

Privacy, Law, and Smartphones

Rebecca Balebako

Advisor: Dr. Lorrie Cranor

**Engineering &
Public Policy**



Agenda

- Quiz
- Reading discussion
- Permission notices on major platforms
- Policy on smartphone privacy
- (Recent research) Impact of timing on privacy notices

Smartphones allow data sharing



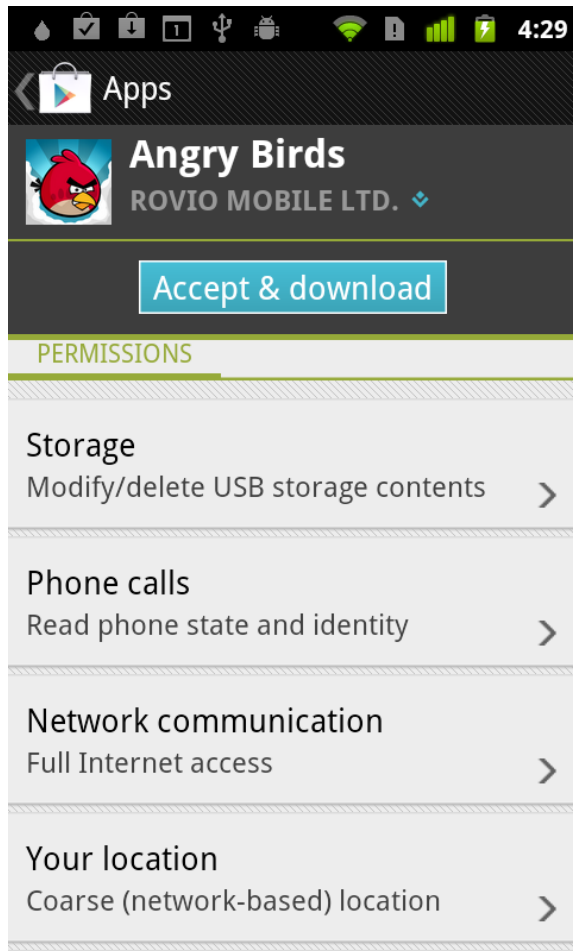
Privacy and security concerns

- 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

Discussion: Do apps on your phone

- Have privacy policy?
- Give you control/access over data collected?
- Have 'Special Notices'?

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.

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

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

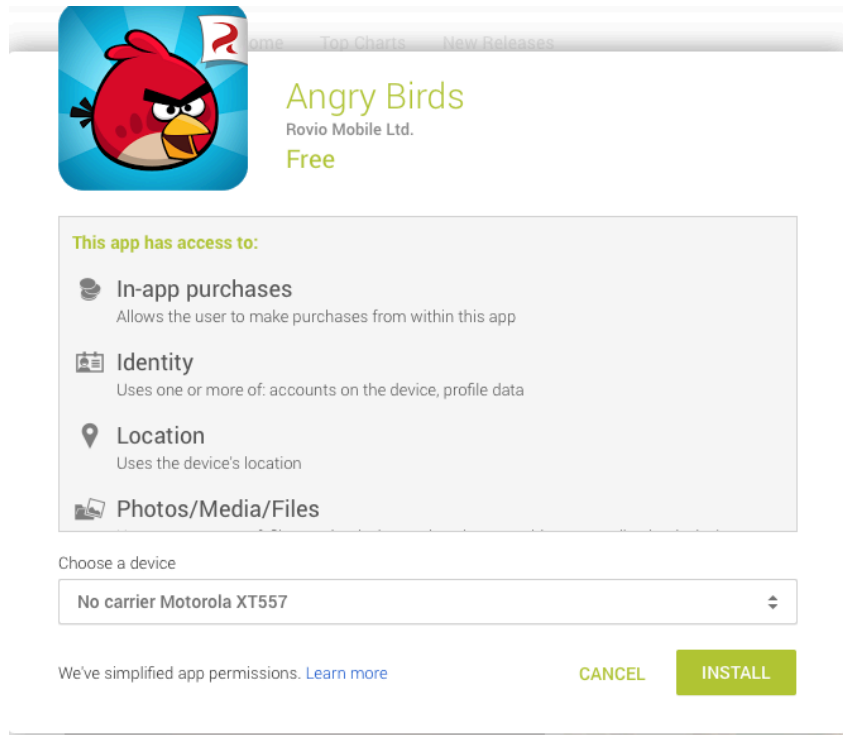
Number of times your **location** has been shared with each app for the past 14 days.

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

[Let me change my settings](#)

[keep sharing my location](#)

2014: Android layered the permissions



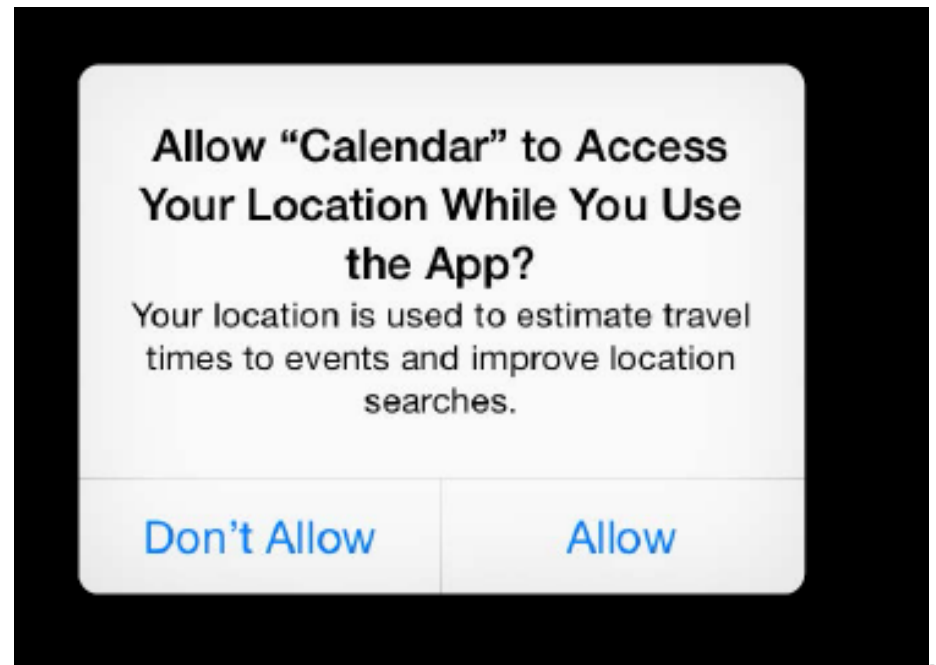
- Location now represents all types of location
- “Network” permissions no longer on top layer

Google Play Store, Oct 19, 2014

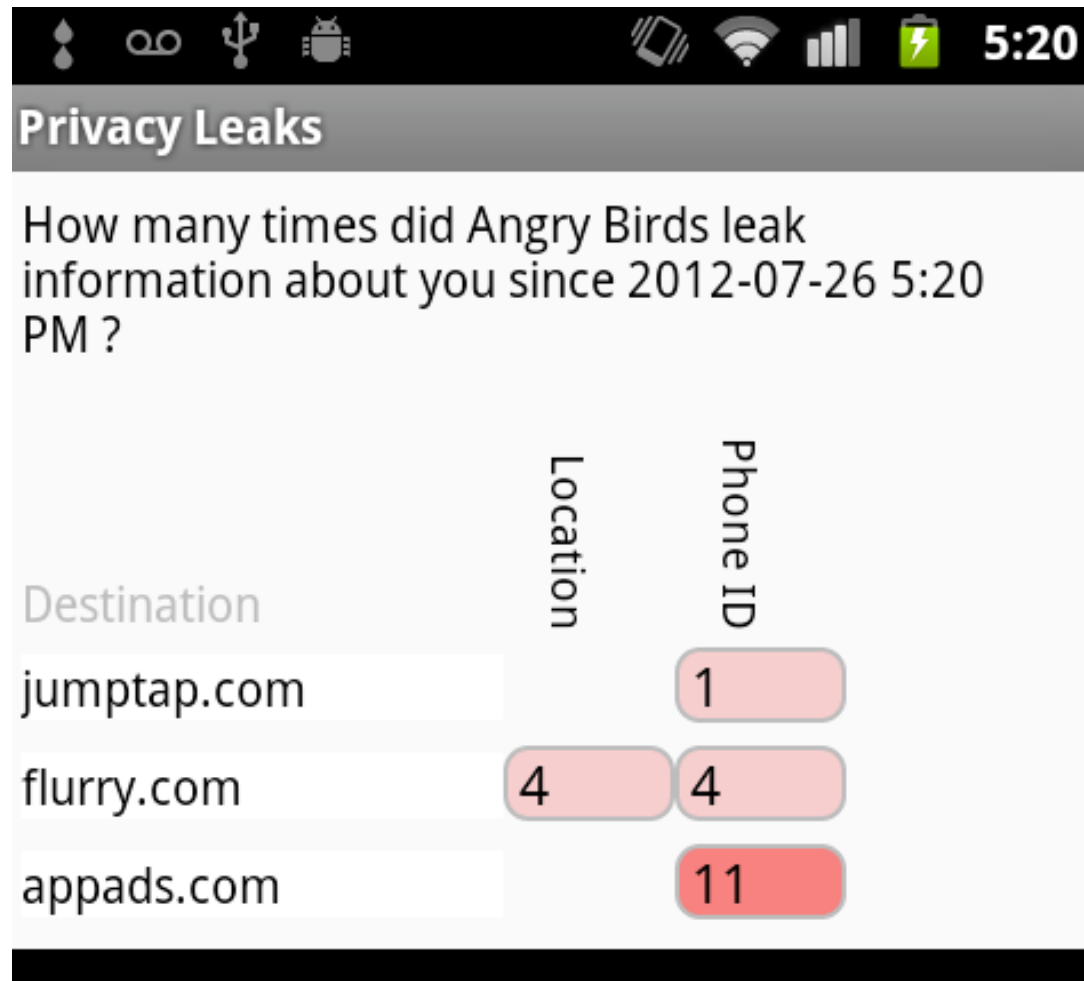
https://support.google.com/googleplay/answer/6014972?p=app_permissions&rd=1

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



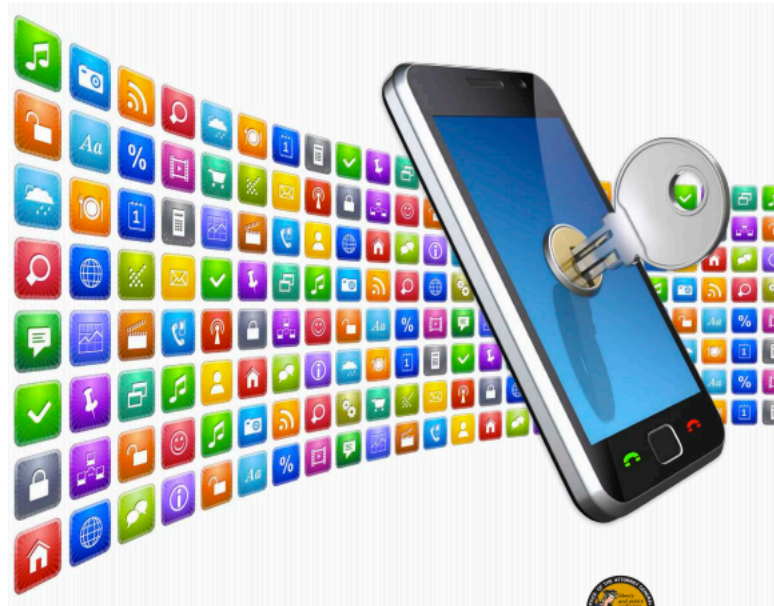
FTC Staff Report | February 2013

California Attorney General

PRIVACY ON THE GO

RECOMMENDATIONS FOR THE MOBILE ECOSYSTEM

January 2013

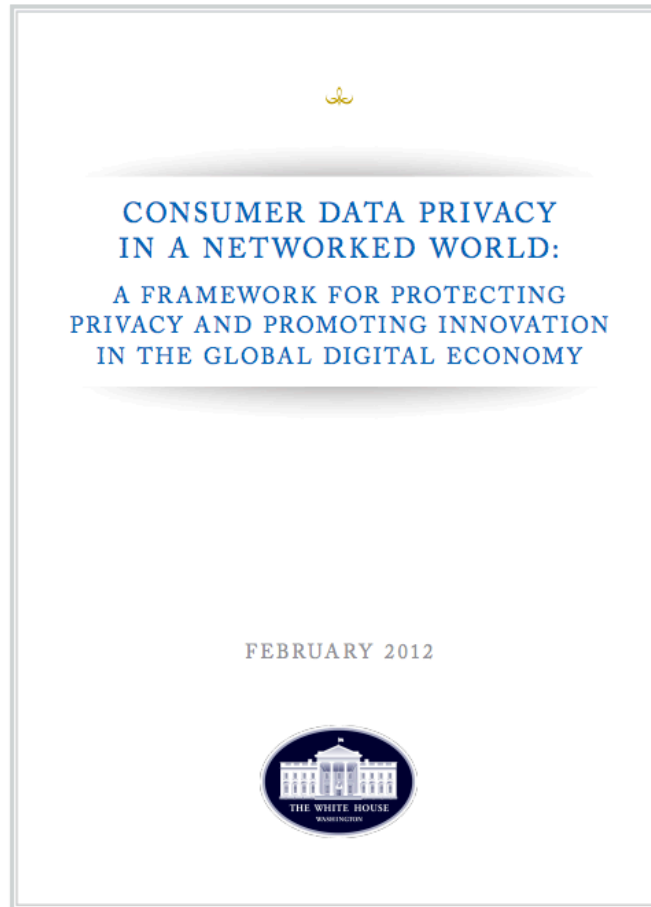


Kamala D. Harris, Attorney General
California Department of Justice


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

Recent Policy: White House



Developing Policy: NTIA MSHP



National Telecommunications & Information Administration

United States Department of Commerce

[TOPICS](#)

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

[NEWSROOM](#)[PUBLICATIONS](#)[BLOG](#)[OFFICES](#)[ABOUT](#)

[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](#)

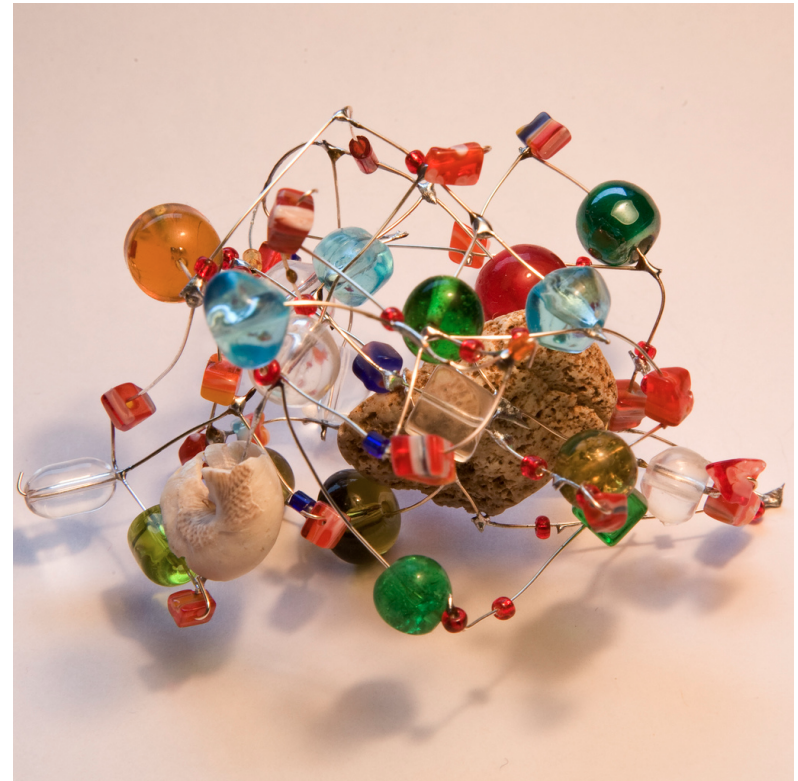
This web page provides details on the NTIA-convened privacy multistakeholder process regarding mobile application transparency. On June 15, 2012, NTIA announced that the goal of the first multistakeholder process is to develop a code of conduct to provide transparency in how companies providing applications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

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



Impact of timing on recall of privacy notices

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

Participants asked to recall the notice after a delay

1. Consent and demographic question
2. 'Download' and play app
3. Delay
 - Web survey: questions about privacy preferences
 - Field experiment: 24 hours
4. Answer recall questions about the app

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

Notice based on NTIA prototype

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.

Conditions varied only when notice was shown

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



Participants remembered notices shown during app use

Condition	Web Survey	Field Experiment
Not shown	3%	9%
App store	17%	14%
Before use	37%*	33%*
During use	43%*	20%*
After use	28%*	37%*

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.



Participants remembered notices shown during app use

- Participants remember notices shown during app use
- Notice shown in app use had better recall than shown in app store
- Notice shown in app store was not significantly different than no notice

balebako@cmu.edu

Thanks!

Engineering &
Public Policy

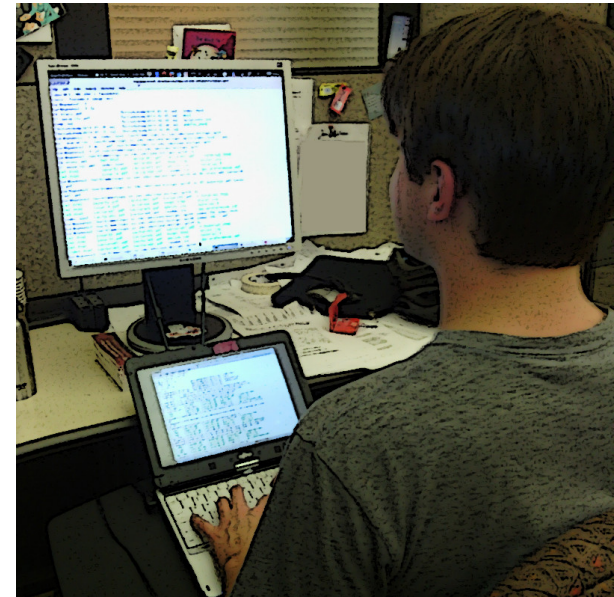


Different Study



App Developer decisions

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



Research Project

- Exploratory Interviews
- Quantitative on-line study

Findings

- Small companies lack privacy and security behaviors
- Small company developers rely on social ties for advice
- Legalese hinders reading and writing of privacy policies
- Third-Party tools heavily used

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

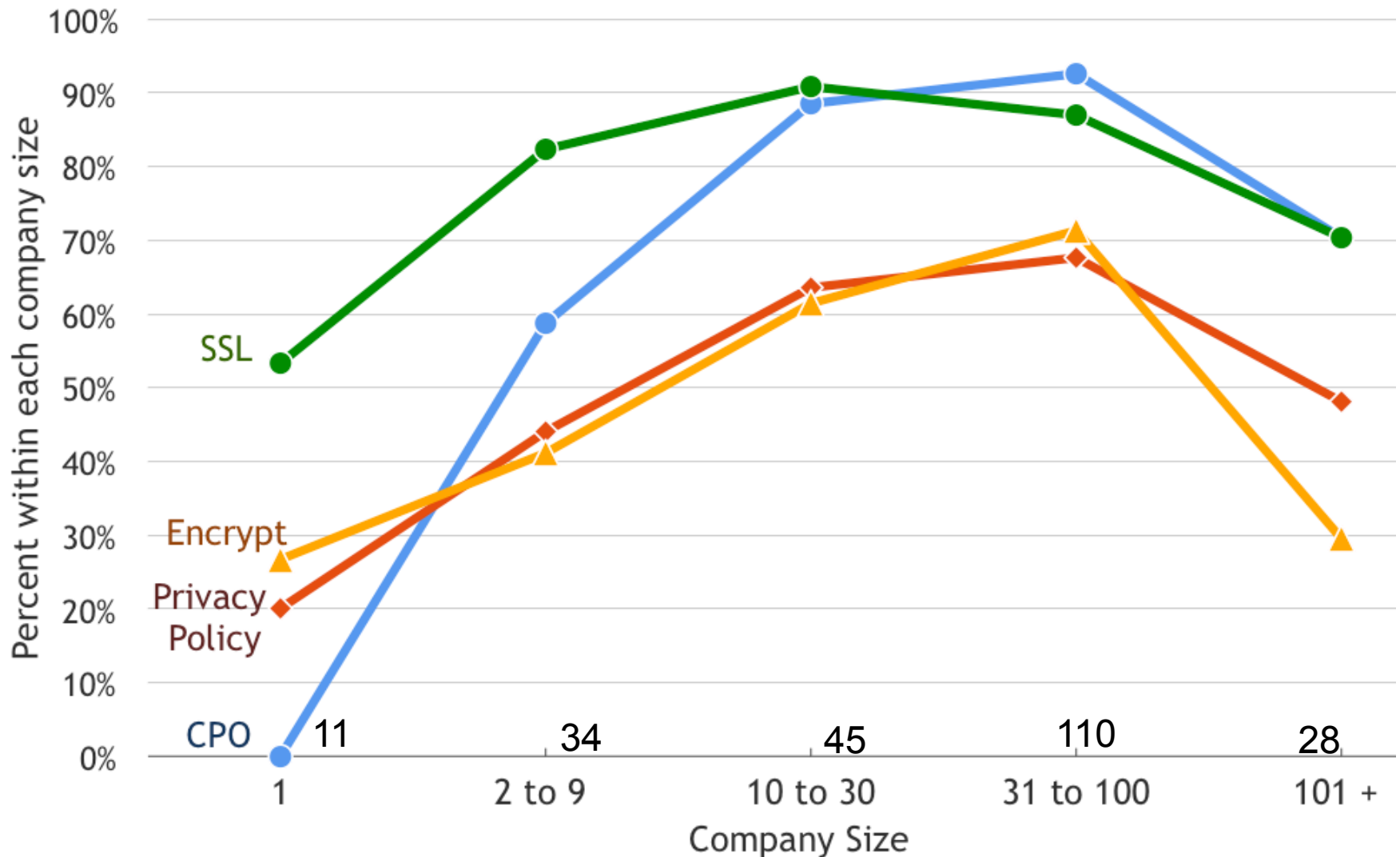
On-line surveys of app developers

- 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)

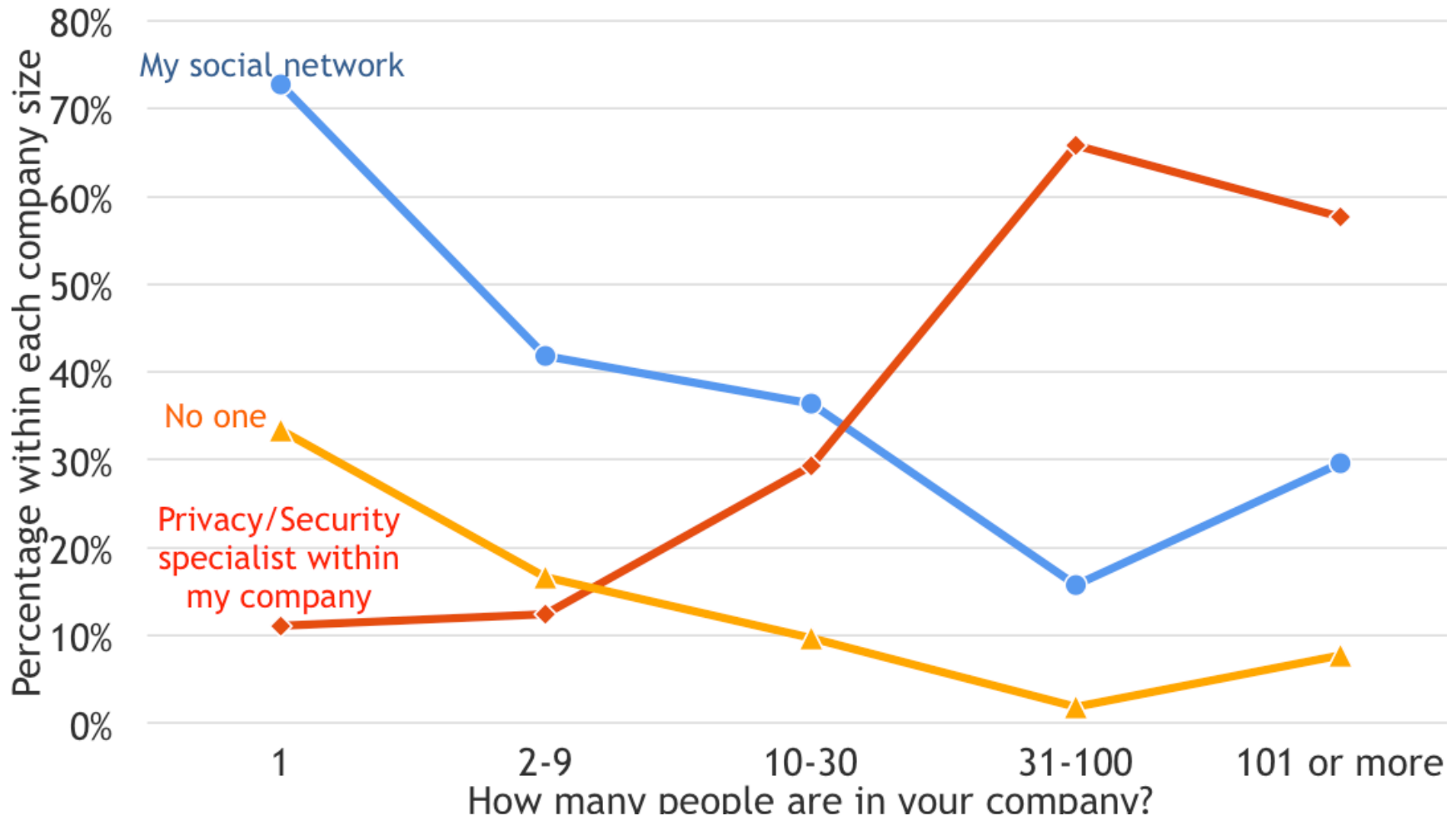
They collect a lot of data

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