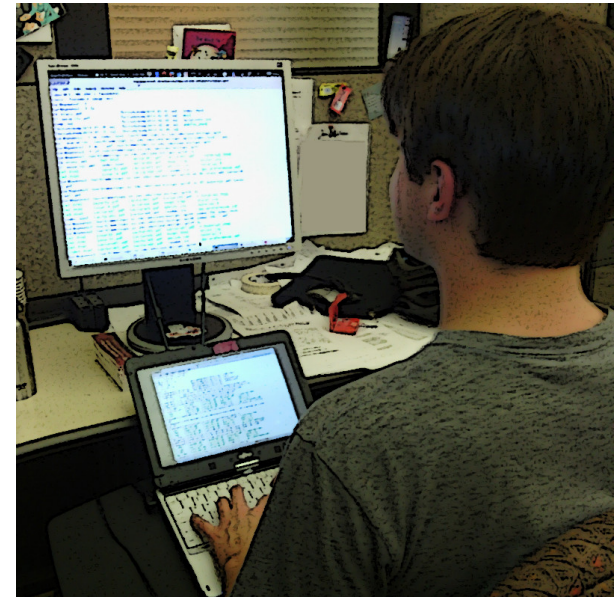


# Different Study



# App Developer decisions

- Privacy and Security features compete with
  - Features requested by customers
  - Data requested by financiers
  - Revenue model



# What is the research question?

- What are app developers doing to protect user privacy and security?
- What influences privacy and security decisions?

# Research Project

- Exploratory Interviews
- Quantitative on-line study

# Participant Recruitment

- 13 developers interviewed
- Recruited through craigslist and Meetups
- \$20 for one-hour interview

# Participant Demographics

- Variety of revenue models
  - Advertising
  - Subscription
  - Pay-per-use
  - Non-Profit
- Seven different states
- Small company size well-represented

# Tools impact privacy and security

- Interviewees do:
  - Use cloud computing
  - Use authentication tools such as Facebook
  - Use analytics such as Google and Flurry
  - Use open source tools such as mysql

# Tools not used

- Interviewees don't use or are unaware of:
  - Use privacy policy generators
  - Use security audits
  - Read third-party privacy policies
  - Delete data



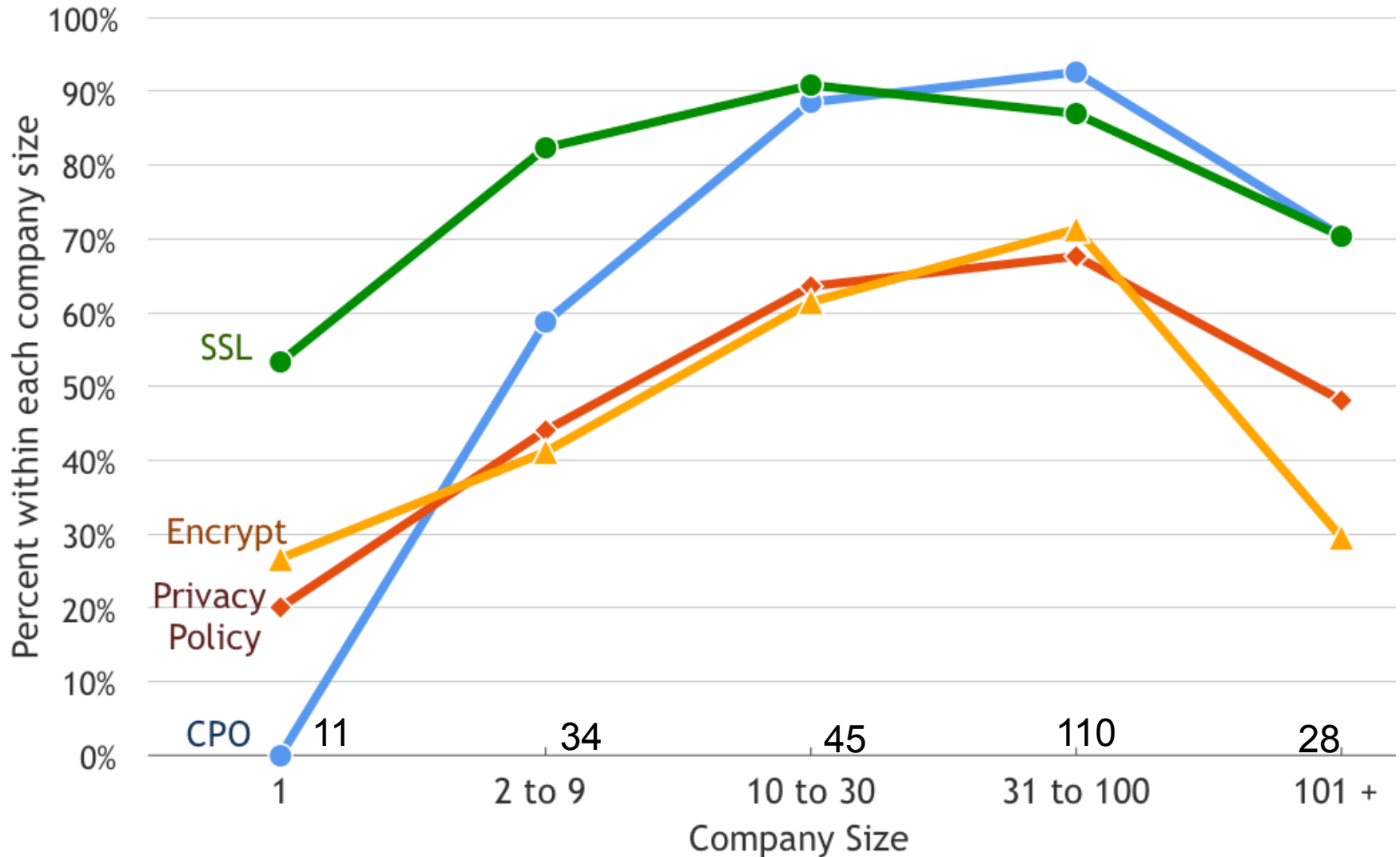
# On-line surveys of app developers

- 228 app developers
- Paid \$5 (avg: 15 minutes)
- Recruited through craigslist, reddit, Facebook, backpage.com
- Developer demographics
  - Majority were ‘Programmer or Software Engineer’ or ‘Product or Project Manager’
  - Avg age: 30 (18-50 years)

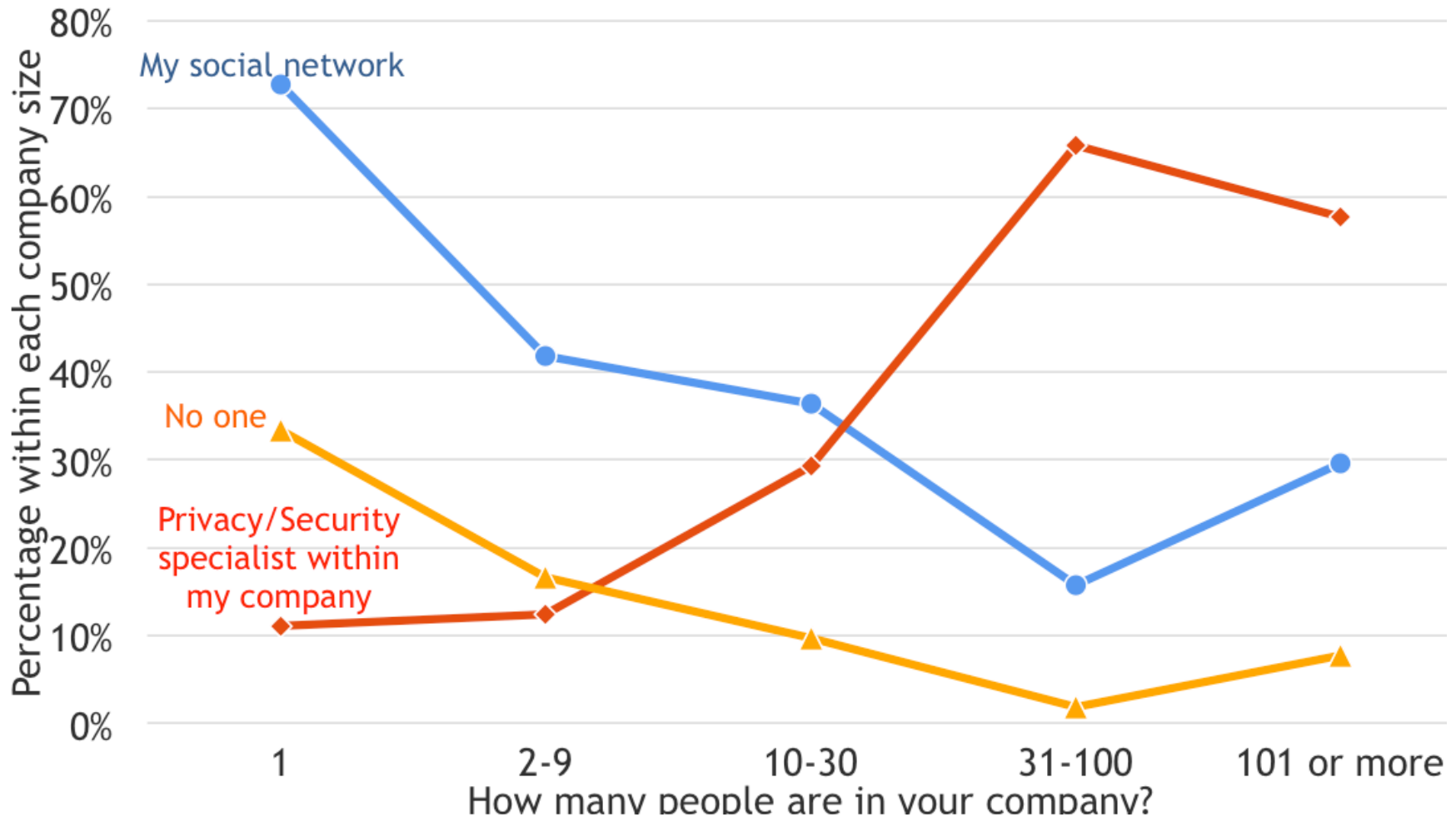
# They collect a lot of data

Behavior	Collect or Store
Parameters specific to my app	84%
Which apps are installed	74%
Location	72%
Sensor information (not location-related)	63%
Contacts	54%
Password	36%

# Small companies less likely to show privacy and security behaviors



# Small companies more likely to turn to social network or no one for advice



# Findings

- Small companies lack privacy and security behaviors
  - Free or quick tools needed
  - Usable tools needed
- Small company developers rely on social ties for advice
  - Opportunities for intervention in social networks
- Legalese hinders reading and writing of privacy policies
- Third-Party tools heavily used
  - Third-party tools should be explicit about data handling