

# USABLE PRIVACY POLICY AND PERSONALIZED PRIVACY ASSISTANT PROJECTS

## ***IoT Security and Privacy: What Can We Learn from the Mobile App Stores?***

Norman Sadeh

Carnegie Mellon University

[www.normsadeh.org](http://www.normsadeh.org)

[usableprivacy.org](http://usableprivacy.org)   [privacyassistant.org](http://privacyassistant.org)

[explore.usableprivacy.org](http://explore.usableprivacy.org)



Latest Projections: Between 20 and 30 billion IoT devices by 2020...

# No Obvious “Killer App”

- Similar to Smartphones
  - No one knows for sure which devices and scenarios will gain broad adoption
- **Ecosystems** create value by enticing device manufacturers and service providers to use **growing collection of APIs and leverage core technologies/infrastructure and existing user bases**
  - Similar to mobile app stores
- Many IoT scenarios mediated by mobile devices  
(e.g., <http://ieeexplore.ieee.org/document/7841466/>)

# Security and Privacy as Major Potential Adoption Impediment

Ever larger “**attack surface**”

A number of risks:

- **Unauthorized access and misuse of personal data**
  - e.g. health data
- Facilitating **attacks on other systems**
  - e.g. DDoS attacks
- **Personal safety**
  - e.g., cars, pacemakers, door locks



<http://www.welivesecurity.com/2016/10/24/10-things-know-october-21-iot-ddos-attacks/>

# Magnitude of the Problem

TELECOM TV

## IoT Security Spending compared to Device Growth

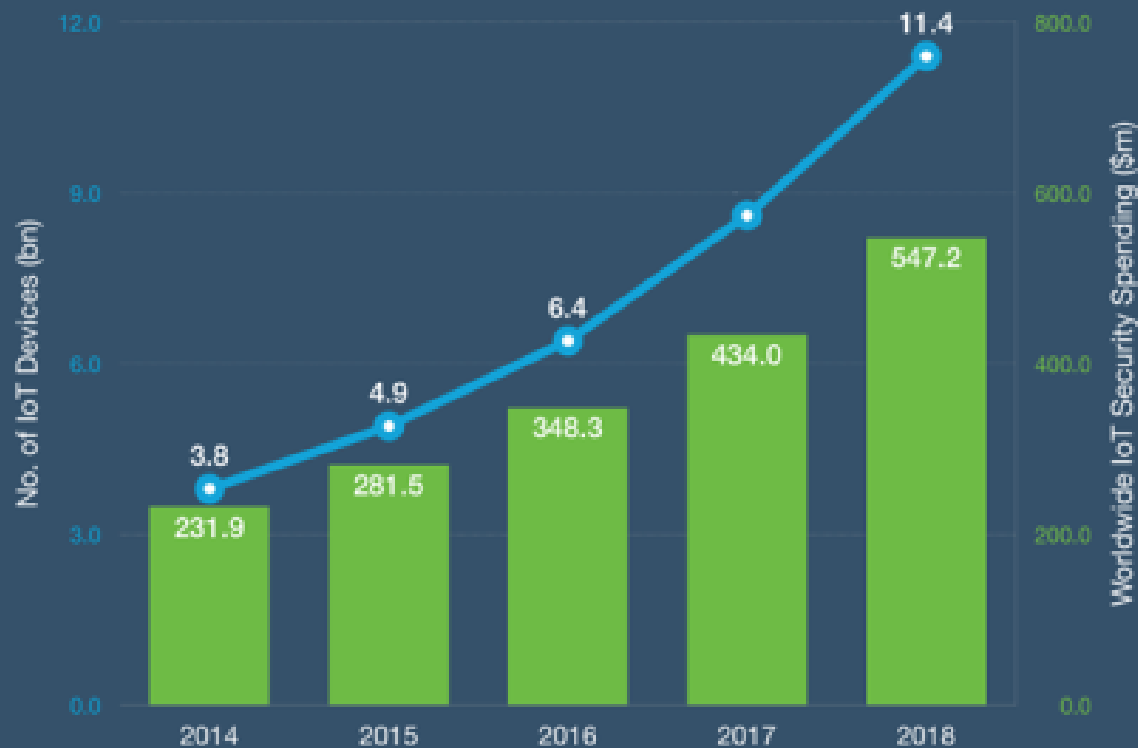
Data: Gartner, various    Graphic: TelecomTV

By 2020

**25%**  
of Enterprise attacks  
will involve IoT

**10%**  
of IT security budgets  
allocated to IoT

**50%**  
of IoT implementations  
will use Cloud security



Source: <https://itu4u.wordpress.com/2016/06/14/improving-iot-security/>

# Real and Present Danger

- A number of recent incidents indicate that there is a “real and present” danger
- Similarities with the mobile app space also offer **guidance**
  - App store model: “Let a thousand flowers bloom”
    - **Unsophisticated developers/providers**
  - And also **unsophisticated end-users**
    - “unmanaged” or “poorly managed” devices
  - **The onus is in great part on the ecosystem operators...just like with mobile app stores**

# Real and Present Danger: Three Examples

1. Car Hacking
2. Home device hacking & DDoS attacks
3. IFTTT scripts

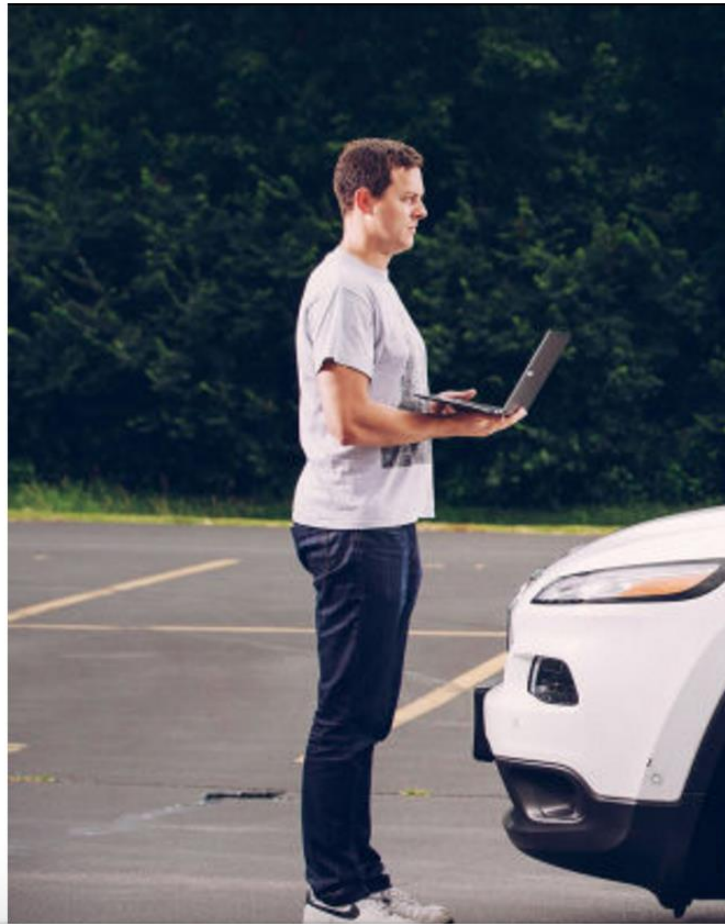
# Example 1: *Car Hacking*





ANDY GREENBERG SECURITY 07/15 6:00 AM

# HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the Jeep Cherokee started blasting cold air at the maximum setting, chilling the sweat on my back through the in-seat climate control system. Next the radio switched to the local hip hop station and began blaring Skee-lo at full volume. I spun the control knob left and hit the power button, to no avail. Then the windshield wipers turned on, and wiper fluid blurred the glass.

As I tried to cope with all this, a picture of the two hackers performing these stunts appeared on the car's digital display: Charlie Miller and Chris Valasek, wearing their trademark track suits. A nice touch, I thought.

ALMOST EXACTLY A year ago, Chrysler announced a recall for 1.4 million vehicles after a pair of hackers demonstrated to WIRED that they could remotely hijack a Jeep's digital systems over the Internet. For Chrysler, the fix was embarrassing and costly. But now those two researchers have returned with work that asks Chrysler and the automotive industry to imagine an alternate reality, one where instead of reporting their research to the automaker so it could be fixed, they had kept working on it in secret—the way malicious hackers would have. In doing so, they've developed a new hack that offers a sobering lesson: It could

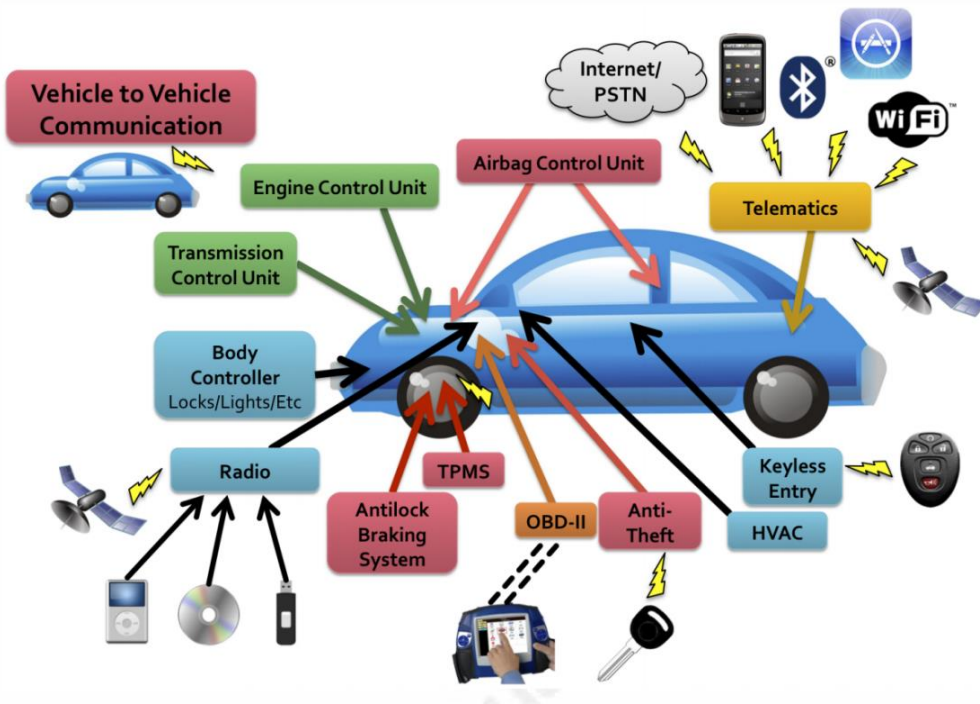
**Took advantage of Uconnect, a system that connects cellular communications, navigation, infotainment, and built-in apps.**

**Demonstration relied on vehicle's IP address but researchers also discovered a port scan that would have allowed them to discover all vulnerable vehicles nationwide!**

week, Miller and Valasek launched attacks against Chrysler's Uconnect system in 2015. Last year, they demonstrated how they could even remotely control a vehicle's engine, locking the doors, and changing the radio station. "If we had known as early as we did that this was more dangerous, we would have accelerated our work on the vehicle's security," says Miller. "If instead of cutting the transmission on the highway, we'd turned the steering wheel 180 degrees," says Chris Valasek. I can imagine. But the

# CAN Bus Vulnerabilities

**Controller Area Network (CAN) Bus:** centralized network on which **all vehicle data traffic is broadcast**



- ✧ No boundary defense
- ✧ No device authentication
- ✧ No encryption
- ✧ Security by obfuscation

Source: <https://www.sans.org/reading-room/whitepapers/ICS/developments-car-hacking-36607>

# Role of the Ecosystem

- Automotive industry has to develop new standards for security
  - Security boundaries
  - Encryption (integrity)
  - Authentication and authorization
  - Process to certify components
  - Promote security by design practices

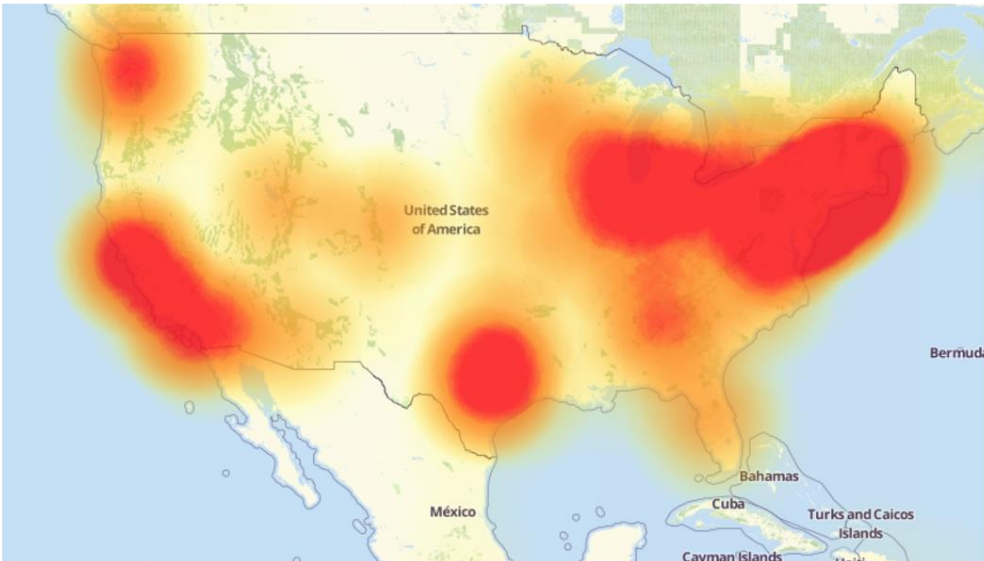
## Example 2: *Home Device Hacking*



## 21 Hacked Cameras, DVRs Powered Today's Massive Internet Outage

A massive and sustained Internet attack that has caused outages and network congestion today for a large number of Web sites was launched with the help of hacked "Internet of Things" (IoT) devices, such as CCTV video cameras and digital video recorders, new data suggests.

Earlier today cyber criminals began training their attack cannons on **Dyn**, an Internet infrastructure company that provides critical technology services to some of the Internet's top destinations. The attack began creating problems for Internet users reaching an array of sites, including Twitter, Amazon, Tumblr, Reddit, Spotify and Netflix.



A depiction of the outages caused by today's attacks on Dyn, an Internet infrastructure company. Source: Downtetector.com.

# October 2016

- ✧ Mirai **Botnet** attacks Dyn – Major DNS service provider
- ✧ Estimates of **600,000 compromised devices** creating traffic of **up to 1.2Tbps** ---  
<https://www.theguardian.com/technology/2016/oct/26/dos-attack-dyn-mirai-botnet>
- ✧ Sites impacted by attack included **Twitter, Pinterest, PayPal, Verizon, Comcast, Playstation, and many others**

TECH | TECHNOLOGY

## What's Attacking the Web? A Security Camera in a Colorado Laundromat

Computer viruses are harnessing webcams, thermostats and other connected devices—while owners remain in the dark



- ✧ Owner didn't notice traffic generated by her camera
- ✧ Camera would regularly crash but she learned to just restart it
- ✧ She lost her password but the manufacturer just resets the password to its default (123456) when this happens
- ✧ The security person who installed the camera learned about the virus after being contacted by the press
- ✧ Camera manufacturer denies any responsibility

A video recorder at this laundromat in Carbondale, Colo., was infected with a computer virus that propagates through household devices connected to the internet. The laundromat's owner was unaware her security system was hosting the virus. PHOTO: BLAKE GORDON FOR

# Unsophisticated Users and IoT Manufacturers

- Devices managed by unsophisticated everyday users
  - Devices not patched
  - Devices using no or default passwords
- Unsophisticated Manufacturers
  - Devices resetting to default passwords (e.g. 123456)
- Some estimates:
  - 15% of home routers are unsecured -  
<http://www.welivesecurity.com/2016/10/19/least-15-home-routers-unsecure/>
  - 73,000 security cameras with default passwords  
<http://www.welivesecurity.com/2014/11/11/website-reveals-73000-unprotected-security-cameras-default-passwords/>



# Manufacturer Usage Descriptions (MUD)

- Proposal developed by CISCO to curb DDoS attacks from compromised devices
  - Connected device provides network controller (or equivalent) a **URI that links to the device manufacturer's MUD server**
  - **MUD description** is an XML file **describing legitimate device behavior**
    - e.g. surveillance camera can communicate with monitoring station but not with Twitter
  - Network controller creates a **security policy** & merges it with its existing network policy that **decides what to allow and what to block**
- IETF RFCI currently under review

## Example 3: *Unsophisticated Everyday IoT Developers*

# If This Then That (IFTTT)

- **Web-based service that allows users to create chains of simple conditional statements (“recipes”)** tied to changes/”triggers” in other services (e.g. gmail, pinterest, facebook, presence sensors, etc)
- Example: “*Whenever I’m tagged by someone on Facebook, add the photo to my cloud-based photo archive*”
- Includes specialized versions for iPhones and Android phones
- In 2012, started **integration with IoT devices** – beginning with Belkin light switch, motion sensors, etc



# IFTT Building Blocks

- **Channels:** data from different web services (e.g. YouTube, Facebook, eBay) and actions controlled by some APIs (e.g . Texting)
- **Triggers:** Event that triggers a recipe (If “this”)
- **Actions:** Action taken when trigger occurs (then “that”)
- **Recipes:** the rules
- **Ingredients:** Parameters made available by trigger (e.g. a particular photo, the subject in an email)

# Sample Shared Recipes

<https://ifttt.com/recipes>

**if** **then**



Save screenshots to a separate iOS album

by [fisjon](#) 93k 2.0k



**if** **then**



Change your Android wallpaper to NASA's image of the day

by [mikesech](#) 165k 3.1k

**if** **then**



Remind yourself to put on sunscreen when the UV Index is high

by [mayallama](#) 32k 727

**if** **then**





Keep your profile pictures in sync

**if** **then**



Save your new Instagram photos to Dropbox

**if** **then**



Save videos in Pocket added to your Watch Later playlist

**As of June 2016: integrated with 300 services, claims 1.2M daily users, and over 400,000 shared recipes**

**Turn off Wi-Fi when your phone's battery is low**

by [maxmeyers](#) 18k 235

**Save a copy of new photos you take to Dropbox**

by [bunnie](#) 71k 2.0k

**Receive a weather report via IF notification at 7:30AM.**

by [htwyford](#) 25k 519

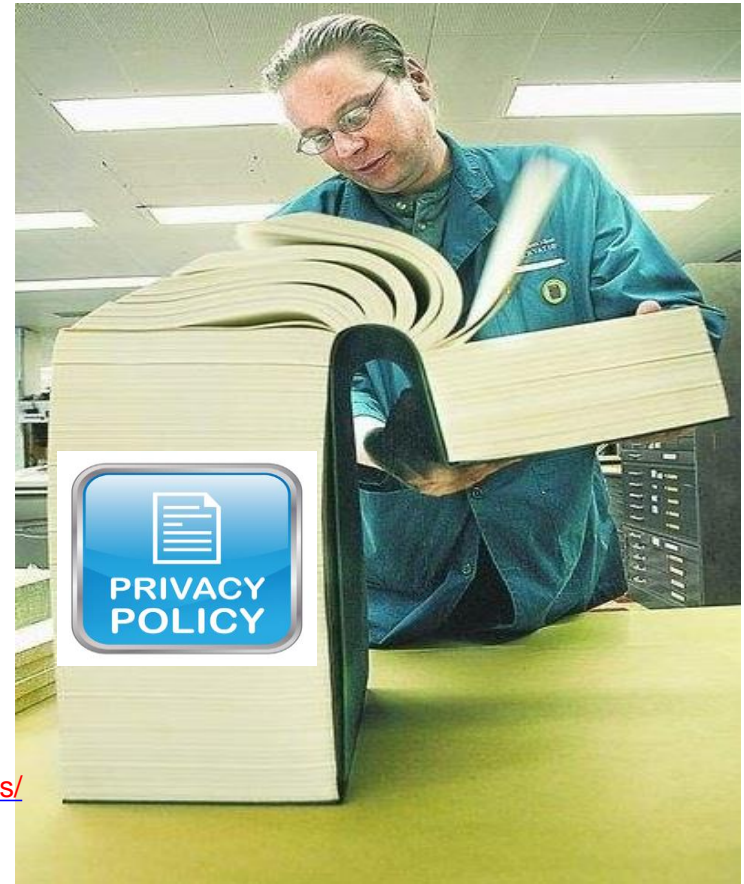
# IFTT – Security and Privacy Concerns

- Integration across a number of APIs means that the “attack surface” is also really large
- Surbatovich, Aljuraidan, Bauer, Das, Jia, “Some Recipes Can Do More than Spoil your Appetite: Analyzing the security and privacy risks of IFTTT recipes”, WWW 2017

# Privacy in the Age of IoT: Similar Challenges

- **Notice and choice** in its current implementation is **not working/practical**
- **91%** of people report feeling they **have lost control over their information**

Pew Survey 2014 <http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/>



# Mobile and IoT: A Number of Complicating Factors

- A typical mobile phone user with 50 mobile apps each requesting 3 permissions would have to **configure 150 settings**
- IoT: Technology is often “invisible”
- **Reading policies is even less practical**
- **Explosion in the number of apps and devices: Developers often lack the necessary sophistication**

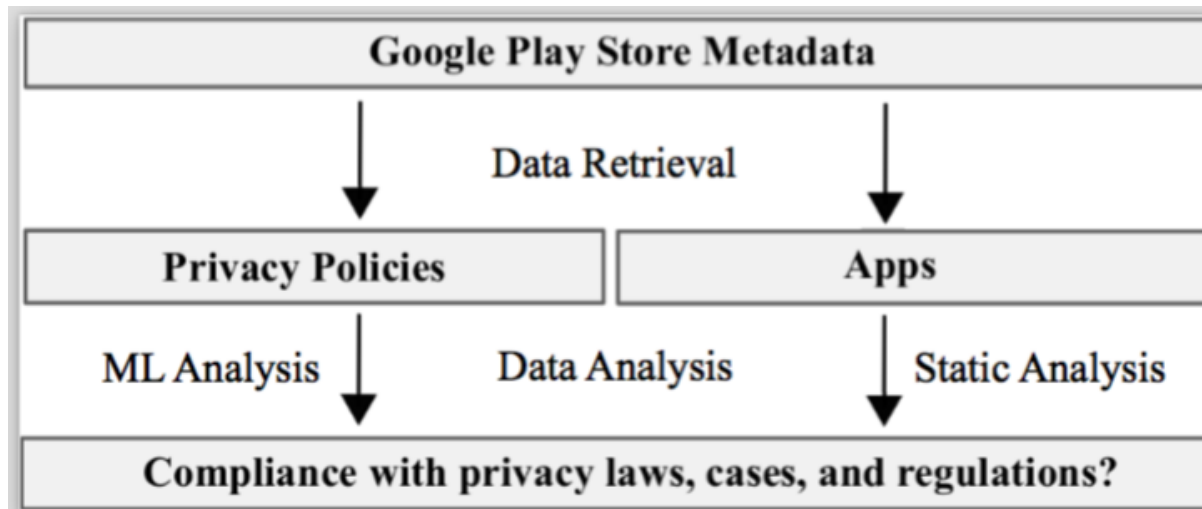
“Modeling Users’ Mobile App Privacy Preferences: Restoring Usability in a Sea of Permission Settings”, J. Lin, B. Liu, N. Sadeh, J. Hong, Proc. of the USENIX Symposium on Usable Privacy and Security, SOUPS 2014, Jul. 2014



# What is Needed...

- **Technology to Help Developers/Device Manufacturers**
  - Articulate and Disclose privacy practices
  - Mobile App Developers have a terrible time articulating their privacy policies. Same problem with IoT developers & manufacturers
- **Technology to Help Users**
  - Selectively inform users about privacy practices they care about & help them configure relevant settings

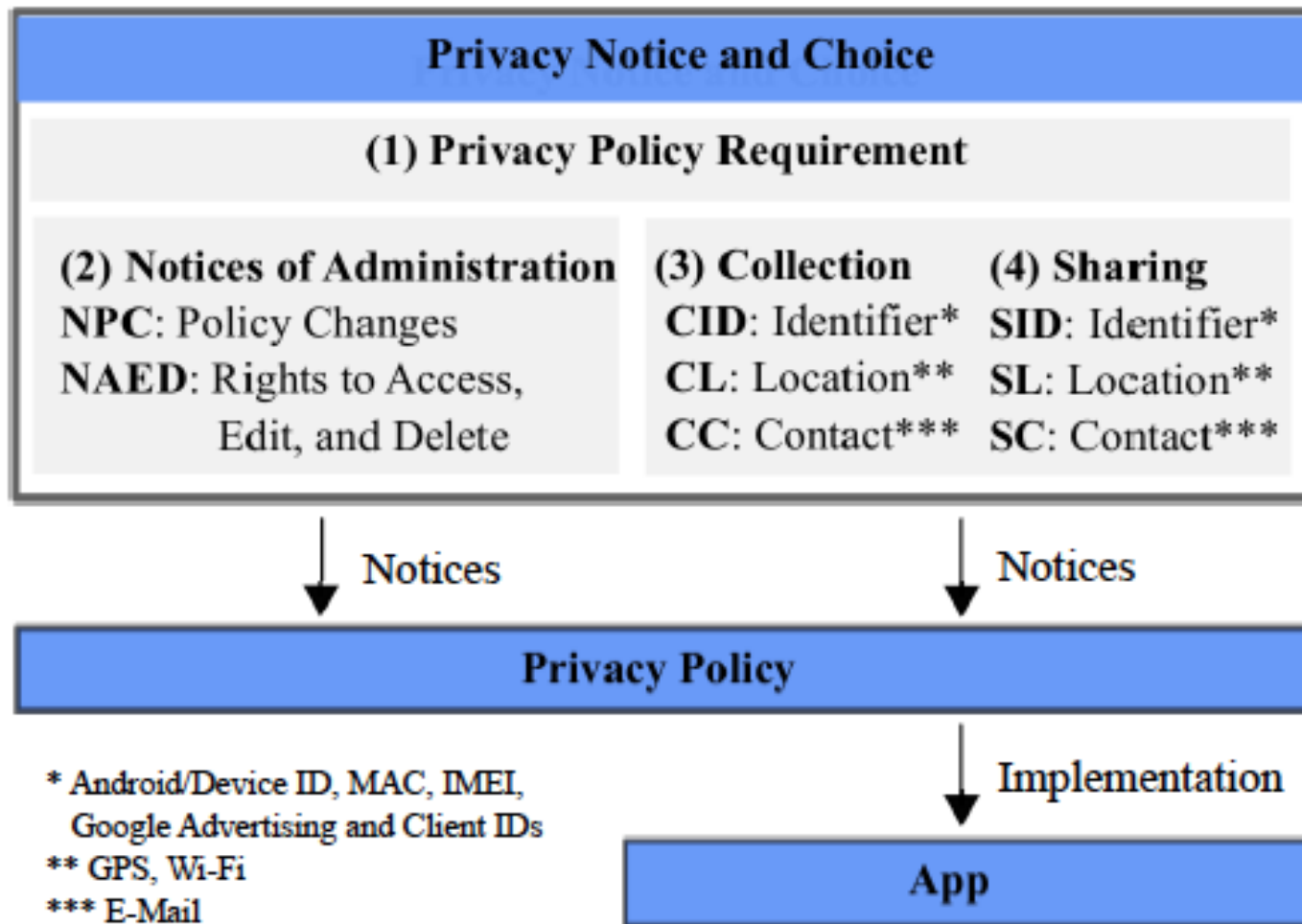
# Identifying Privacy Violations – Work @ CMU



- Training **machine learning classifiers** to extract relevant policy statements
- Compare these statements against:
  - **Regulatory requirements**
  - What the software actually does
    - **Static and dynamic code analysis**

“Analyzing and Predicting Privacy Law Compliance of Mobile Apps”, S. Zimmeck, Z.Wang, L. Zou, B. Liu, F. Schaub, S. Wilson, N. Sadeh, S. Bellovin, J. Reidenberg, NDSS 2017.

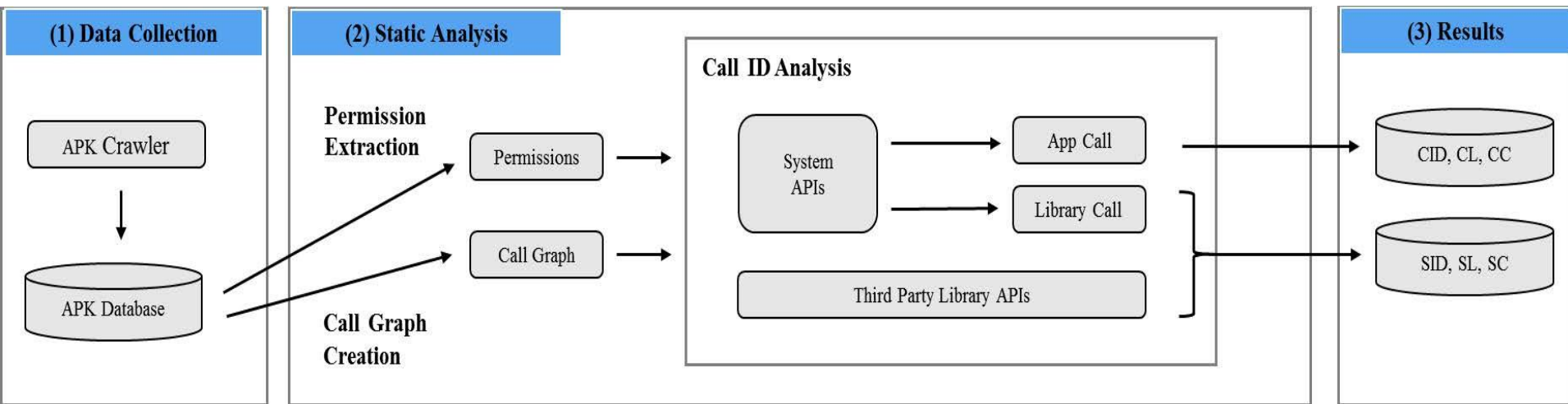
# Formalizing the Problem



**Note:** In US, FTC FIPPS mandates notice before collection of PII; COPPA requires policies for apps directed to children; CalOPPA: policy required if PII collected; COPPA requires NAED; CID and CL require disclosure under CalOPPA and COPPA and sharing requires consent; CalOPPA and DOPPA require description of notification process for policy change

# Initial Study

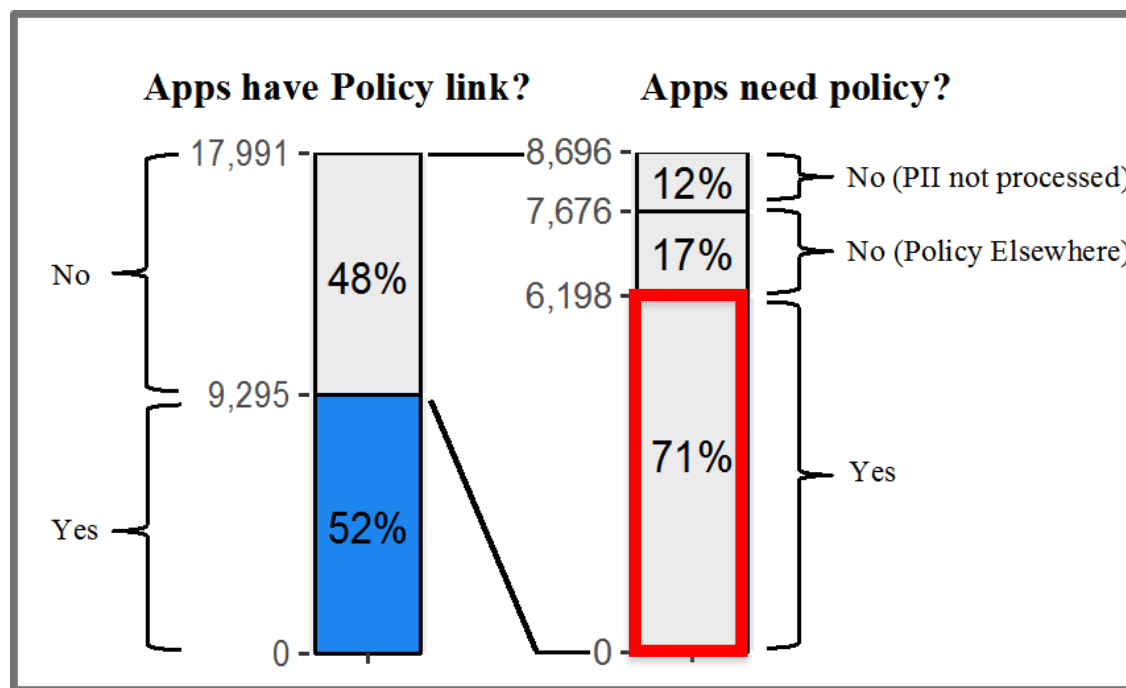
- Analysis of 17,991 free mobile apps on Google Play Store
  - For reference, in 2014, the Global Privacy Enforcement Network (GPEN) was only able to analyze 1,211 apps in one week with the involvement of 26 data protection agencies



Adapted Androguard

# Major Findings - I

- No Policy Link in app store



71% of apps with no policy seem to be in violation

# Major Findings –II

*Apps with privacy policies (9,295)*: average of 2.79 potential violations

## Examples:

- 71% SID but only 10% disclose it! **Suggests 61% might be non-compliant**
- 20% SL but only 12% disclose it! **Suggests 8% might be non-compliant**

# Possible Use of this Technology

- Tools to **help developers** avoid being in violation of relevant laws – to be provided by app stores/ecosystems
- Tools to **help app stores (and regulators)** identify potential violations of relevant laws

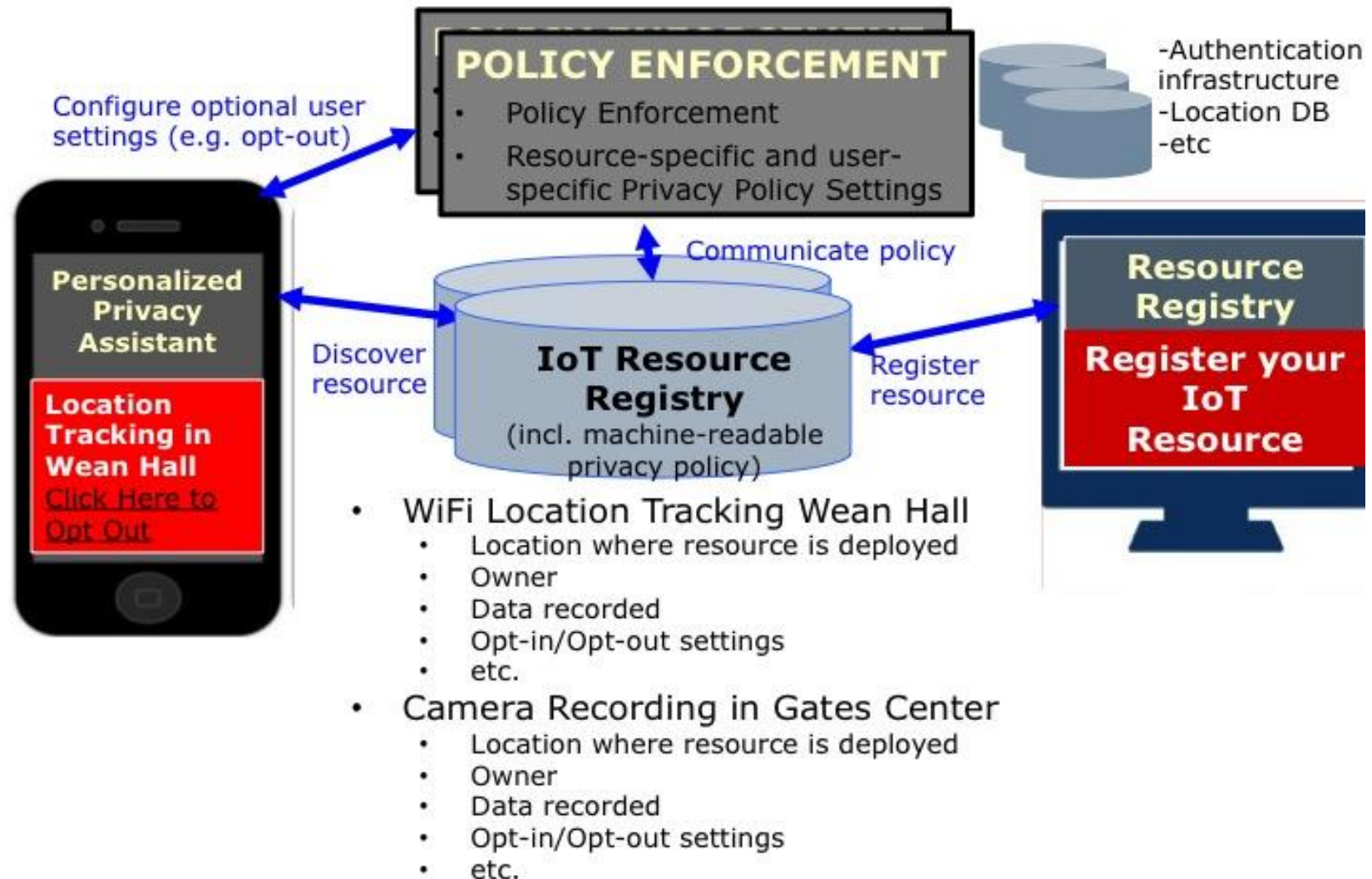
**Illustrates the important role to be played by ecosystem operators**

# IoT Privacy Notice: Another Example





# Privacy Infrastructure for IoT



# Key Infrastructure Components

- **Registries** and associated **admin portals**
- **Authentication and Authorization**
  - **Advertising IoT resources and their privacy practices**
- **Privacy policy language**
- Protocols for **discovery and querying**
- Protocols to **configure** available **settings**
- **Privacy Assistants** – incl. user modeling

# IoT Resource Registry Portal

IRR

IoT Resources ▾


IoT Services ▾


 Martin Degeling ▾


## Register a new IoT Resource


 Basic Information


 Context

 Collected Data

 Granularity

 Purpose

 Times and Retention

 Shared With

 Control Options

SUBMIT

## Control Options

Service ID


concierge

Subsystem ID

wifi

Response URL

<https://tippersweb.uci.edu/api>

 add action

Opt in

Description

▼ WIFI Location Tracking is enabled

Link to additional information

<https://tippersweb.uci.edu/api/opt-in>



Opt out

Description

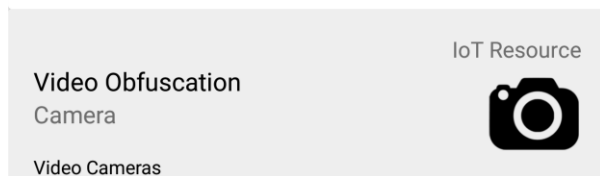
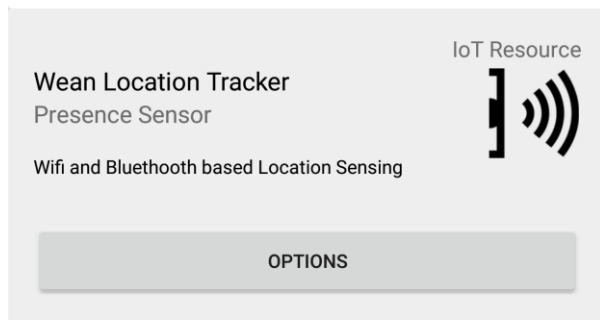
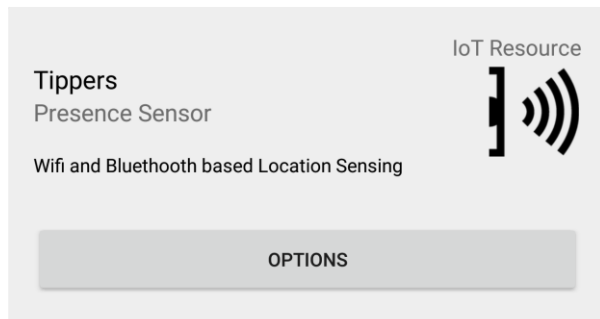
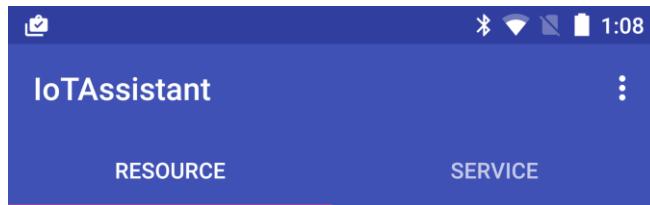
▼ WIFI Location Tracking is disabled

Link to additional information

<https://tippersweb.uci.edu/api/opt-out>



# IoT Assistant



## Wifi and Bluetooth based Location Sensing

### Details

#### COLLECTOR

Collector Description  
Wifi and Bluetooth based Location Sensing

#### LOCATION

Location Name  
Donald Bren Hall

Location Owner Name  
UC Irvine

#### OPERATOR

Operator Name  
Information Systems Group

#### RETENTION

#### AVAILABLE PRIVACY SETTINGS

Coarse grained location tracking is enabled ☒

Fine grained location tracking is enabled ☒

# System in Action



Video: 6 minutes

# Current Status - I

- **Initial deployments at CMU and UCI**
  - Extending infrastructure to accommodate diverse set of devices, sensors/services and apps
- **Learning people's privacy preferences, expectations and notification preference**
  - Successfully demonstrated for mobile app permission preferences: user answers 3 to 5 questions & privacy assistants can predict many of the user's permission settings

# Current Status – II



## [ROOT] Privacy Assistant

Mobile Commerce Lab @ Carnegie Mellon University

Tools

★★★★★ 4

Everyone

Add to Wishlist

Install

**Tell Us About Your Privacy Preferen...**

To help the privacy assistant recommend settings, please answer a few quick questions.

(You will be asked up to 5 questions. This shouldn't take more than a couple of minutes.)

**Privacy Assistant**

In general, do you feel comfortable with **Social** apps accessing your **Camera**?

Social apps installed on your phone accessing Camera:

- Google+
- Facebook
- Snapchat

**Privacy Assistant**

In general, do you feel comfortable with **Finance** apps accessing your **Location**?

Finance apps installed on your phone accessing Location:

- PayPal
- Citi Mobile
- Chase

MOSTLY NO NOT SURE MOSTLY OK



# Current Status - III

- **Templates for off-the-shelf IoT devices and services**
  - Currently a dozen templates – e.g., Nest cam, Amazon Echo, Google Home, Microsoft Kinect, Apple TV, Wink Relay, Canary sensors, Honeywell Lyric T5 Thermostat, CUJO smart firewall
  - End-user can now **download templates to populate Information Registry** at home or at the office
- **Tool for IoT developers/manufacturers to create registry templates for their resources**



# Summary - I

- Unless addressed early on, broad **IoT adoption could be hampered by security and privacy issues**
  - A number of attacks and incidents already illustrate how serious a problem this is likely to become
- IoT is characterized by:
  - **Growing attack surfaces** – variety of devices and services that are all intended to be interoperable
  - **Wide variety of device/service/app providers** – many of them **lacking the sophistication** and **tools** to properly address security and privacy issues
  - **End users as system administrators**
  - All amounting to a recipe for disaster

# Summary - II

- As with the mobile ecosystem, the **large ecosystem operators will have to take responsibility for developing tools, standards, and infrastructure elements that lower the bar** for developers and end-users when it comes to supporting security and privacy

# Summary - III

- Examples include technologies developed at CMU to:
  - Help **articulate privacy policies that are compliant**
  - Help **advertise IoT resources and their data practices**, including available **settings**
  - Help users **discover and configure security and privacy settings**
    - **Privacy and Security Assistants**

**Acknowledgements:** Work funded by the National Science Foundation, DARPA and Google

The **Usable Privacy Policy Project** and the **Personalized Privacy Assistant Project** both involve a collaborations with a number of individuals. See **[usableprivacy.org](http://usableprivacy.org)** and **[privacyassistant.org](http://privacyassistant.org)** for additional details incl. lists of collaborators and publications

**Q&A**