

# SoK: Privacy on Mobile Devices It's Complicated

**Chad Spensky**, Jeffrey Stewart, Arkady Yerukhimovich, Richard Shay,  
Ari Trachtenberg, Rick Housley, and Robert K. Cunningham

**Privacy Enhancing Technologies Symposium 2016**





# Is Privacy Possible on Mobile Devices?

**“Privacy as we knew it in the past is no longer feasible...**

**How we conventionally think of privacy is dead”**

- Margo Seltzer, World Economic Forum, 2015



**How to stop Facebook from spying on you while you're on your phone**

**East Idaho News - Jul 1, 2016**

The most recent **privacy** buzz is Facebook's ability to **listen** to people's conversations in order to bring them more relevant ads. One expert has ...



**U.S. senator probes Pokemon GO maker over data **privacy** concerns**

**Yahoo News - Jul 12, 2016**

The augmented reality **mobile** game "Pokemon Go" by Nintendo is shown on a smartphone screen in this photo illustration taken in Palm ...

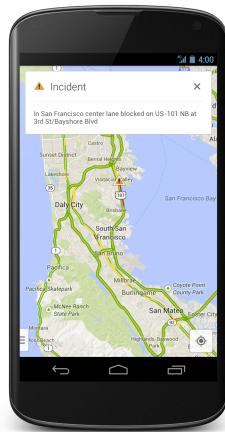
**Pokemon Go: Gotta catch all your personal data**

**In-Depth - CNET - Jul 11, 2016**



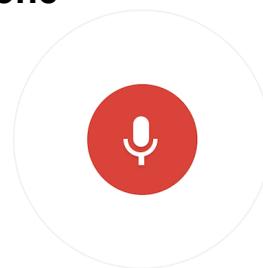
# Mobile Devices Features vs. Privacy

## Location Tracking

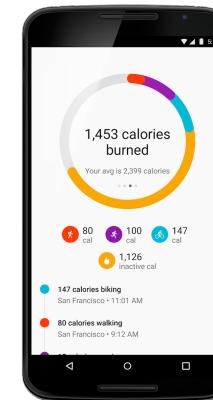


## Microphone

Listening...



## Environmental Sensors



## Personal and Financial Data

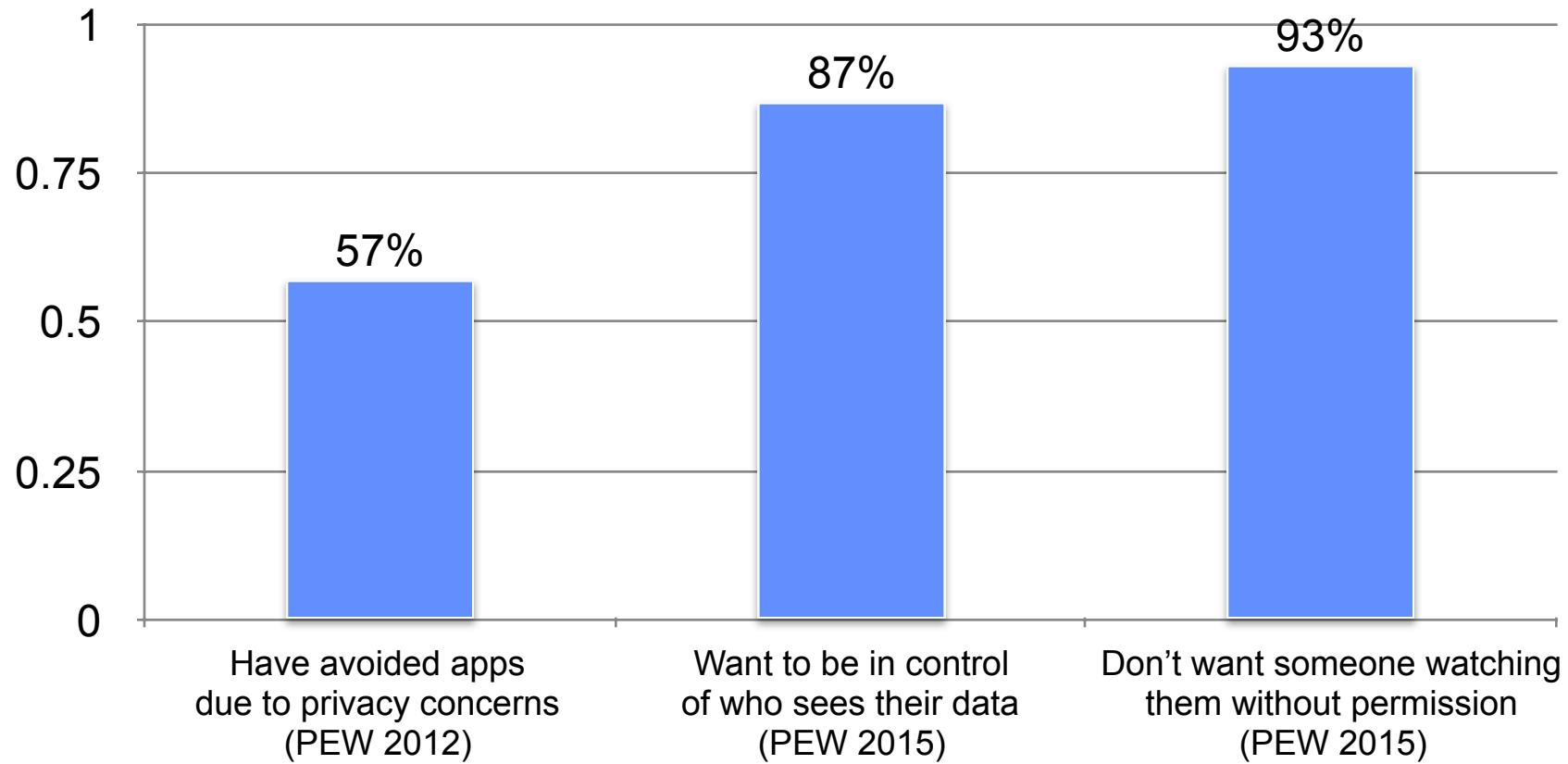


## Cameras





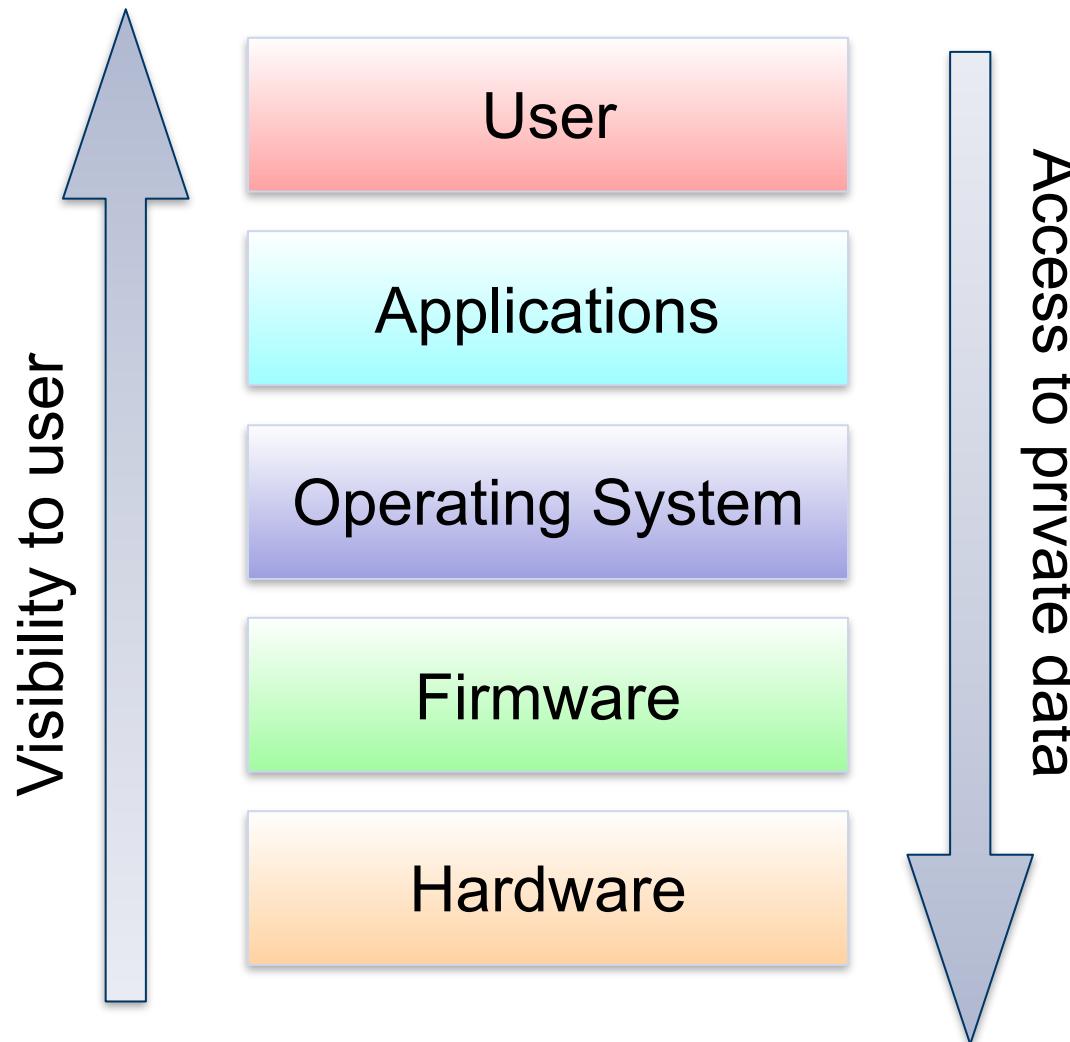
# Users Still Want Privacy



**Top companies are even marketing their privacy-enhancing technologies**



# Systematizing Mobile Device Privacy

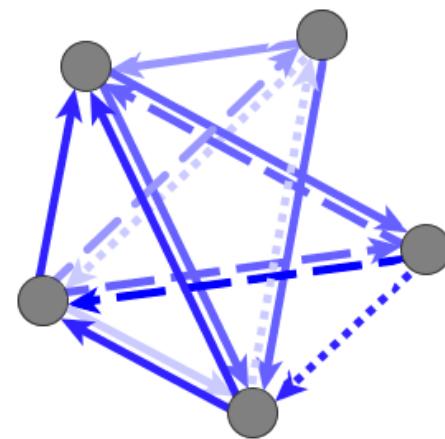




# Our Methodology



Evaluate available  
protections



Consider components  
and their interactions



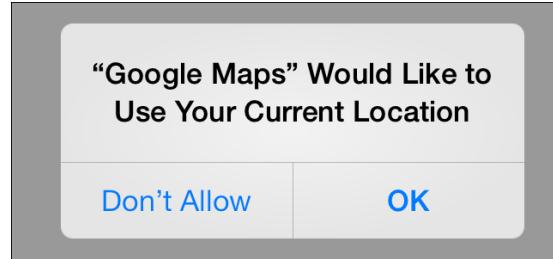
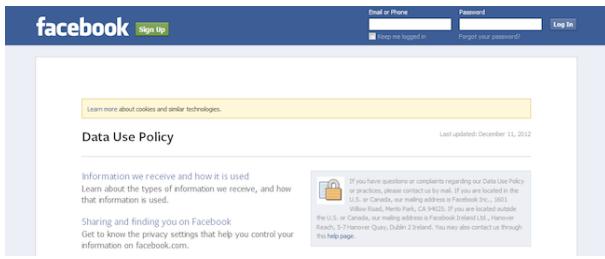
Examine parties  
and their motives

***Pull all of this together into a “privacy world view”***



# Mobile Privacy-enhancing Technologies

## User



## Privacy Policies

### Analyzed

- Top 50 free/paid (Android)
- Top 100 free/paid (iOS)

### Result

Only 32% are accessible to someone without a college education

## User Prompts

### Over-permissioning

- Over 1/3 of apps request permissions they don't need [90,150]
- Users don't understand what data these apps can access [29, 91, 92]

User

App

OS

Firmware

Hardware



# Mobile Privacy-enhancing Technologies

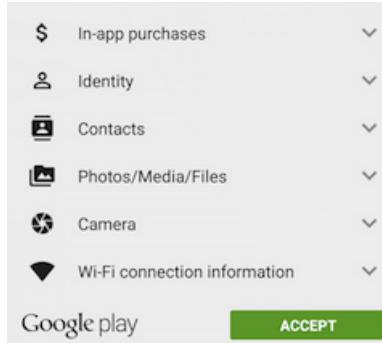
## Software



### Encryption

Analyzed  
Top 50 banking apps

Results  
Apps still incorrectly validate  
SSL certificates  
iOS: 4  
Android: 2



### Permissions Models

#### App with no permissions

- Can access
  - Wallpaper
  - Network Activity
  - Directory Structure
- Low-level kernel crashes on both Android and iOS





# Mobile Privacy-enhancing Technologies

## Software



### Application Sandboxing



### Application Vetting

User

App

OS

Firmware

Hardware

#### Breaking Out

- Root-level malware [31]
- Infect developer tools [110]

#### Side-Channels

- Intercept taps [3-5]
- Location from power [8]

#### Evasion (Android)

- Dynamic code [79]
- Unknown sources [78]

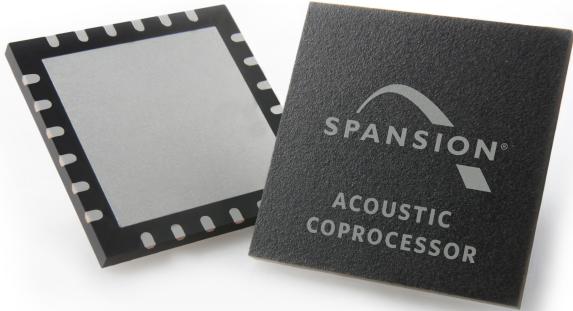
#### Evasion (iOS)

- Private APIs [83]
- Enterprise apps [111]



# Mobile Privacy-enhancing Technologies

## Firmware



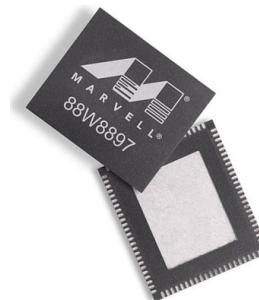
### Specialized Co-Processors

#### Purpose

- Record audio
- Capture user movements

#### Concern

- Could be compromised to permit covert data capture



### Communication Chipsets

#### Analyzed

- NFC chipset on Android
- Require special drivers

#### Results

- Nexus S: **856 crashes**
- Nexus 4: **7 crashes**

User

App

OS

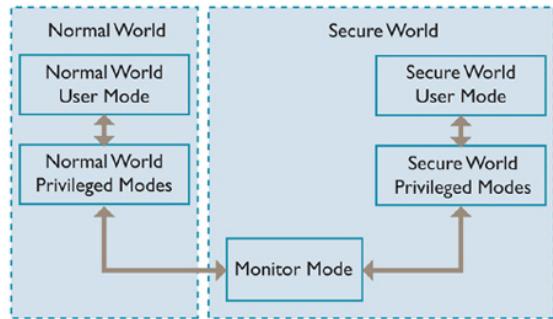
Firmware

Hardware



# Mobile Privacy-enhancing Technologies

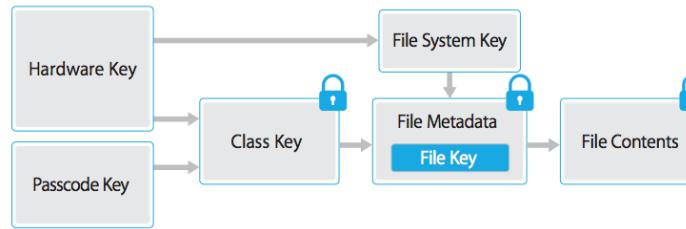
## Hardware



### Trusted Execution Environment

**Purpose**  
Protects user data from software-based attacks

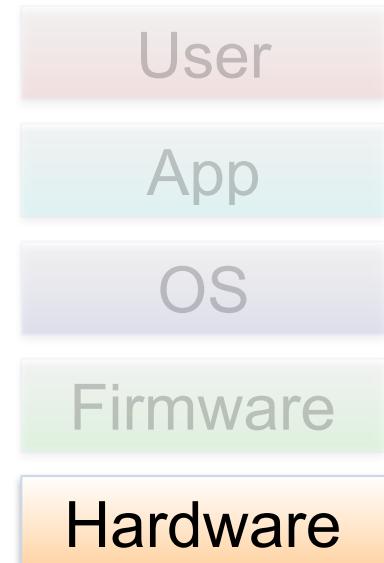
**Concern**  
Has unlimited access to the entire system



### Dedicated Cryptographic Units

**Purpose**  
Protect user data even if the device is stolen or lost

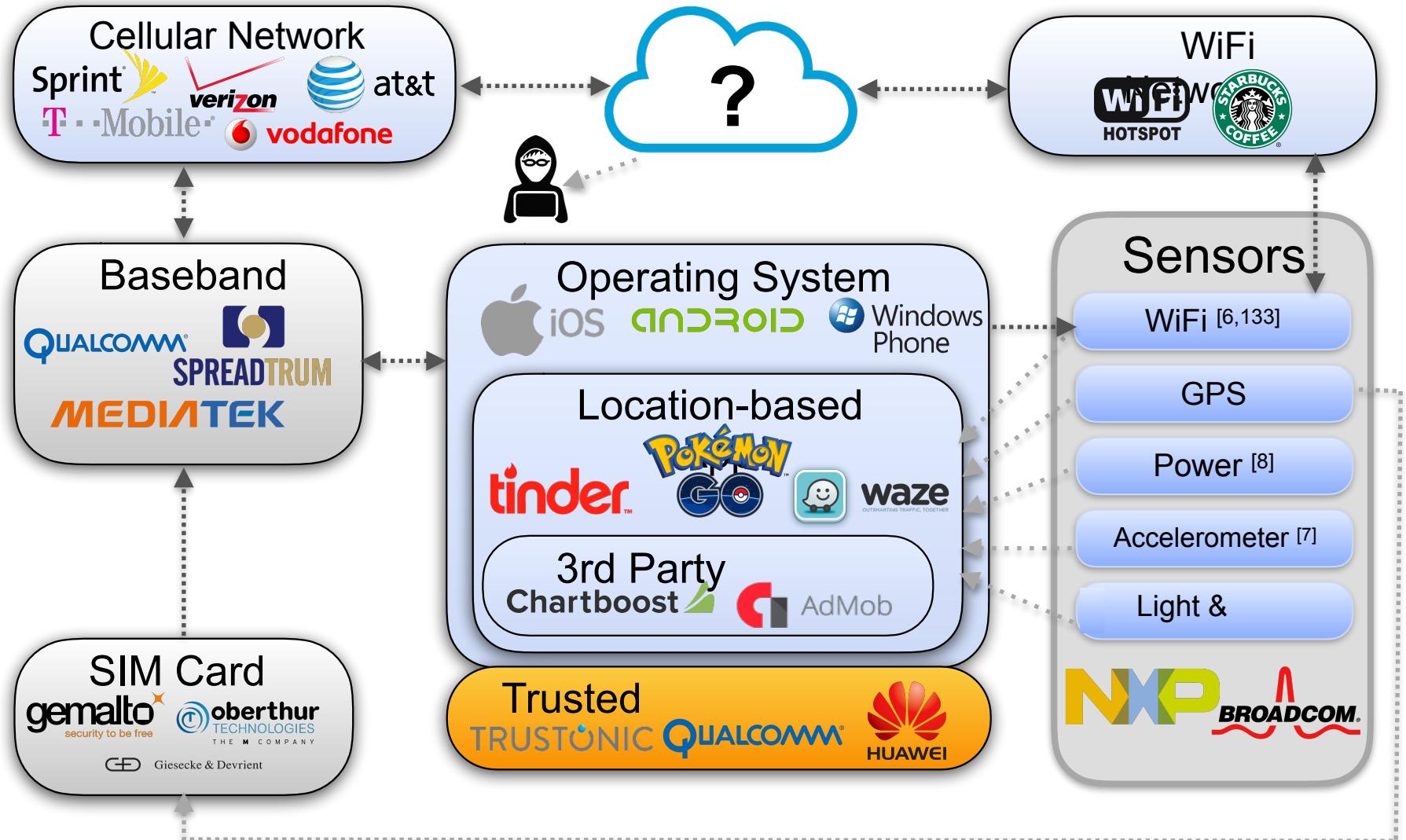
**Concern**  
Low visibility and regulation on implementation





# Privacy World View

## Location-based Application





# Summary

- Modern mobile devices are extremely complex, across all layers
- Ill-defined trust relationships lead to un-intended data leakages
- Effective privacy-enhancing technologies must consider the entire stack
- We are likely going to see even more data leaks without fundamentally new approaches

Complexity is the enemy of both **security** and **privacy**



# Can We Do Better?



- **Reducing Trust Relationships**
  - e.g., Hardware segregation



- **Guiding Users Toward Privacy**
  - e.g., Personalized Privacy Assistant (SOUPS '16)



- **Mechanism Design for Privacy**
  - e.g., Bitcoin [183]



# Questions?

