Privacy, Law, and Smartphones

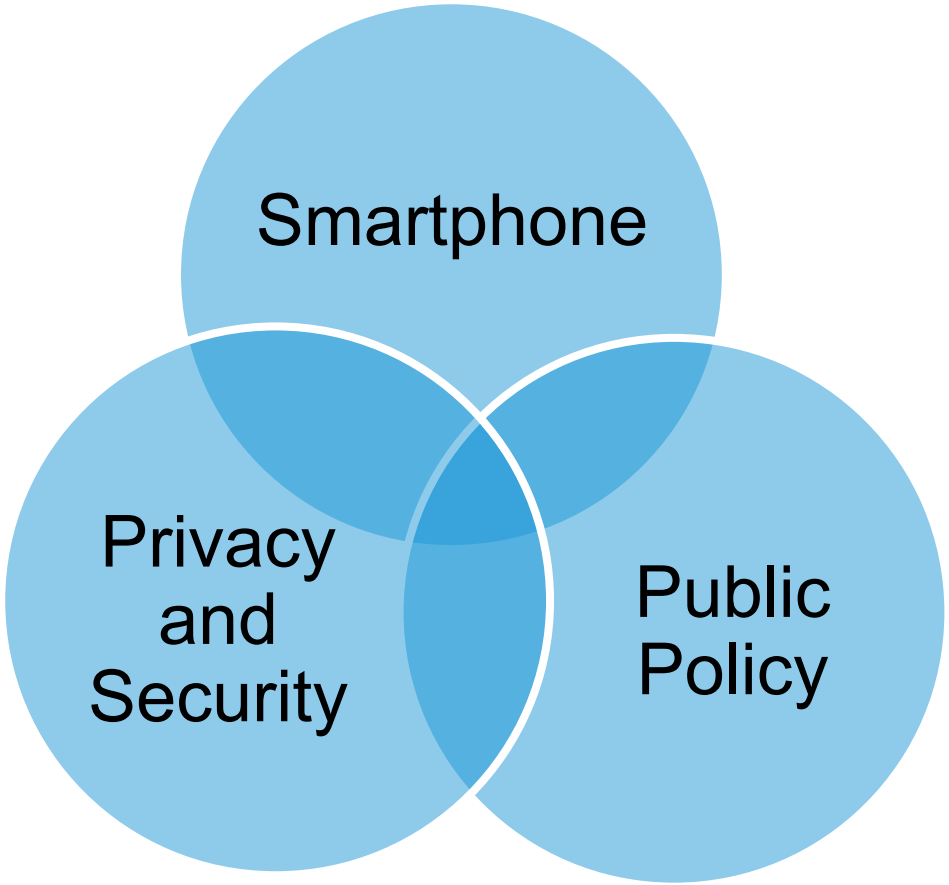
Rebecca Balebako, PhD Candidate

Advisor: Dr. Lorrie Cranor

Carnegie Mellon University
CyLab

Engineering & Public Policy

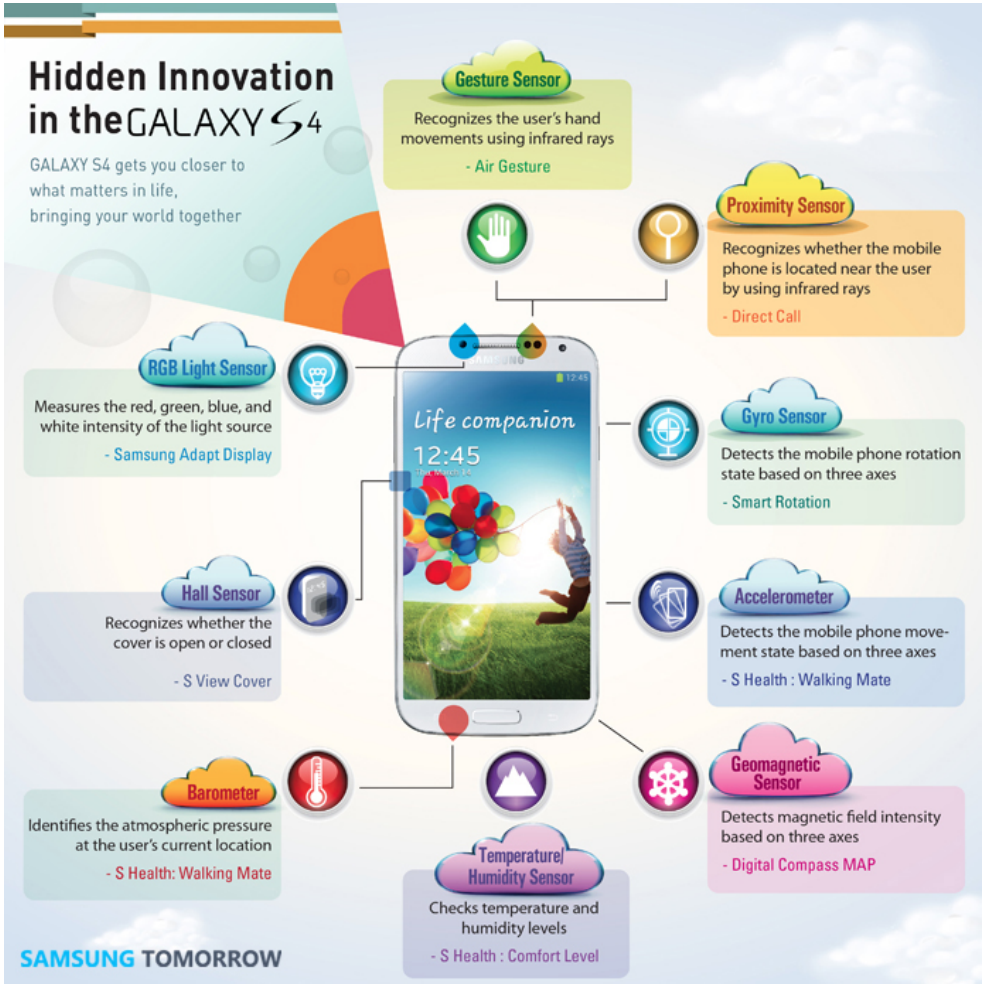
Privacy and Security Concerns



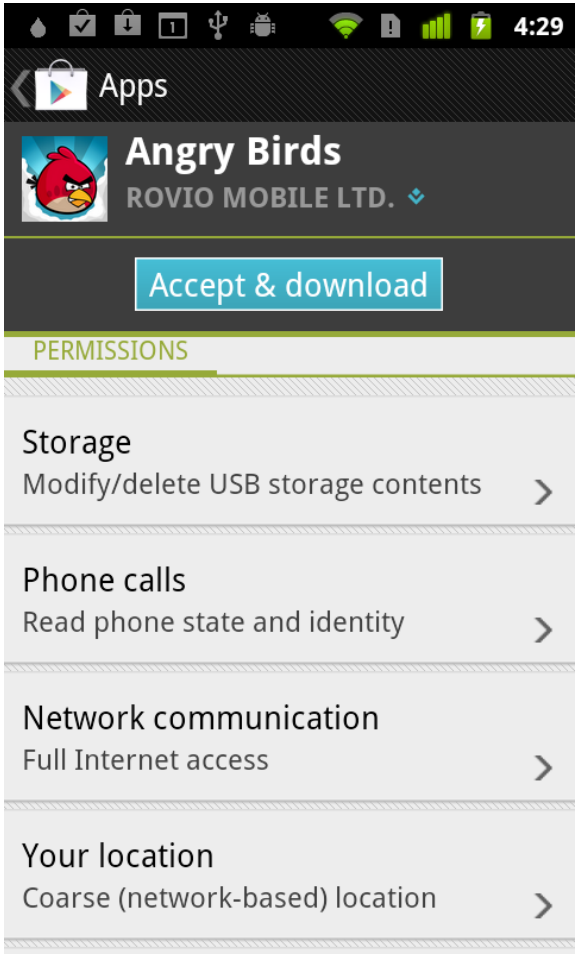
Smartphones

- Increasingly popular
- Smartphones are different that personal computers:
  - Sensors
  - Always on
  - Immature
  - Smaller screens

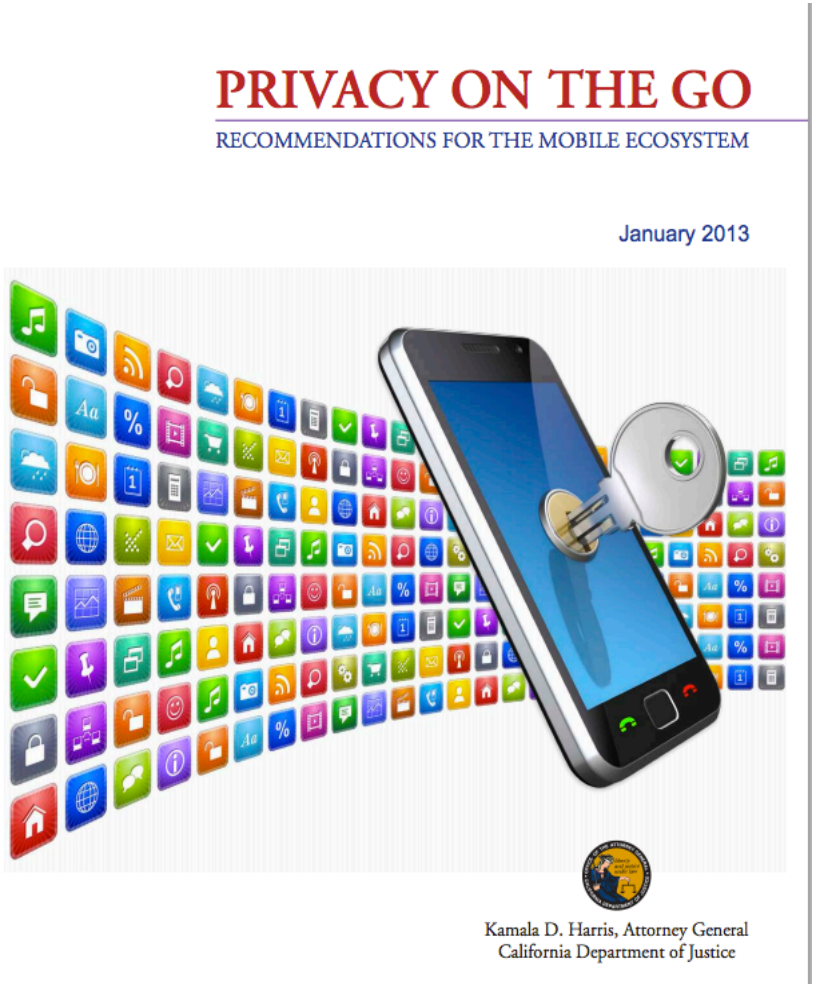
Information on smartphones



Evaluating smartphone interfaces



California Attorney General



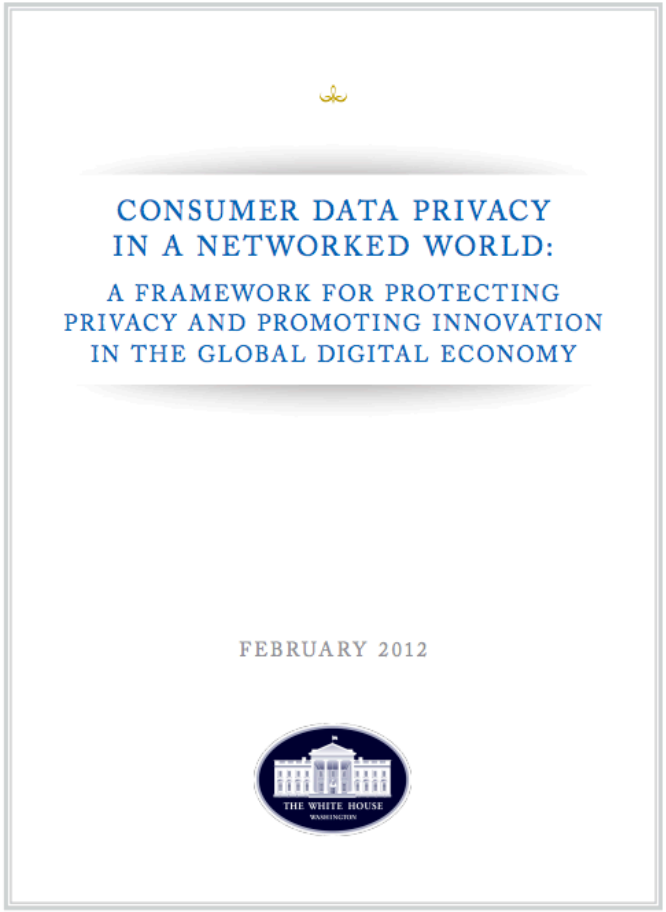
App Developers Should…

- 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

Do apps on your phone:

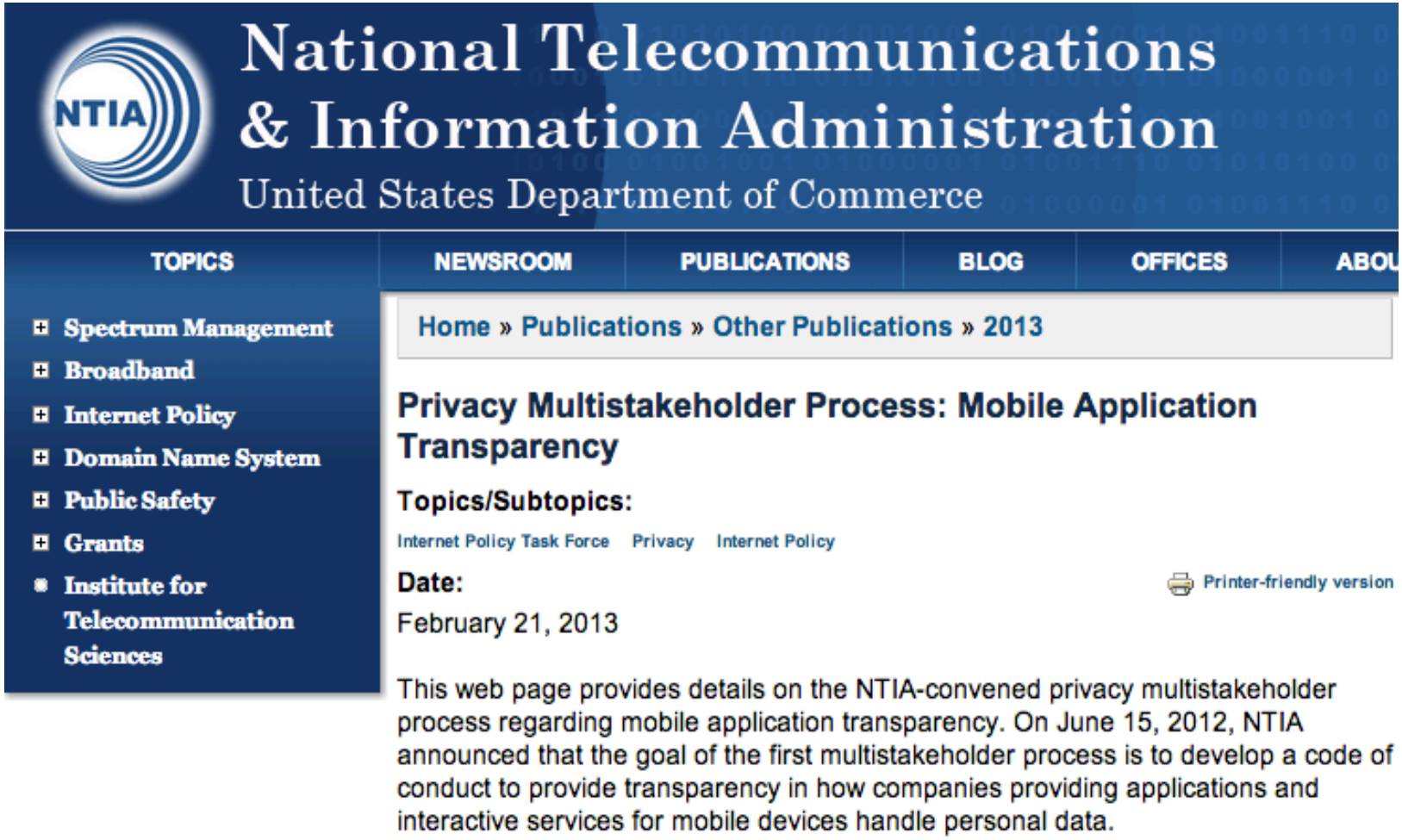
- Have privacy policy
- Give you control/access over data collected
- Have ‘Special Notices’

Recent Policy: White House



Recent Policy: FTC Staff Report

Developing Policy: NTIA MHP



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

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.)

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.)

Survey

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.

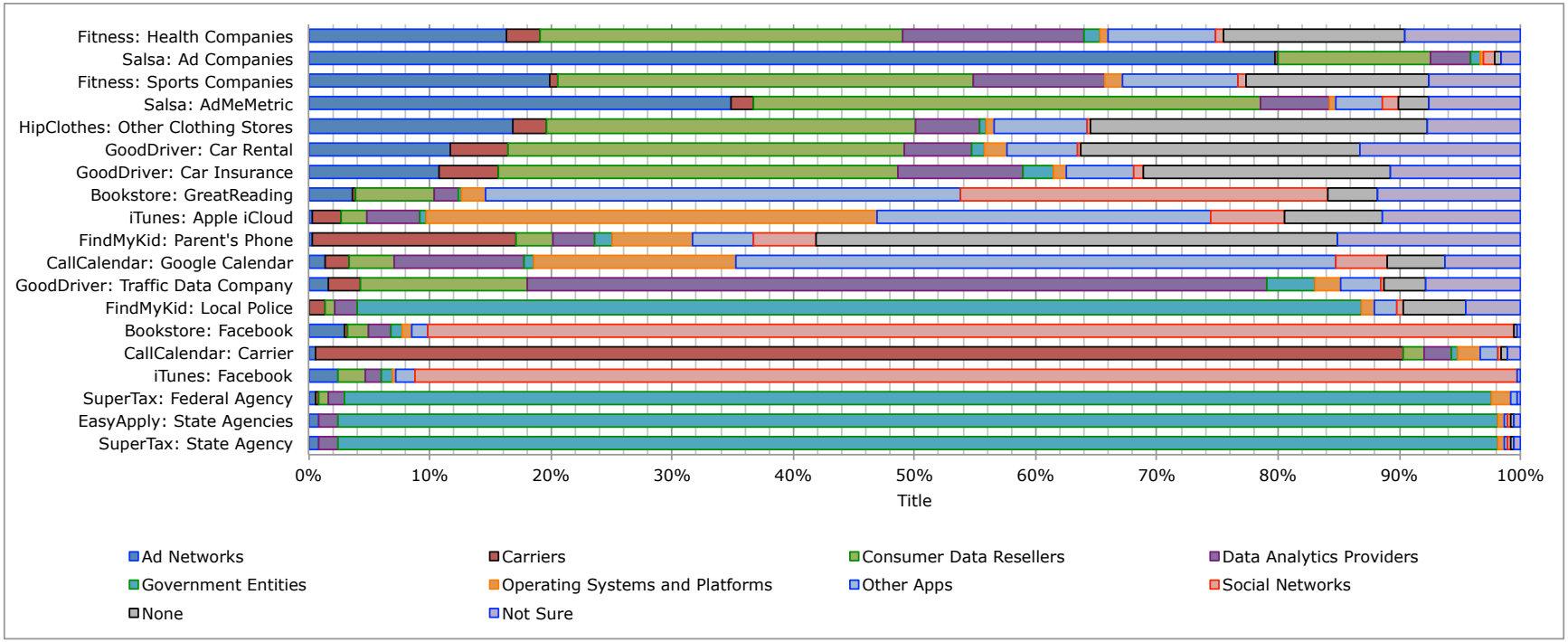
It will then submit your return to state and federal agencies.

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	○	○	○	○	○	○	○	○	○
Salary	○	○	○	○	○	○	○	○	○
Interest Income	○	○	○	○	○	○	○	○	○

Common understanding



Why so bad?

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

Is Your Inseam a Biometric? Evaluating the Understandability of Mobile Privacy Notice

Technical reports: CMU-CyLab-13-011

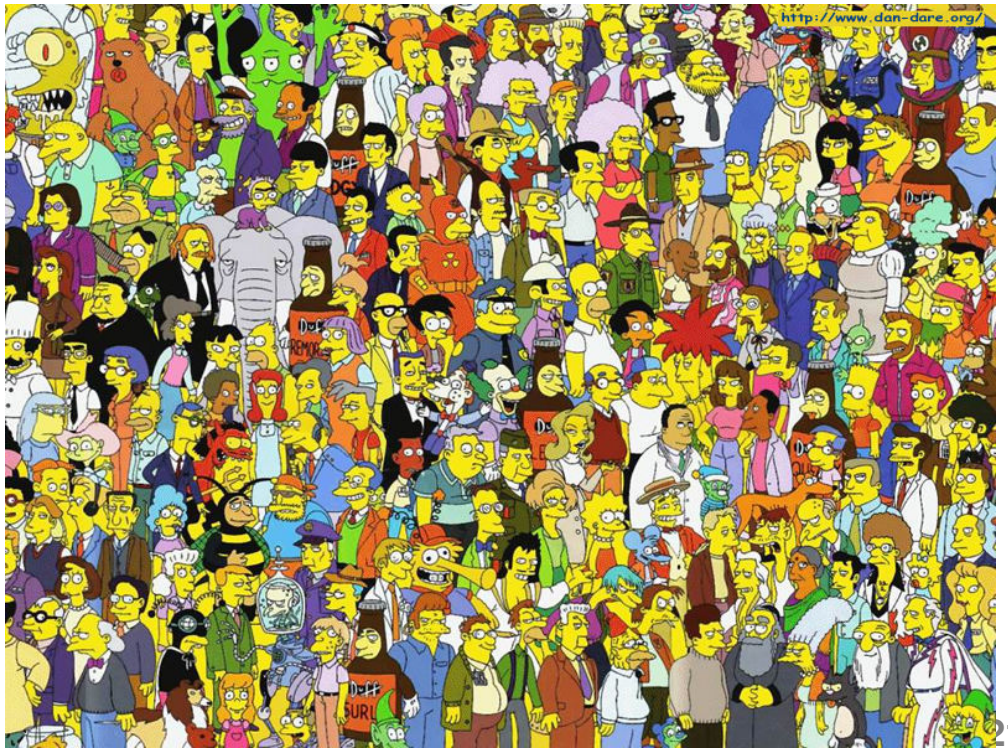
Carnegie Mellon University
CyLab

Engineering & Public Policy

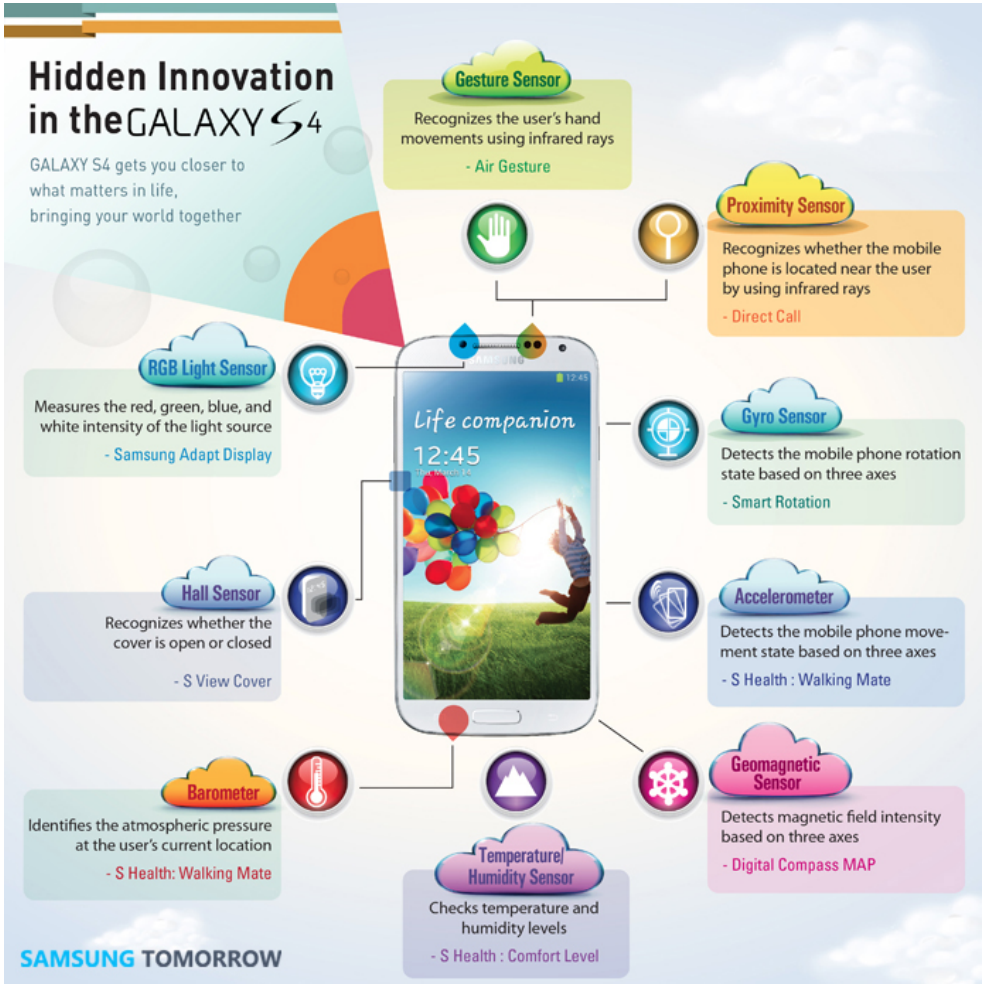
Different Study

App Developers

- 200,000 iOS developers
- 800,000 iOS apps and 800,000 Android apps
- Low barrier to entry



Information on smartphones



App Developer study

- Exploratory Interviews (13)
- Quantitative on-line study (228)

Interview app developers

- How do they decide what privacy and security measures to take?
  - Search engines
  - Some training
  - Talk to friends
  - May have access to legal counsel
  - May need legal counsel

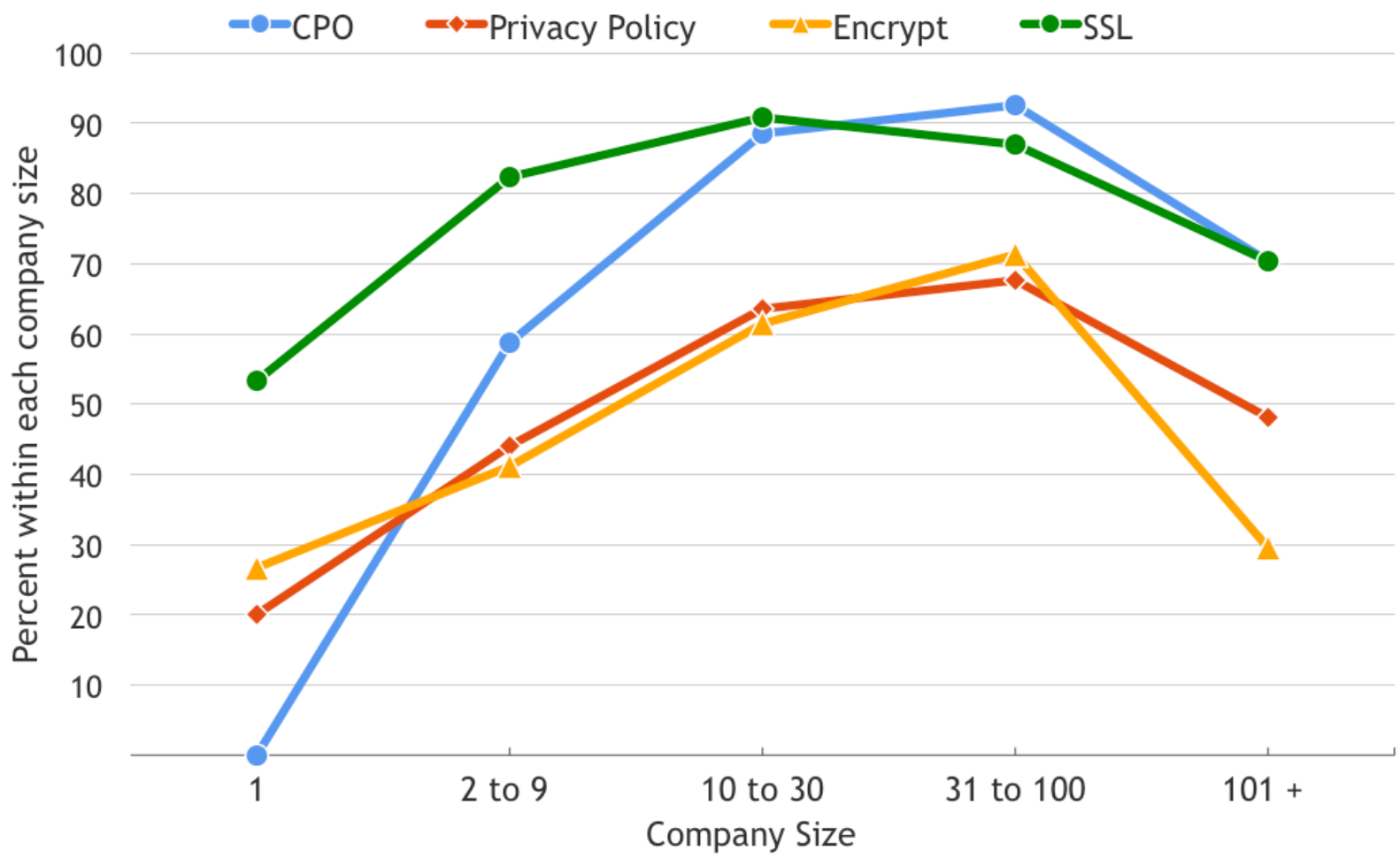
App developer tools

- Do
  - Cloud computing
  - Authentication (Facebook)
  - Analytics such as Google and Flurry
  - Open source tools such as mysql
- Don’t
  - Privacy Policy generators
  - Security audits
  - Read third-party privacy policies
  - Delete data

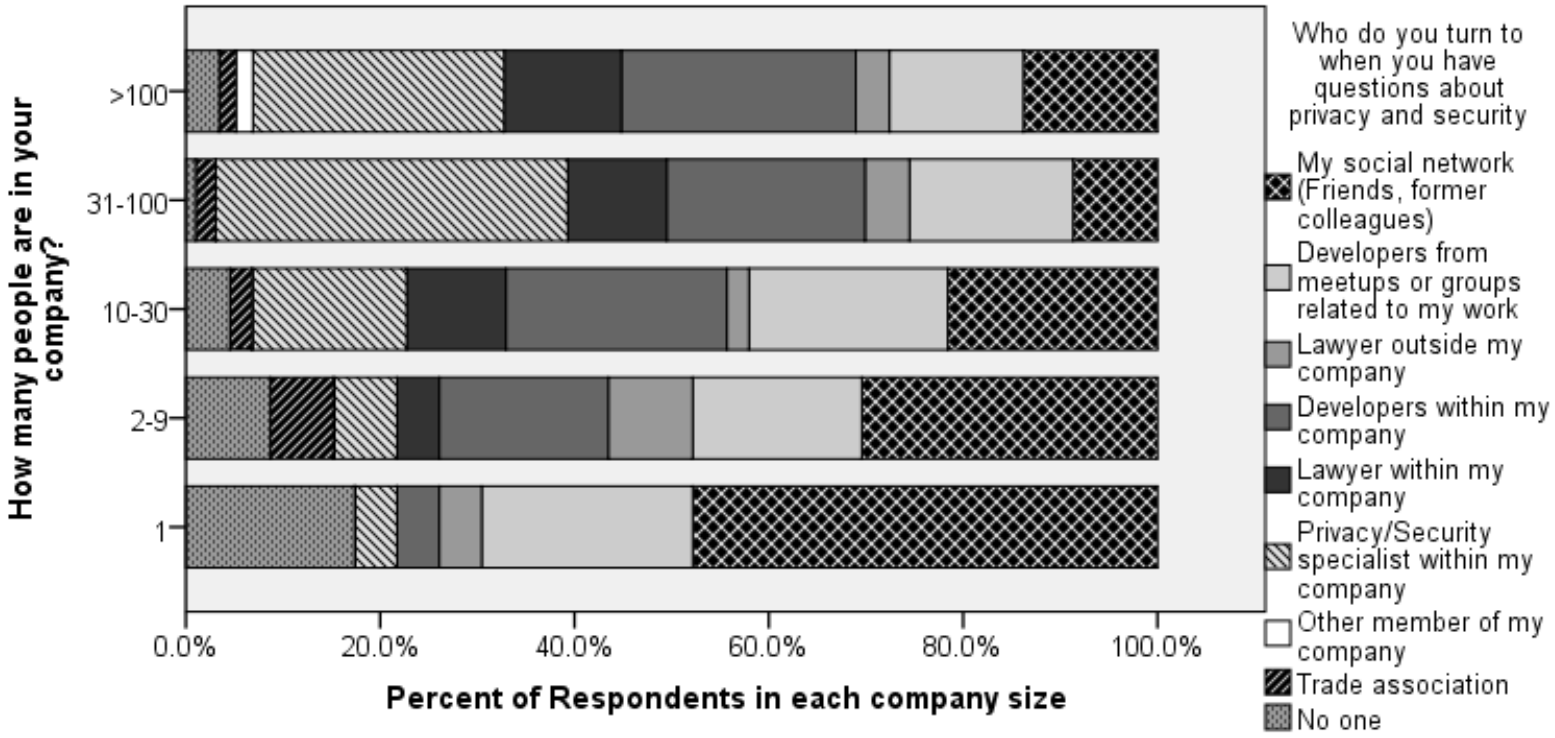
Quantitative Survey

- Behaviors:
  - Privacy Policy
  - CPO or equivalent
  - Encrypt stored data
  - Use SSL
  - Data minimization

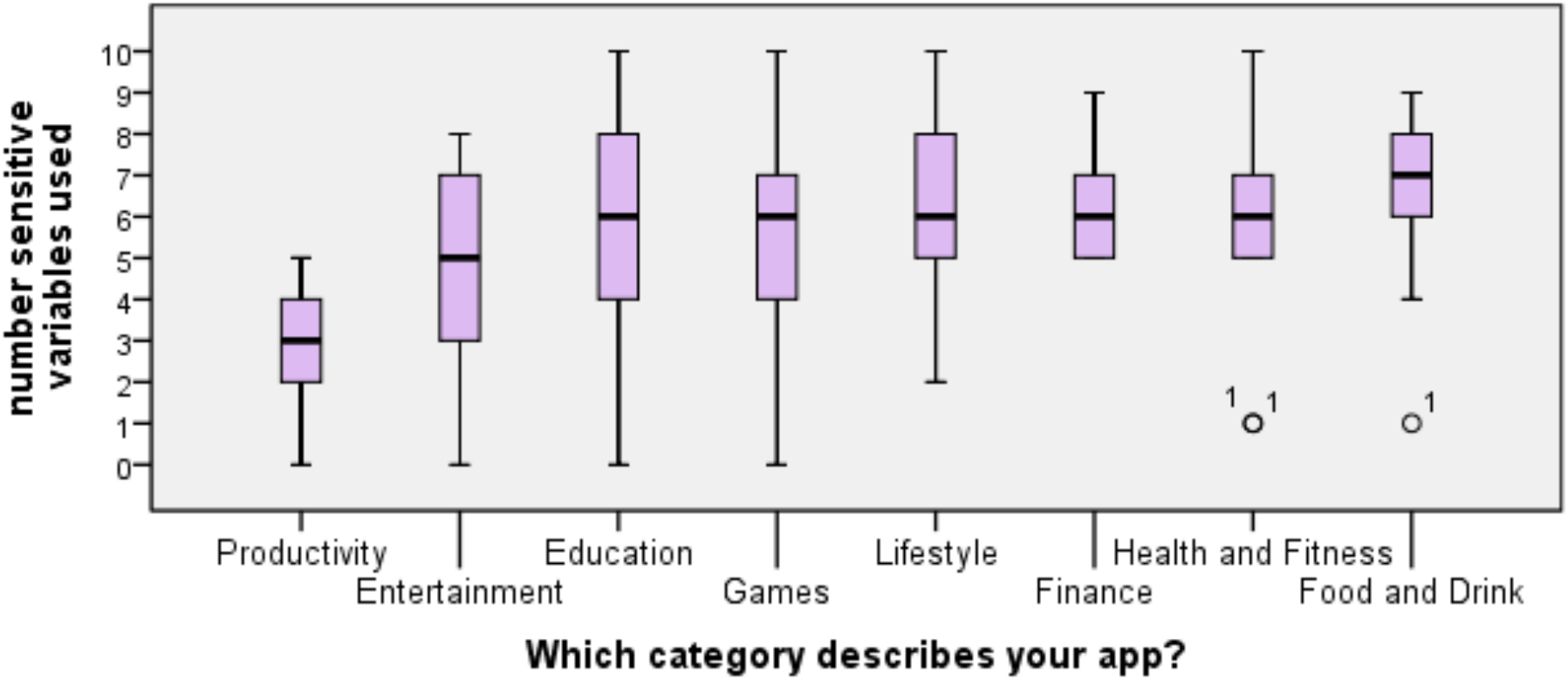
Company size



Company size



Data Type	Collect or Store
Parameters specific to my app	83.9%
Which apps are installed	73.9%
Location	71.6%
Advertising ID	70.6%
Sensor (not location)	63.0%
Phone Id	54.5%
Contacts	54.0%
Phone Number	44.1%
Password	35.5%
Credit Card Information	30.3%


number sensitive variables used
10
9
8
7
6
5
4
3
2
1
0
1
1
1
Productivity
Entertainment
Education
Games
Lifestyle
Finance
Health and Fitness
Food and Drink
Which category describes your app?

SECURITY SAYS YOUR EMPLOYEE LOCATOR DEVICE ISN'T TURNED ON.
MY WHAT?
I THINK YOU CALL IT A SMART-PHONE.
I MIGHT HAVE SOME QUESTIONS.
PUT THEM IN A TEXT TO YOURSELF. I'LL READ THEM LATER.
DilbertCartoonist@gmail.com
Dilbert.com
5-27-11 © 2011 Scott Adams, Inc. /Dist. by Universal Uclick

balebako@cmu.edu

Thanks!

Carnegie Mellon University
CyLab

Engineering & Public Policy