



# PRIVACY CON

FEDERAL TRADE COMMISSION

📍 DC // 1.14.16



# Session 5: Security and Usability



# Sarthak Grover

Princeton University

## *The Internet of Unpatched Things*

Co-author: Nick Feamster (Princeton University)



# The Internet of Unpatched Things

Sarthak Grover and Nick Feamster  
Princeton University

PrivacyCon '16

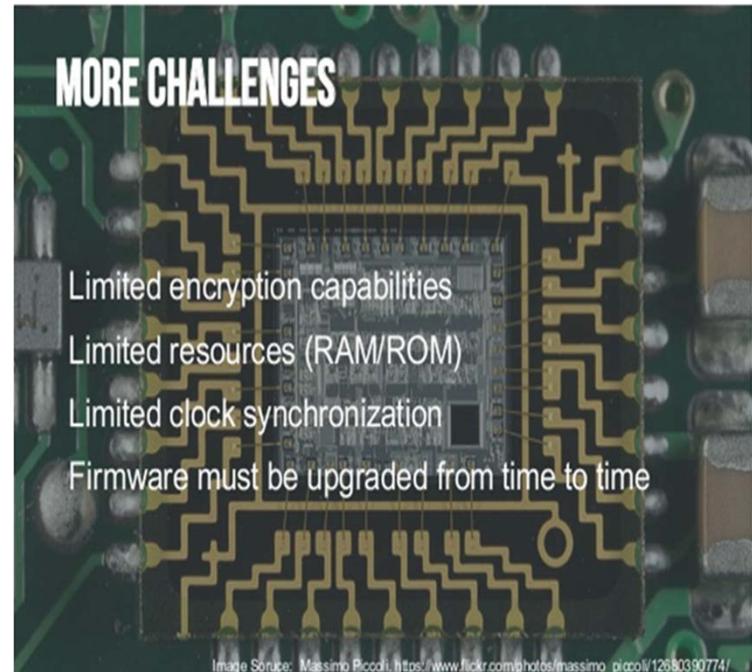
# Current State of Consumer Smart Devices

Many different manufacturers, small startups, novice programmers

Low capability hardware, not enough for security protocols

Most data goes to an online server on the cloud

Even devices in the same home communicate via the cloud



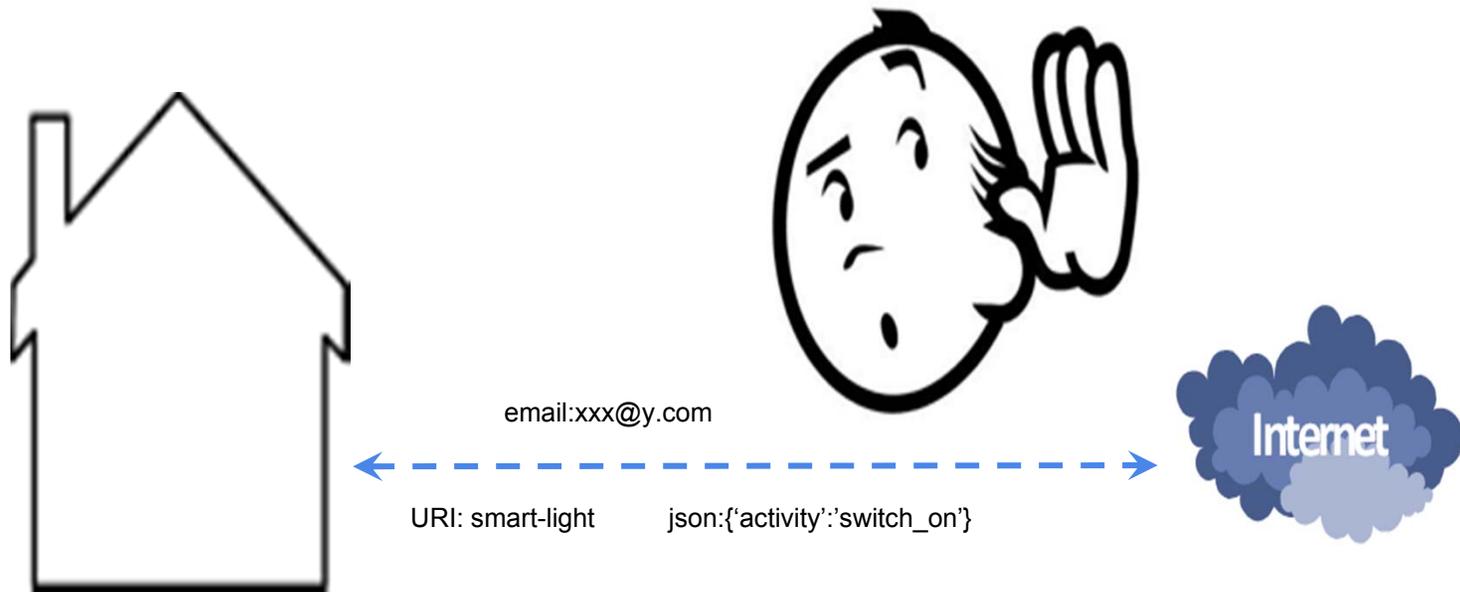
# Unpatched IoT Devices Put Our Privacy at Risk

IoT device network traffic:

Leaks user information

Identifies the device being used

May also identify current user activity and behavior!



# Case Study of Some Common Home IoTs



# Digital Photoframe: Traffic Analysis

All traffic and feeds (RSS) cleartext over HTTP port 80

All actions sent to server in HTTP GET packet

Downloads radio streams in cleartext over different ports

DNS queries: [api.pix-star.com](http://api.pix-star.com), [iptime.pix-star.com](http://iptime.pix-star.com)



# Photoframe: Privacy Issues

User **email ID** is in clear text  
when syncing account

Current **user activity** in clear text  
in HTTP GET

DNS queries and HTTP traffic  
identifies a pix-star photoframe

```
805 789.12607306 176.31.232.79 10.42.0.22 80 55833 HTTP/XML
20613 800.90983706 176.31.232.79 10.42.0.22 80 55838 HTTP
20683 846.60266706 10.42.0.22 176.31.232.79 43560 80 HTTP
20685 846.71147606 176.31.232.79 10.42.0.22 80 43560 HTTP/XML
20693 846.86485306 10.42.0.22 176.31.232.79 43561 80 HTTP
20696 846.86538306 10.42.0.22 176.31.232.79 43562 80 HTTP
Hypertext Transfer Protocol
  HTTP/1.1 200 OK\r\n
  [Expert Info (Chat/Sequence): HTTP/1.1 200 OK\r\n]
    [HTTP/1.1 200 OK\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Version: HTTP/1.1
    Status Code: 200
    Response Phrase: OK
    Server: nginx/1.4.1\r\n
    Date: Tue, 03 Feb 2015 21:02:31 GMT\r\n
    Content-Type: application/xml;charset=UTF-8\r\n
    Content-Length: 171\r\n
    Connection: keep-alive\r\n
    \r\n
    [HTTP response 1/1]
    [Time since request: 0.108809000 seconds]
    [Request in frame: 20683]
  eXtensible Markup Language
    <xml>
      <status
        SLEEPING="0"
        ADDRESS="livinglab@mypixstar.com"
        ALBUM="1"
        RADIO="1422997193"
        EMAIL="0"
        DEFAULT="0 0"
        FIRMWARE="1.023"
        SYNC_TIME="80"
        CONTACTS_TIME="1"/>
      </xml>
```

email

current activity

```
Hypertext Transfer Protocol
  GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listcontacts HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listcontacts HTTP/1.1\r\n]
    [GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listcontacts HTTP/1.1\r\n]
Hypertext Transfer Protocol
  GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listradiogenres HTTP/1.1\r\n
  [Expert Info (Chat/Sequence): GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listradiogenres HTTP/1.1\r\n]
    [GET /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listradiogenres HTTP/1.1\r\n]
    [Severity level: Chat]
    [Group: Sequence]
    Request Method: GET
    Request URI: /api/?hsh=call148eddae99b98a7689abf83fdd06&usr=b4ab2c083cf8&action=listradiogenres
    Request Version: HTTP/1.1
```

# IP Camera: Traffic Analysis

All traffic over cleartext HTTP port 80, even though viewing the stream requires login password

Actions are sent as HTTP GET URI strings

Videos are sent as image/jpeg and image/gif in the clear

FTP requests also sent in clear over port 21, and FTP data is sent in clear text over many ports above 30,000

DNS query: [www.sharxsecurity.com](http://www.sharxsecurity.com)



# IP Camera: Privacy Issues

Video can be recovered from FTP data traffic by network eavesdropper

DNS query, HTTP headers, and ports identify a Sharx security camera

private user data

8	14.679939000	10.42.0.44	46.252.157.130	45962	21	FTP	74	Request: TYPE I
9	14.820736000	46.252.157.130	10.42.0.44	21	45962	FTP	96	Response: 200 TYPE is now 8-bit binary
10	14.821660000	10.42.0.44	46.252.157.130	45962	21	TCP	66	45962-21 [ACK] Seq=17 Ack=88 Win=8280 Len=0 TSval=1256532 TSe
11	14.823297000	10.42.0.44	46.252.157.130	45962	21	FTP	72	Request: PASV
12	14.957638000	46.252.157.130	10.42.0.44	21	45962	FTP	117	Response: 227 Entering Passive Mode (46,252,157,130,124,42)
13	14.959068000	10.42.0.44	46.252.157.130	60649	31786	TCP	74	60649-31786 [SYN] Seq=0 Win=5840 Len=0 MSS=1460 SACK PERM=1 T
14	14.995413000	10.42.0.44	46.252.157.130	45962	21	TCP	66	45962-21 [ACK] Seq=23 Ack=139 Win=8280 Len=0 TSval=1256550 TS
15	15.092593000	46.252.157.130	10.42.0.44	31786	60649	TCP	74	31786-60649 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1386 S
16	15.093262000	10.42.0.44	46.252.157.130	60649	31786	TCP	66	60649-31786 [ACK] Seq=1 Ack=1 Win=5840 Len=0 TSval=1256559 TS
17	15.096021000	10.42.0.44	46.252.157.130	45962	21	FTP	102	Request: STOR M 2015-03-17 17-37-23 348.jpg
18	15.230540000	46.252.157.130	10.42.0.44	21	45962	FTP	96	Response: 150 Accepted data connection
19	15.231793000	10.42.0.44	46.252.157.130	45962	21	TCP	66	45962-21 [ACK] Seq=59 Ack=169 Win=8280 Len=0 TSval=1256573 TS
20	15.233158000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440	FTP Data: 1374 bytes
21	15.233544000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440	FTP Data: 1374 bytes
22	15.233885000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1414	FTP Data: 1348 bytes
23	15.371483000	46.252.157.130	10.42.0.44	31786	60649	TCP	66	31786-60649 [ACK] Seq=1 Ack=1375 Win=17280 Len=0 TSval=258450
24	15.371922000	46.252.157.130	10.42.0.44	31786	60649	TCP	66	31786-60649 [ACK] Seq=1 Ack=2749 Win=20096 Len=0 TSval=258450
25	15.372409000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440	FTP Data: 1374 bytes
26	15.372557000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440	FTP Data: 1374 bytes
27	15.372976000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440	FTP Data: 1374 bytes
28	15.373113000	10.42.0.44	46.252.157.130	60649	31786	FTP-DATA	1440	FTP Data: 1374 bytes



# Ubi: Traffic Analysis

All voice-to-text traffic sent in clear over port 80

Activities sent in clear, and radio streamed over port 80

Sensor readings are synced with server in the background over port 80

Only communication with google API used HTTPS on port 443 and port 5228  
(google talk)

DNS query: portal.theubi.com, www.google.com, mtalk.google.com,  
api.grooveshark.com

# Ubi: Privacy Issues

Although HTTPS is clearly available, Ubi still uses HTTP to communicate to its portal. Eavesdropper can intercept **all voice chats and sensor readings** to Ubi's main portal

Sensor values such as sound, temperature, light, humidity can identify if the user is home and currently active

**Email in the clear** can identify the user

DNS query, HTTP header (UA, Host) clearly identifies Ubi device

```
.._/.... .....)
..POST / ubi/v2/s
ensor?ac cessToke
n=89da8e e0-7f66-
4796-9f9 0-1a436a
1f58ce H TTP/1.1.
.Accept: applica
tion/jso n..Conne
ction: C lose..Co
ntent-Ty pe: appl
ication/ json..Us
er-Agent : Dalvik
/1.6.0 ( Linux; U
; Androi d 4.4.2;
UBI MK8 02IV Bui
ld/KOT49 H)..Host
: portal .theubi.
com..Acc ept-Enco
ding: gz ip..Cont
ent-Leng th: 311.
...[{"se nsorName
": "sound level", "
sensorVa lue": "66
.28", "ti meDetect
ed": 1427 07436052
6}, {"sen sorName"
: "temper ature", "
sensorVa lue": "20
.31", "ti meDetect
ed": 1427 07436173
9}, {"sen sorName"
: "light", "sensor
Value": " 221.0", "
timeDete cted": 14
27074361 740}, {"s
ensorNam e": "humi
dity", "s ensorVal
ue": "41. 73", "tim
eDetecte d": 14270
74361741 }]]
```

current activity

```
▼ JavaScript Object Notation: application/json
  ▼ Array
    ▼ Object
      ▼ Member Key: "category"
        String value: UTTERANCE
      ▼ Member Key: "message"
        String value: how do I talk to you
      ▼ Member Key: "type"
        String value: FROMUSER
      ▼ Member Key: "time"
        Number value: 1427075208996
```

current state

```
▼ Object
  ▼ Member Key: "category"
    String value: UTTERANCE
  ▼ Member Key: "message"
    String value: I am not fond of me at all
  ▼ Member Key: "type"
    String value: FROMUBI
  ▼ Member Key: "time"
    Number value: 1427075209004
```

# Nest Thermostat: Traffic Analysis

All traffic to nest is HTTPS on port 443 and 9543

Uses TLSv1.2 and TLSv1.0 for all traffic

We found some incoming weather updates containing location information of the home and weather station in the clear.

**Nest has fixed this bug after our report.**

DNS query: time.nestlabs.com, frontdoor.nest.com, log-rts01-iad01.devices.nest.net. transport01-rts04-iad01.transport.home.nest.com



# Nest: Privacy Issues

Fairly secure device: all outgoing personal traffic, including configuration settings and updates to the server, use HTTPS

\*User zip code bug has been fixed

DNS query as well as the use of the unique port 9543 clearly identifies a Nest device.

```
{HTTP/1 .1 200 0
K..Conte nt-Type:
  applica tion/jso
n..Conte nt-Lengt
h: 7531. .Connect
ion: kee p-alive.
...{"085 42,US":{
"locatio n":{"sta
tion_id" : "KNJPRI
NC11", "c ountry":
"US", "la t": "40.3
5179138" , "lon": "
-74.6601 6388", "s
hort_nam e": "Prin
ceton, NJ ", "timez
one": "ED T", "time
zone_lon g": "Amer
ica/New_York", "g
mt_offse t": "-4.0
0", "full_name": "
Princeto n, NJ 085
42 US", " city": "P
rinceton ", "state
": "NJ", " zip": "08
542"}, "c urrent":
{"temp_f ": 36.6, "
temp_c": 2.6, "con
dition": "Clear",
```

user zip code\*

# Smarthings Hub: Traffic Analysis

All traffic over HTTPS on port 443 using TLS v1.2

No clear text port 80 traffic

Flows to an Amazon AWS instance running smarthings server

3-5 packets update every 10 sec in the background

DNS query: `dc.connect.smarthings.com`

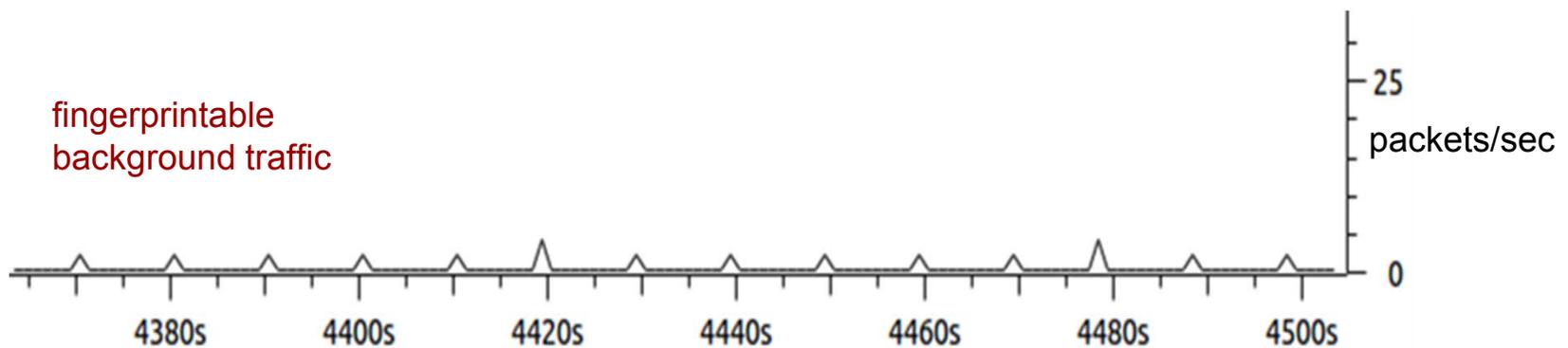


# Smarthings: Privacy Issues

Very secure: No information about IoT devices attached to hub is leaked

Background updates every 10 seconds (over HTTPS) fingerprint the hub

DNS query identifies Smarthings hub, but not individual devices



Smarthings Traffic

# Conclusion: Be Afraid!

Very difficult to enforce security standards

Multiple manufacturers

Low capability devices

Use of non-standard protocols and ports

Difficult to maintain and patch due to low workforce and/or expertise

Who is responsible? (ISPs? Consumers? Manufacturers?)

Who is liable? Who should pay?

# Conclusion: Be Afraid!

Very difficult to enforce security standards

Multiple manufacturers

Low capability devices

Use of non-standard protocols and ports

Difficult to maintain and patch due to low workforce and/or expertise

Who is responsible? (ISPs? Consumers? Manufacturers?)

Who is liable? Who should pay?

**Can we solve this on the network? If so, how?**

How much information about user behavior do devices leak to the network?

Can we offload device security to the home gateway or the cloud?

**Thanks!**

# Vitaly Shmatikov

Cornell Tech

*What Mobile Ads Know About Mobile Users*



# What Mobile Ads Know About Mobile Users

Vitaly Shmatikov

joint work with  
Sooel Son and Daehyeok Kim

# 1.8 million

apps in Google Play Store

source: AppBrain

41% include at least one  
mobile advertising library

source: AppBrain

# Every third

ad-supported app includes  
multiple advertising libraries

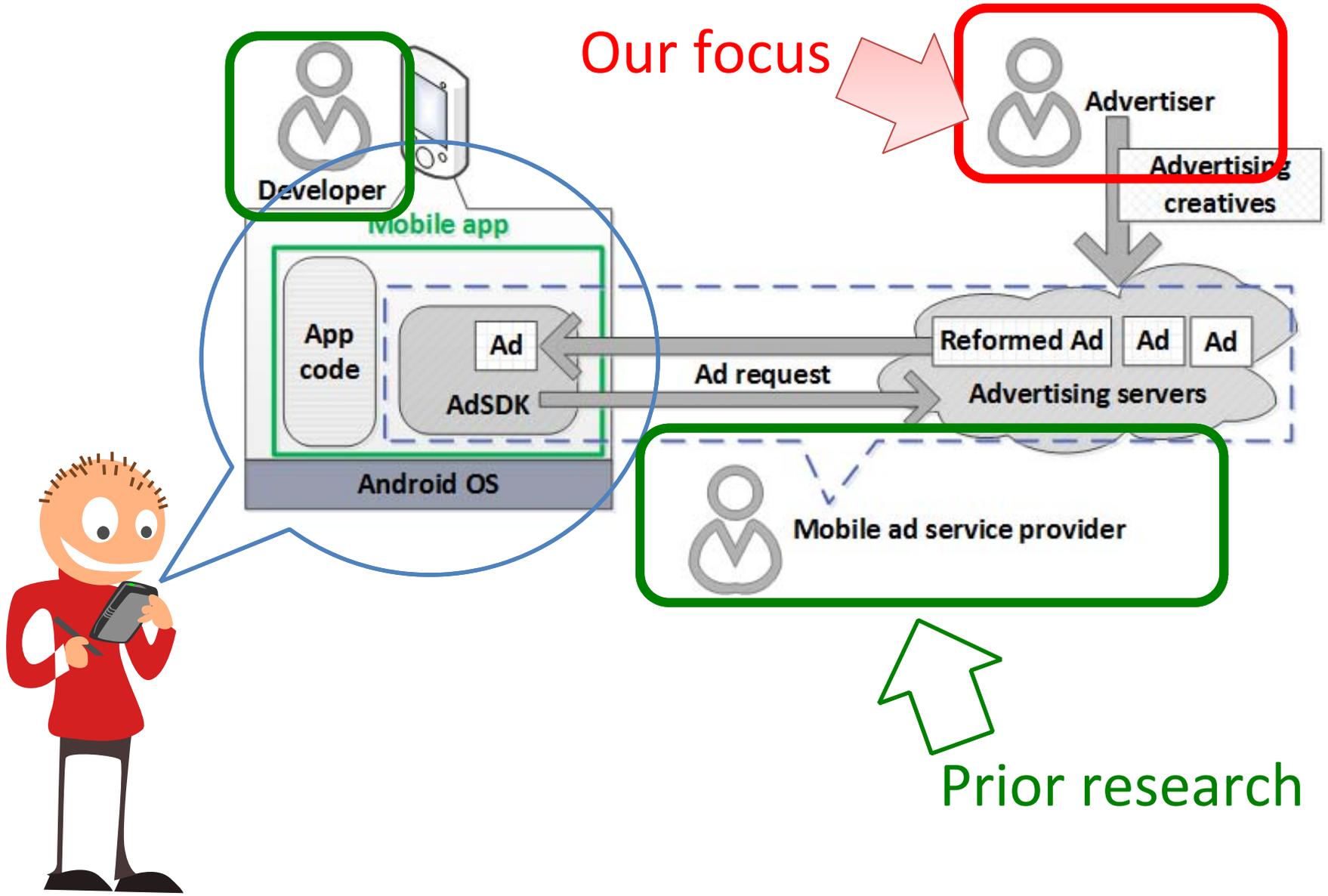
source: Shekhar et al. (USENIX Security 2012)

# Web



# Mobile





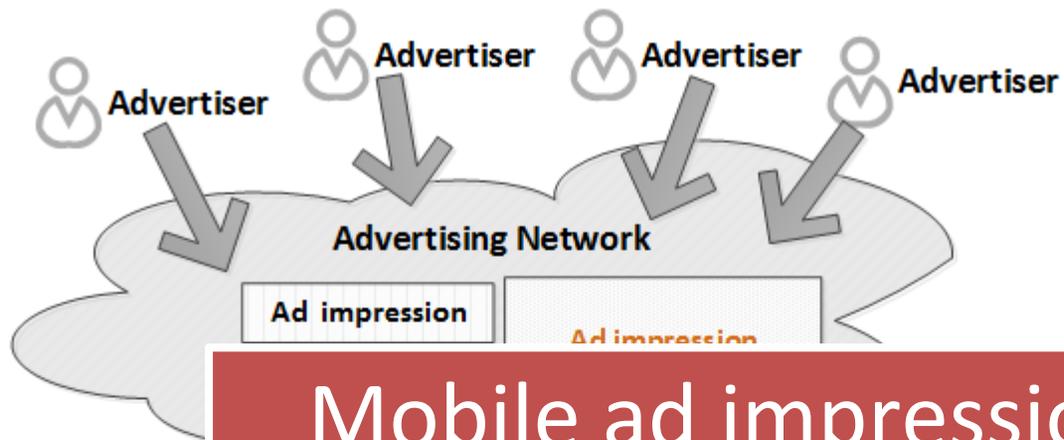
## Advertising services

- Large businesses
  - AdMob (Google),  
Mopub (Twitter),  
AirPush, many others
- Provide **AdSDK libraries** to 100,000s of developers
- Millions of \$ in revenue
- Reputation at stake

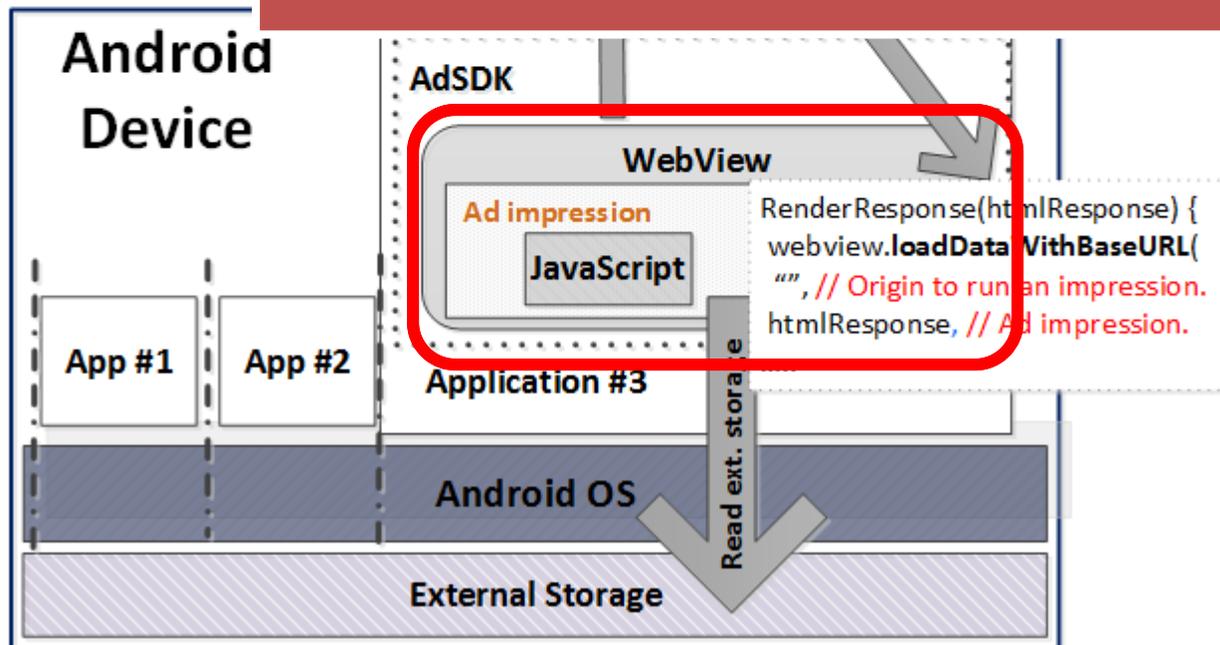
## Advertisers

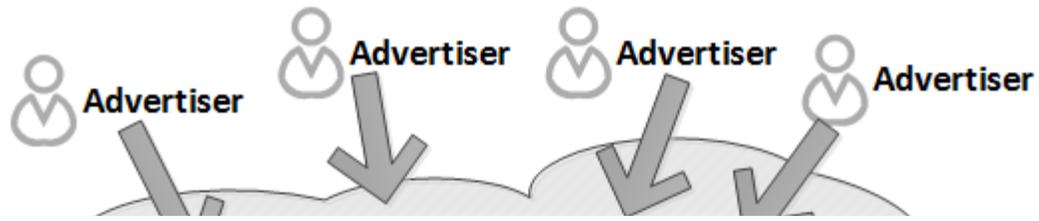
- Lots of fly-by-night operators
- Ads resold via auctions, brokers, exchanges
- No reputation at stake, no accountability
- Dynamic filtering and sanitization are hard

Ad libraries must protect users  
from malicious advertising

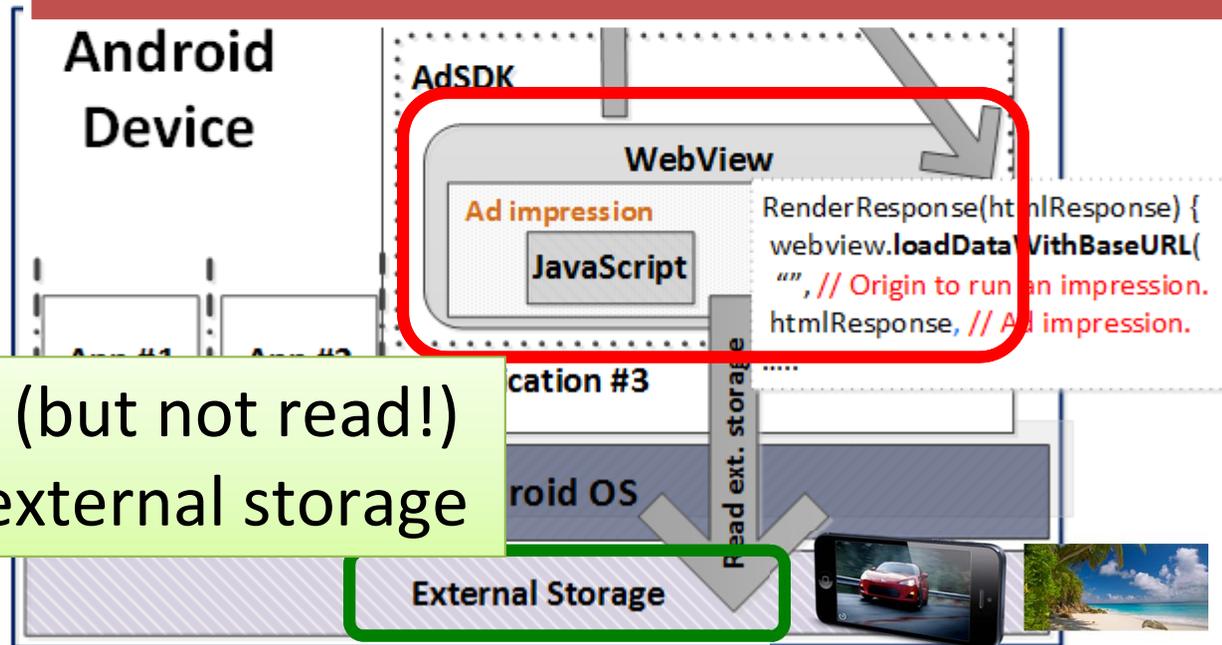


Mobile ad impressions are sandboxed inside WebView





Standard Web same origin policy:  
JavaScript in a mobile ad cannot read or write content from other origins



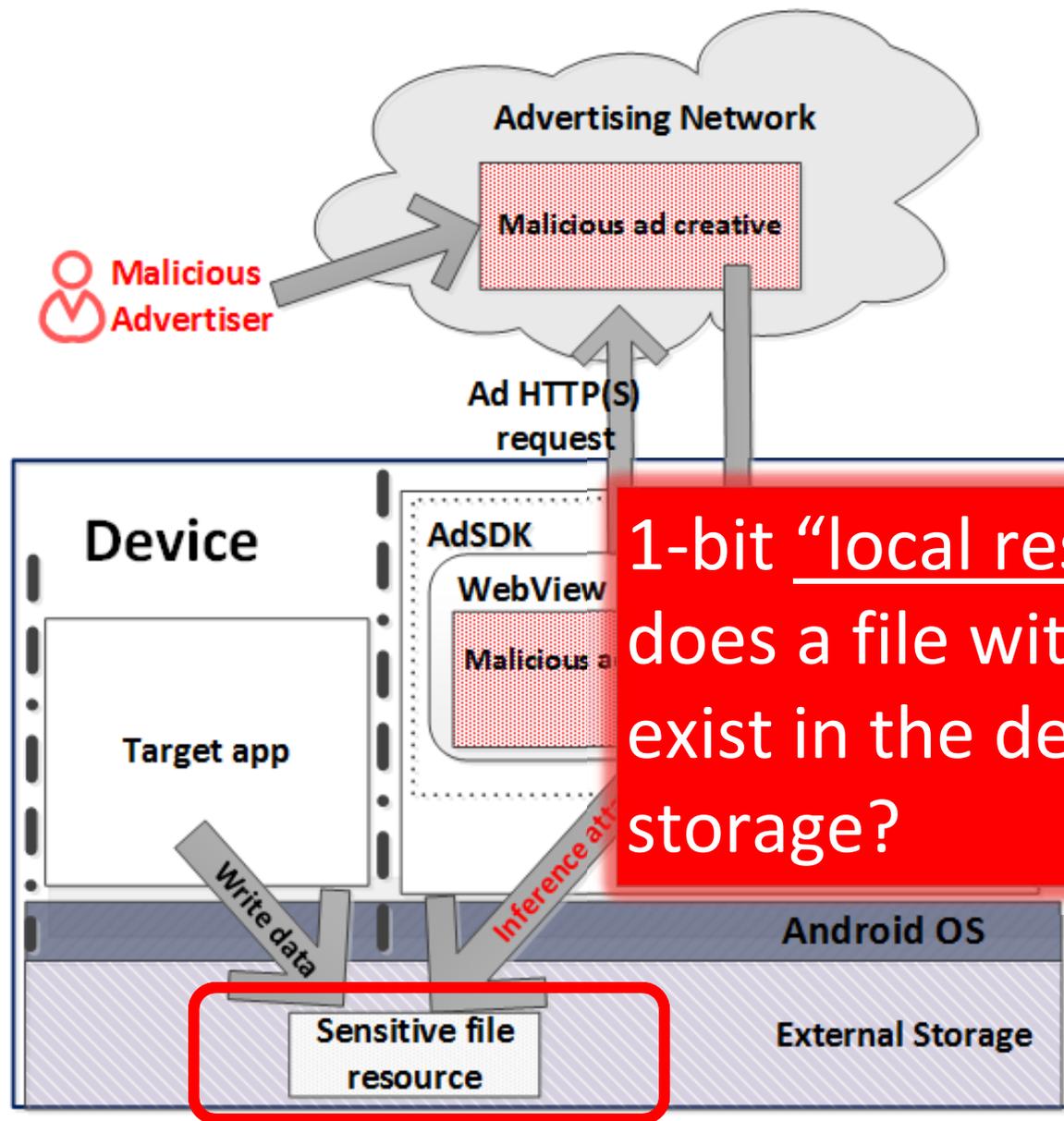
... can load (but not read!)  
files from external storage

# Android External Storage



- Can be read or written by any app with appropriate permissions
- Media-rich mobile ads require access to external storage to cache images, video
- Very weak access control for external storage
  - Any app can read any other app's files
  - But mobile ads are not apps. **Same origin policy = untrusted JavaScript cannot read ext-storage files ... but can attempt to load them**

**iab.**  
MRAID 2.0



1-bit “local resource oracle”:  
does a file with a given name  
exist in the device’s external  
storage?



App for finding pharmacies, compare drug prices  
(1 to 5 million installs in Google Play Store)

Bookmark functionality

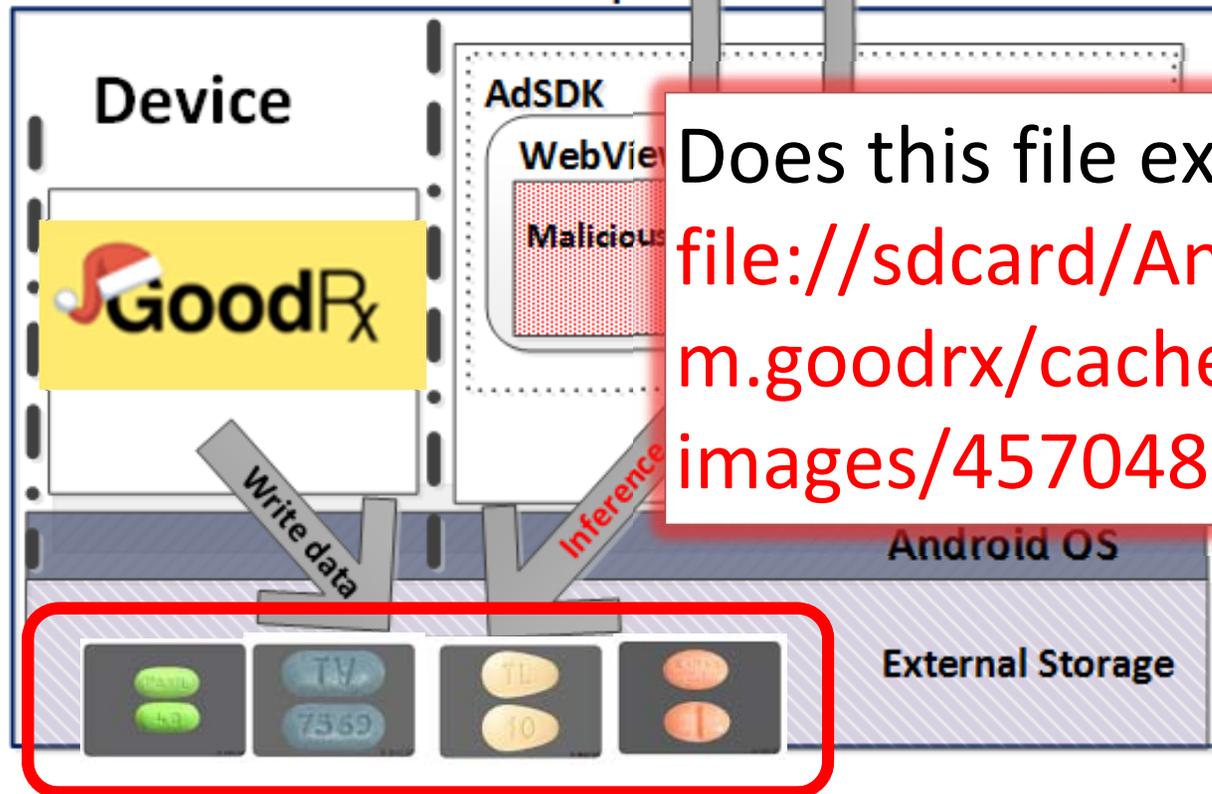
Thumbnail images of drugs  
that the user searched for  
cached in external storage

The screenshot shows the 'My Rx' section of the GoodRx app. It features a yellow header with a gear icon, the text 'My Rx', and a search icon. Below the header is a grey bar with a location pin icon and the text 'Pharmacies Near Current Location'. The main content is a list of four drug entries, each with a date 'Jan 29' on the left, a thumbnail image of the drug, the drug name, dosage, and price.

Date	Drug Thumbnail	Drug Name	Dosage	Price
Jan 29		<b>aripiprazole</b>	30 tablets 5mg	as low as \$270.00
		<b>Brintellix</b>	30 tablets 10mg	as low as \$297.31
		<b>Xanax</b>	30 tablets 0.5mg	as low as \$98.48
		<b>Paxil</b>	30 tablets 40mg	as low as \$179.80

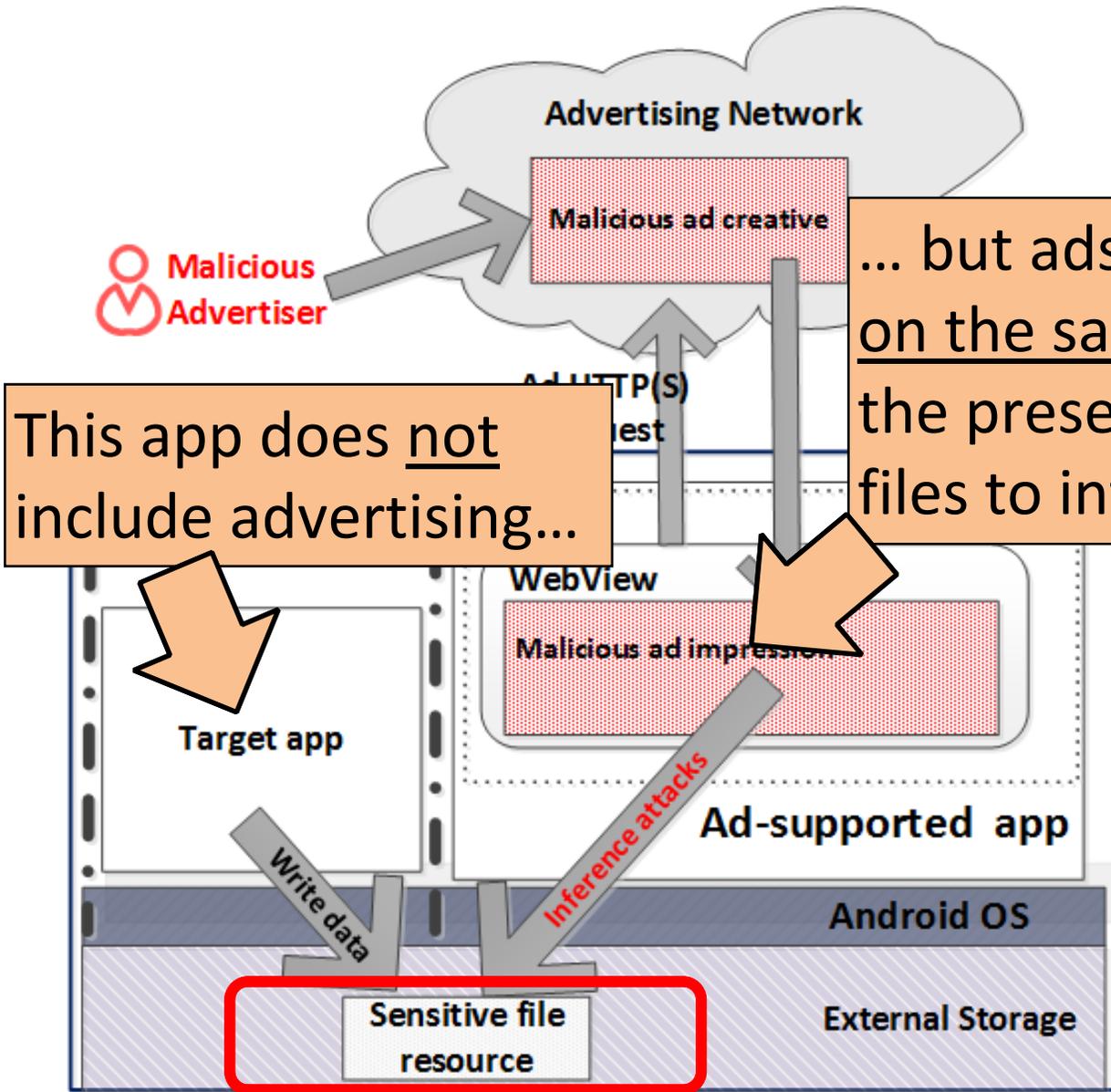
Advertising Network

Any ad displayed in any other app on the same device can infer which drugs the user is taking



Does this file exist?

file:///sdcard/Android/data/com.goodrx/cache/ui-images/45704837



This app does not include advertising...

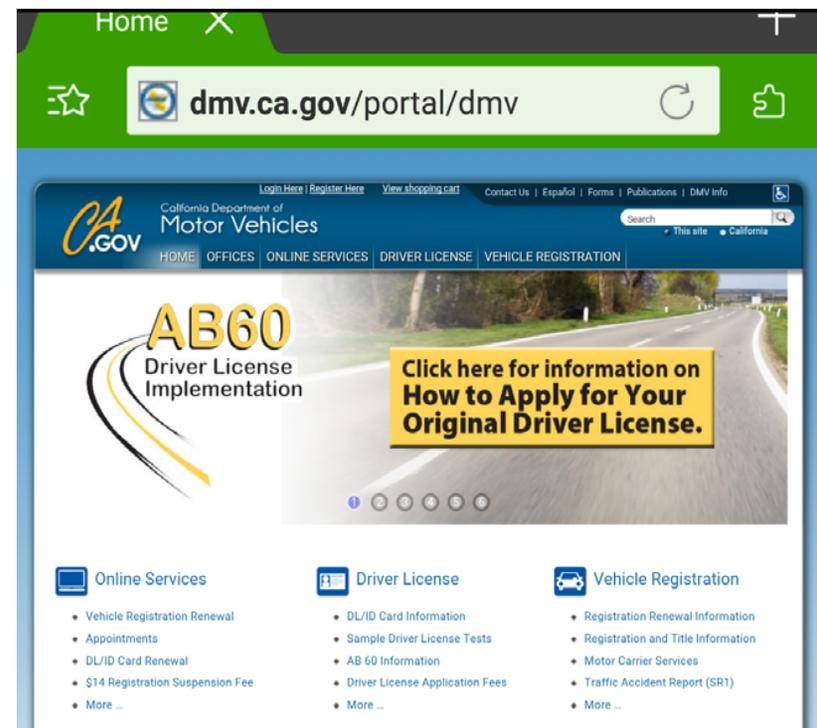
... but ads shown in any app on the same device can use the presence of its cached files to infer user's secrets

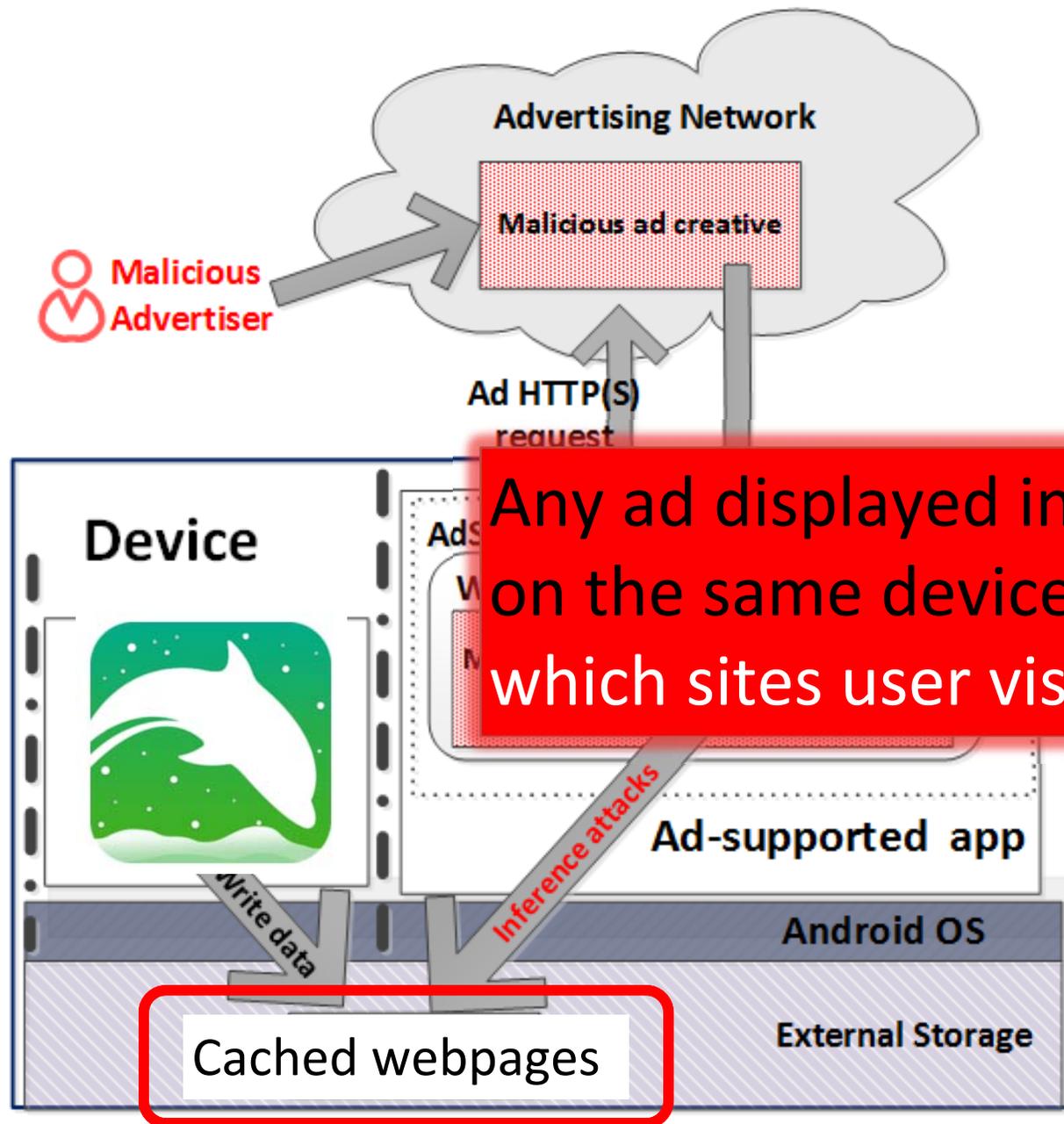
Does not violate same origin policy



## Dolphin mobile browser (50 to 100 million installs in Google Play Store)

To reduce bandwidth usage and response time, caches fetched images, HTML, and JavaScript in external storage





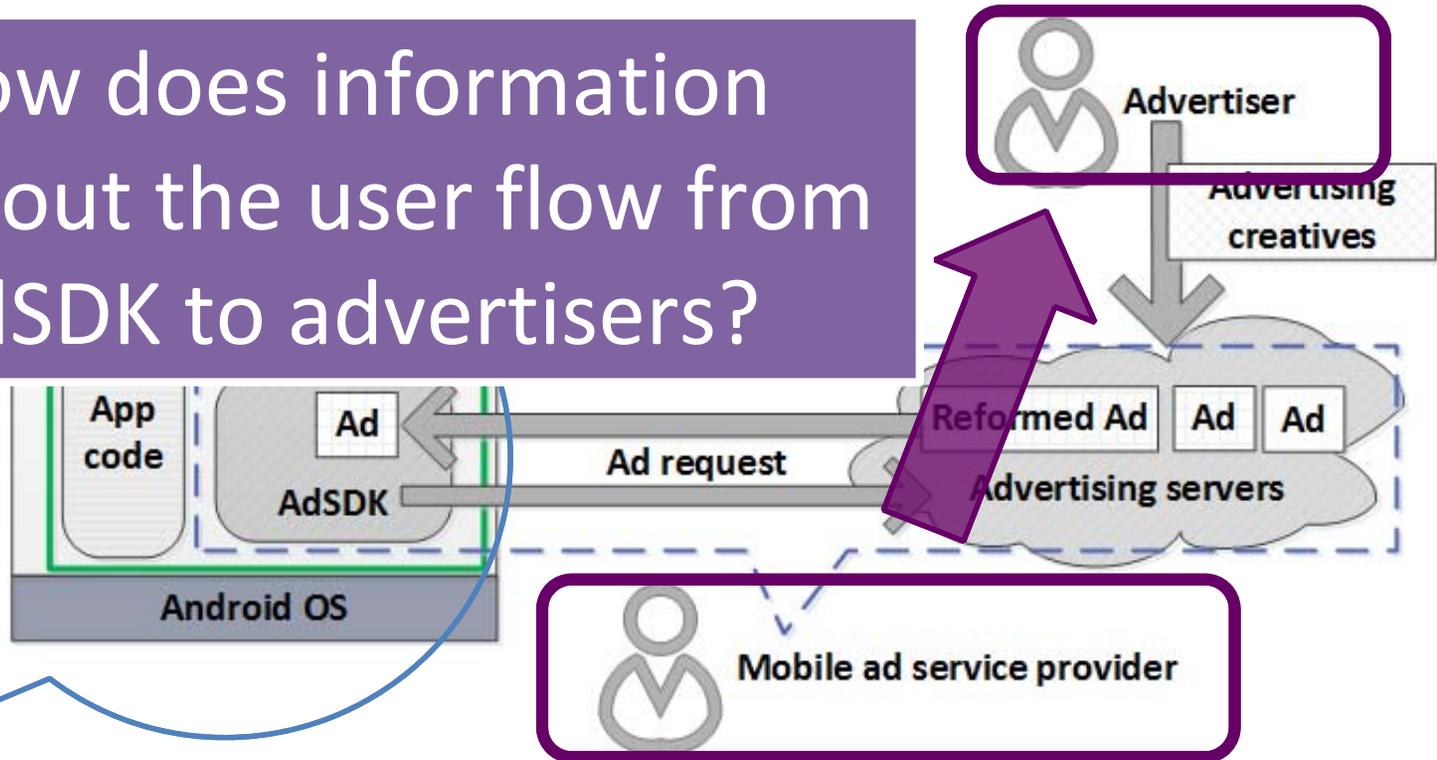
# Our Study

- Several major Android advertising libraries

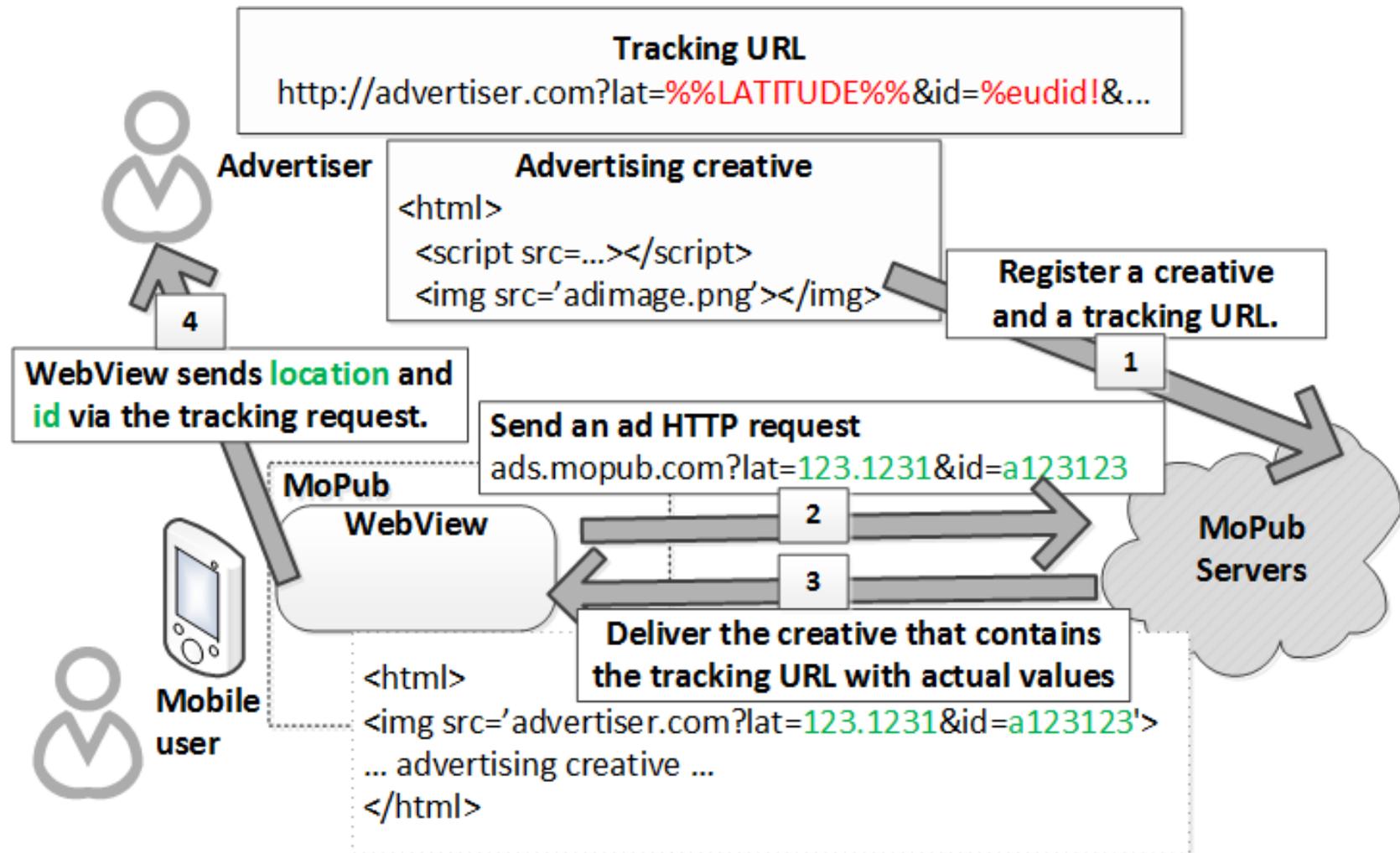


- “Local resource oracle” present in all of them
- All acknowledged the issue,  
several fixed in their latest AdSDK releases

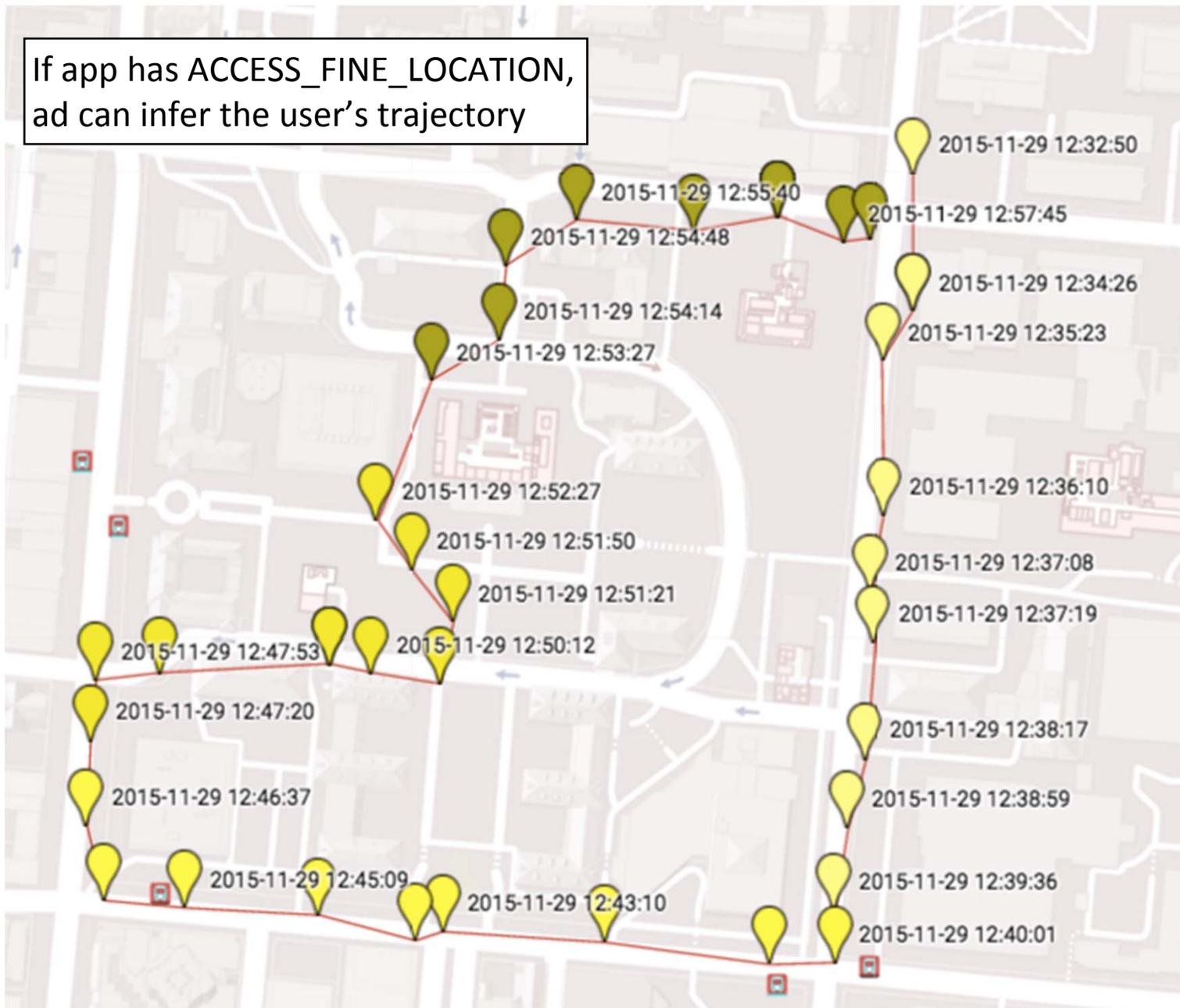
How does information about the user flow from AdSDK to advertisers?



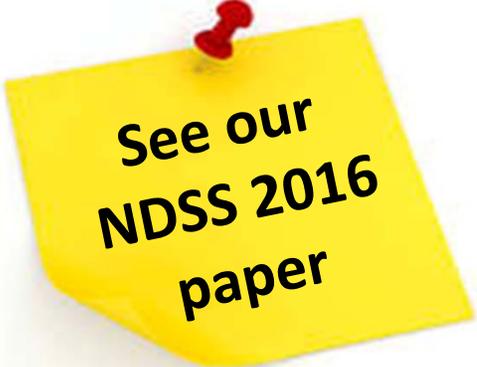
# Flow of User's Location in MoPub



If app has ACCESS\_FINE\_LOCATION,  
ad can infer the user's trajectory



# Our Results



See our  
NDSS 2016  
paper

- First study of how Android advertising services protect users from malicious advertising
- Standard Web same origin policy is no longer secure in the mobile context
  - Mere existence of a certain file in external storage can reveal sensitive information about the user
  - Other security and privacy issues
- Proposed a defense; direct impact on the design of the mobile advertising software stack

# Florian Schaub

Carnegie Mellon University

## *Towards Usable Privacy Policies: Semi-automatically Extracting Data Practices From Websites' Privacy Policies*

Co-authors: Norman Sadeh, Alessandro Acquisti, Travis D. Breaux, Lorrie Faith Cranor, Noah A. Smith, Fei Liu, Shomir Wilson, James T. Graves, Pedro Giovanni Leon, Rohan Ramanath, Ashwini Rao (Carnegie Mellon University); Aleecia M. McDonald (Stanford University); Joel Reidenberg, N. Cameron Russell (Fordham University)



# Towards Usable Privacy Policies

Semi-automatically Extracting  
Data Practices from Privacy Policies

**Florian Schaub**

Carnegie Mellon University

**Norman Sadeh** | Lead Principal Investigator

Carnegie Mellon University

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

**USABLE PRIVACY.ORG**  
the usable privacy policy project

**Carnegie  
Mellon  
University**

**CLIP** | Center on  
Law and  
Information  
Policy  
AT FORDHAM LAW SCHOOL

**CIS**  
The Center for  
Internet and Society



A NSF SaTC  
Frontier project  
(CNS-1330596)

**Norman Sadeh, Alessandro Acquisti, Travis Breaux,  
Lorrie Cranor, Noah Smith**

Jaspreet Bhatia, Aswarth Dara, Harishma Dayanidhi, James Graves,  
Bin Liu, Fei Liu, Alessandro Oltramari, Mads Schaarup Andersen,  
Florian Schaub, Shomir Wilson, Rohan Ramanath, Ashwini Rao,  
Kanthashree Sathyendra

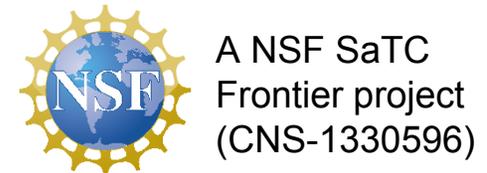


**Joel Reidenberg**

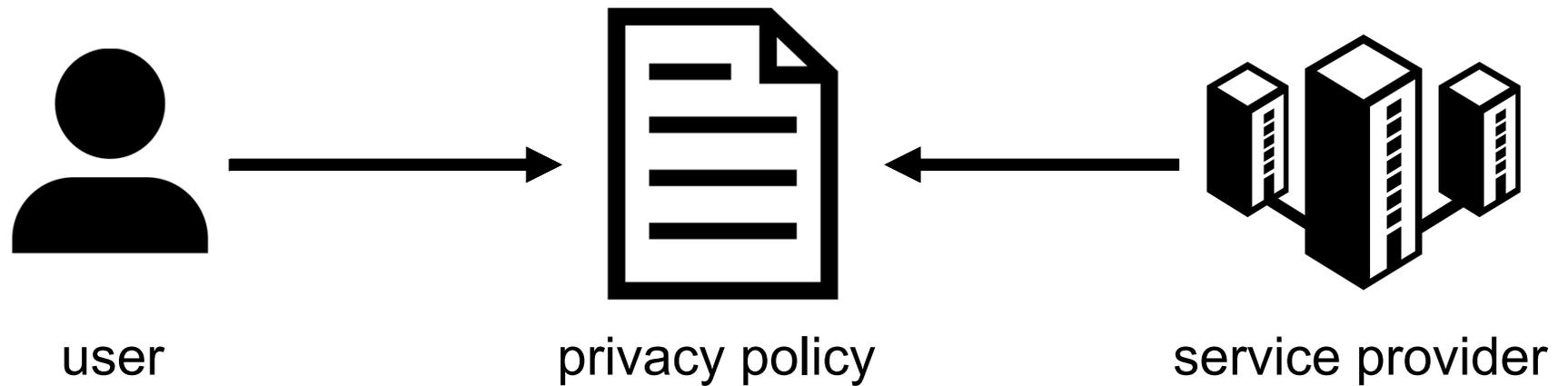
N. Cameron Russell, Thomas B. Norton, Antoine Bon, Samuel  
Borenzweig, Alexander Callen, Timothy Carter, Elle Davis, Amanda  
Grannis, Sophia Qasir, Stephanie Tallering

**Aleecia McDonald, Barbara van Schewick**

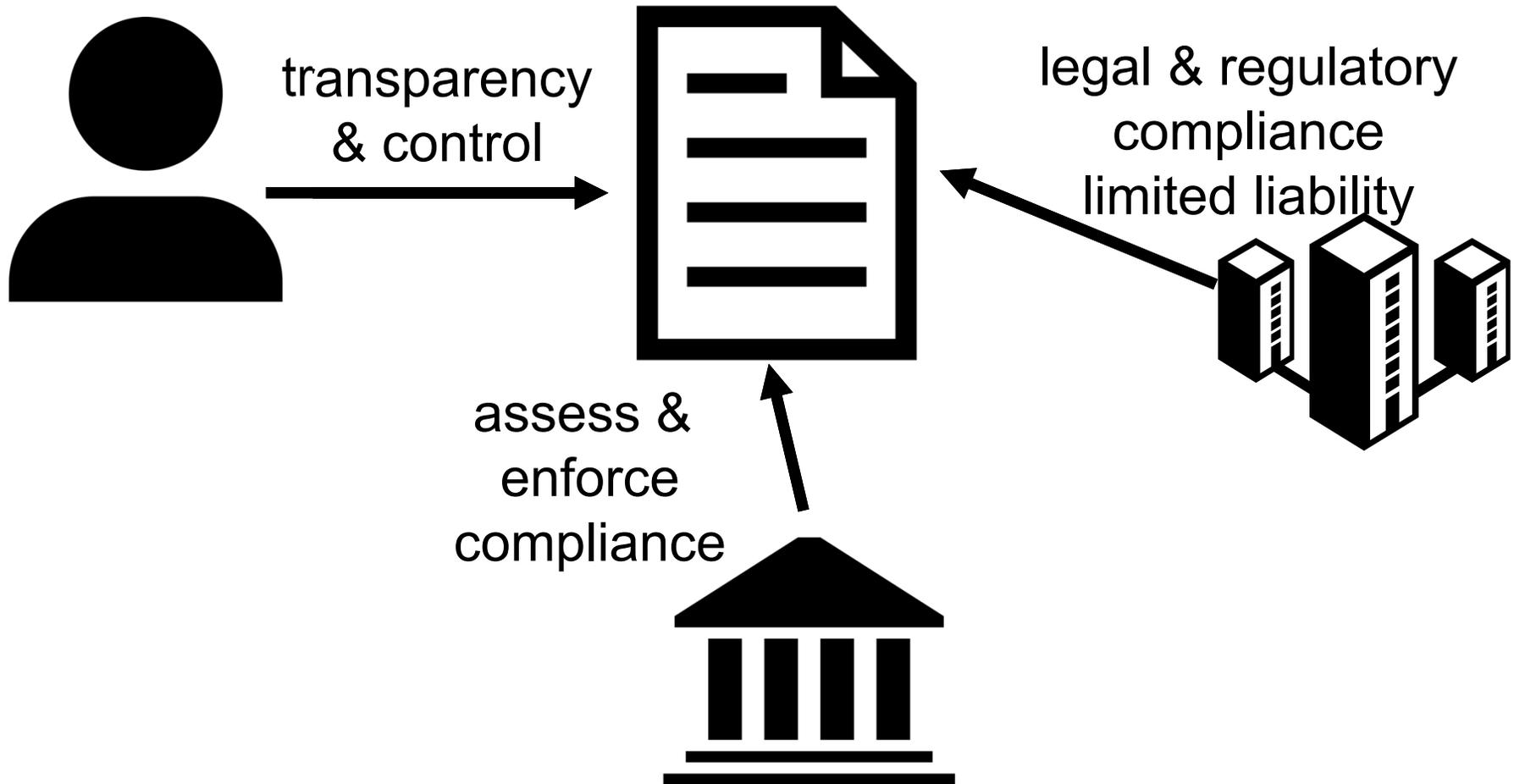
Pedro Giovanni Leon, Margaret Hagan



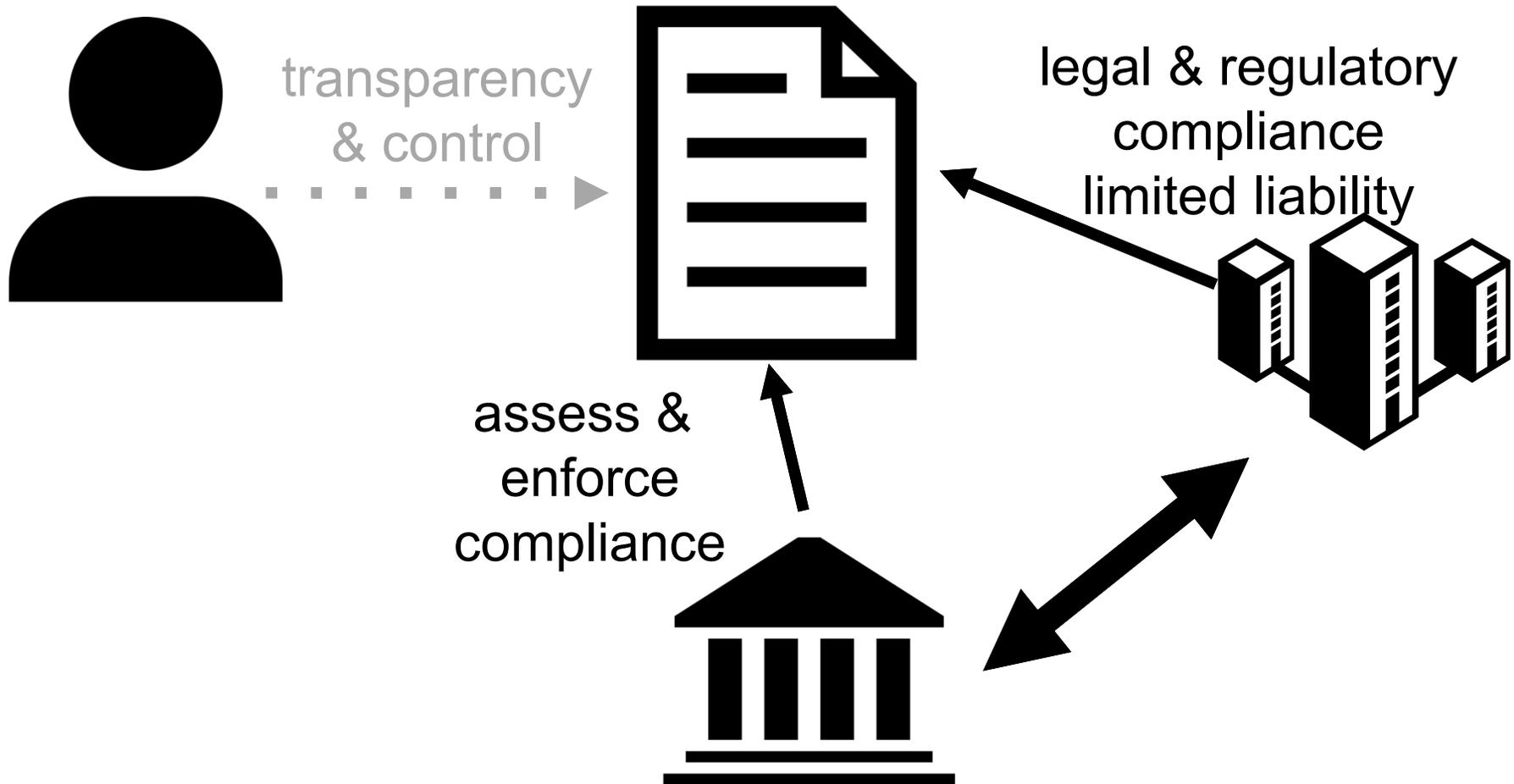
# Privacy notice & choice



# Privacy notice & choice

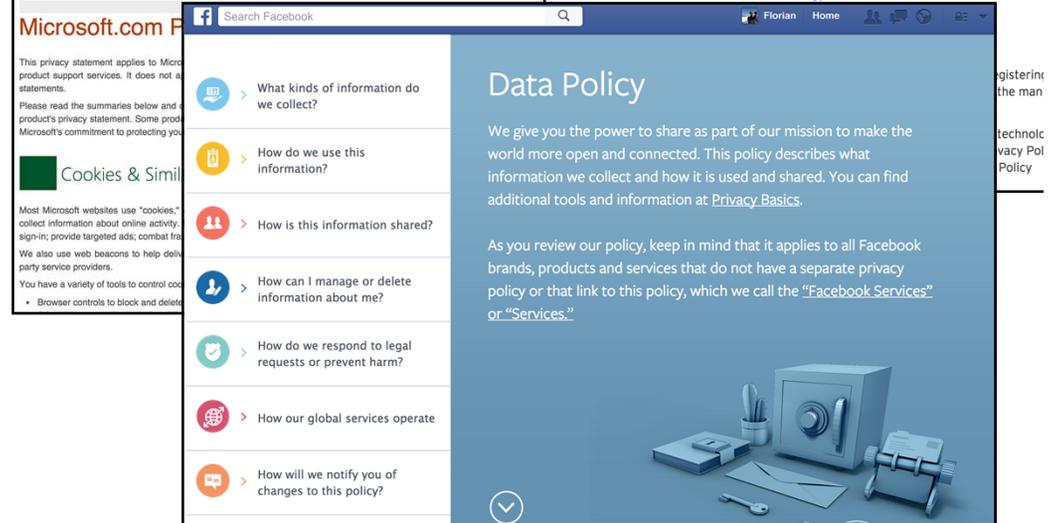
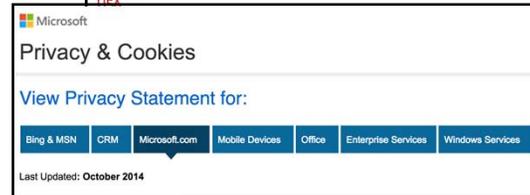


# Privacy notice & choice



# Privacy policies

- long & complex
- difficult to understand
- jargon & vagueness
- lack of choices

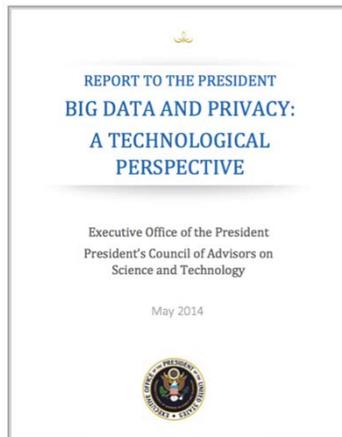
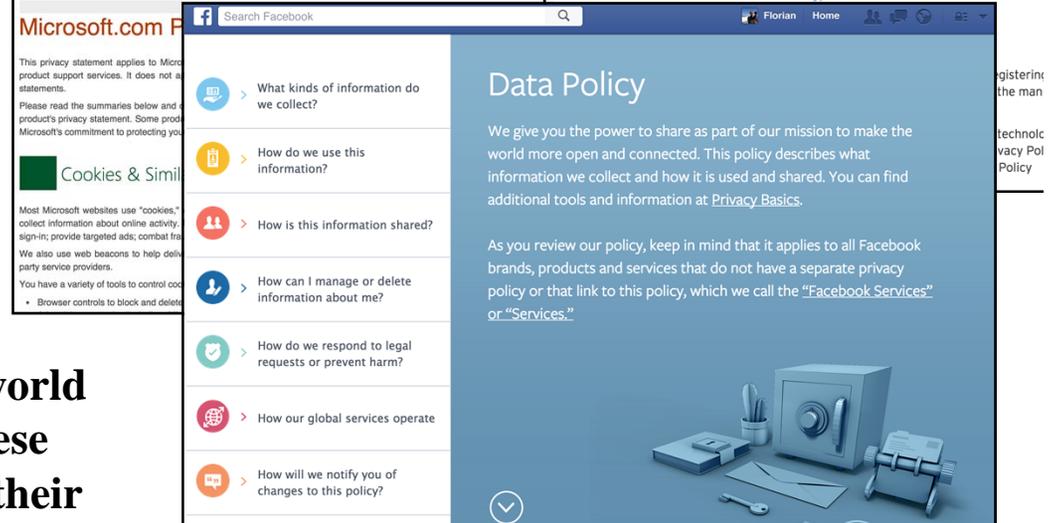
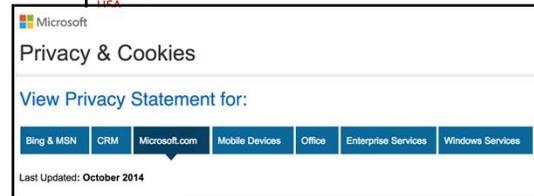


Schaub et al., *A Design Space for Effective Privacy Notices*. SOUPS'15: Symposium on Usable Privacy and Security, June 2015.

USABLE PRIVACY.ORG

# Privacy policies

- long & complex
- difficult to understand
- jargon & vagueness
- lack of choices

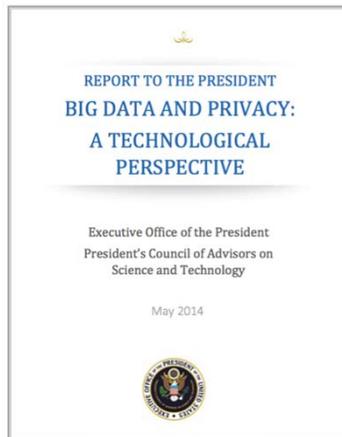
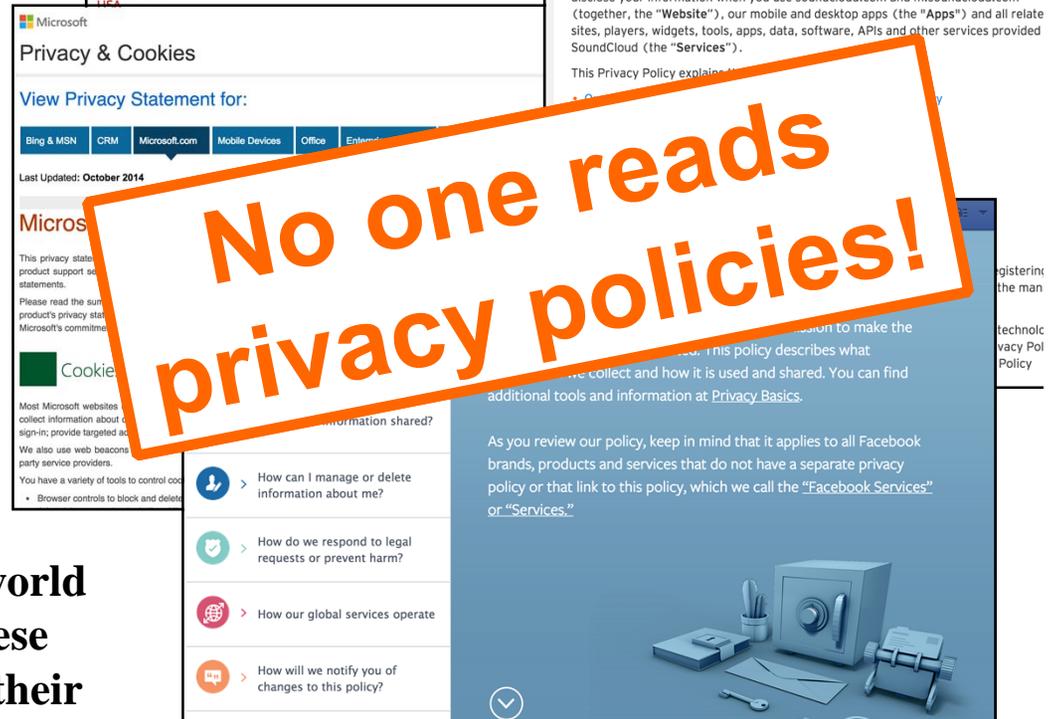


**“Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent”**

**USABLE PRIVACY.ORG**

# Privacy policies

- long & complex
- difficult to understand
- jargon & vagueness
- lack of choices

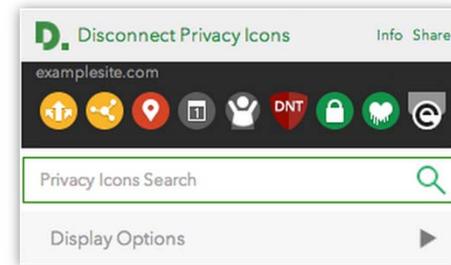


**“Only in some fantasy world do users actually read these notices and understand their implications before clicking to indicate their consent”**

**USABLE PRIVACY.ORG**

# Overcoming the status quo

- Layered privacy notices
- Privacy nutrition labels
- Privacy icons
- Machine-readable policies (e.g. P3P or Do Not Track)
- ...



Acme information we collect	ways we use your information					information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums	
contact information		opt out	opt out				
cookies							
demographic information		opt out	opt out				
financial information							
health information							
preferences		opt out	opt out				
purchasing information		opt out	opt out				
social security number & gov't ID							
your activity on this site		opt out	opt out				
your location							

Access to your information  
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site  
Please email our customer service department

some.com  
3000 Forbes Avenue  
Pittsburgh, PA 15213 United States  
Phone: 800-555-5555  
help@acme.com

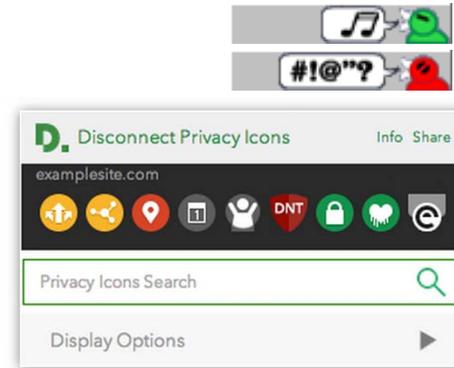
The Platform for Privacy Preferences 1.1 (P3P1.1) Specification  
W3C Working Group Note 13 November 2006

```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
  entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
  <DISPUTES service="http://www.PrivacySeal.org"
    resolution-type="independent"
    description="PrivacySeal, a third-party seal provider"
    image="http://www.PrivacySeal.org/Logo.gif"/>
  </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
  <CONSEQUENCE-GROUP>
  <CONSEQUENCE>a site with clothes you would appreciate</CONSEQUENCE>
  </CONSEQUENCE-GROUP>
  <RECIPIENT>ours/</RECIPIENT>
  <RETENTION>indefinitely/</RETENTION>
  <PURPOSE>custom/<develop/></PURPOSE>
  <DATA-GROUP>
  <DATA name="dynamic.cookies" category="state"/>
  <DATA name="dynamic.miscdata" category="preference"/>
  <DATA name="user.gender"/>
  <DATA name="user.home." optional="yes"/>
  </DATA-GROUP>
  </STATEMENT>
  <STATEMENT>
  <RECIPIENT>ours/</RECIPIENT>
  <PURPOSE>admin/<develop/></PURPOSE>
  <RETENTION>indefinitely/</RETENTION>
  <DATA-GROUP>
  <DATA name="dynamic.clickstream.server"/>
  <DATA name="dynamic.http.useragent"/>
  </DATA-GROUP>
  </STATEMENT>
</POLICY>
```

# Overcoming the status quo

- Layered privacy notices
- Privacy nutrition labels
- Privacy icons
- Machine-readable policies (e.g. P3P or Do Not Track)
- ...

**Lack of industry support & adoption incentives**



Acme information we collect	ways we use your information					information sharing	
	provide service and maintain site	marketing	telemarketing	profiling	other companies	public forums	
contact information		opt out	opt out				
cookies							
demographic information		opt out	opt out				
financial information							
health information							
preferences		opt out	opt out				
purchasing information		opt out	opt out				
social security number & gov't ID							
your activity on this site		opt out	opt out				
your location							

Access to your information  
This site gives you access to your contact data and some of its other data identified with you

How to resolve privacy-related disputes with this site  
Please email our customer service department

some.com  
3000 Forbes Avenue  
Pittsburgh, PA 15213 United States  
Phone: 800-555-5555  
help@acme.com

The Platform for Privacy Preferences 1.1 (P3P1.1) Specification  
W3C Working Group Note 13 November 2006

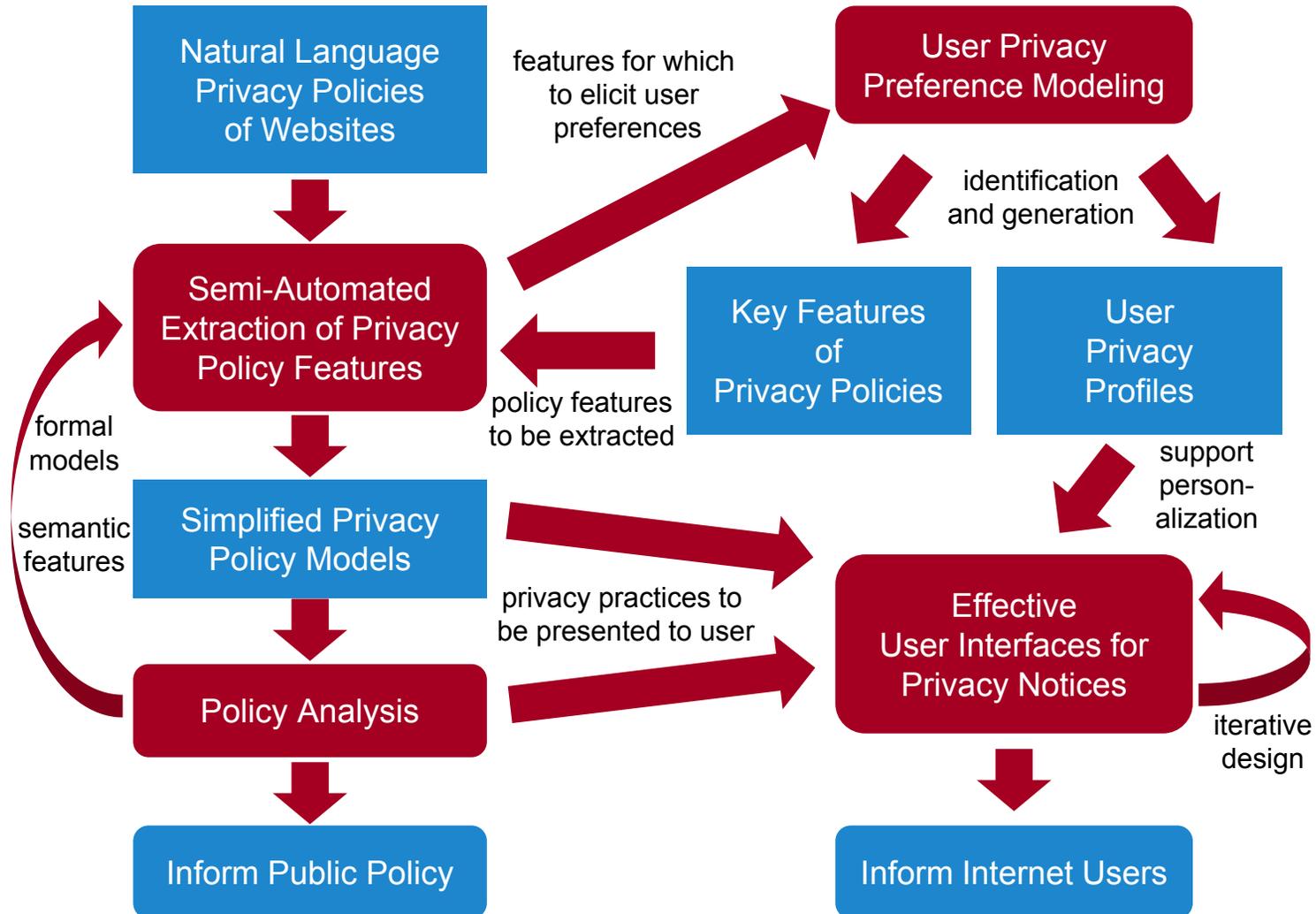
```
<POLICY xmlns="http://www.w3.org/2000/P3Pv1"
  entity="TheCoolCatalog, 123 Main Street, Seattle, WA 98103, USA">
  <DISPUTES-GROUP>
    <DISPUTES service="http://www.PrivacySeal.org"
      resolution-type="independent"
      description="PrivacySeal, a third-party seal provider"
      image="http://www.PrivacySeal.org/Logo.gif"/>
  </DISPUTES-GROUP>
  <DISCLOSURE discuri="http://www.CoolCatalog.com/Practices.html" access="none"/>
  <STATEMENT>
    <CONSEQUENCE-GROUP>
      <CONSEQUENCE>a site with clothes you would appreciate</CONSEQUENCE>
    </CONSEQUENCE-GROUP>
    <RECIPIENT>ours</RECIPIENT>
    <RETENTION>indefinitely</RETENTION>
    <PURPOSE><custom/><develop/></PURPOSE>
  </STATEMENT>
  <DATA-GROUP>
    <DATA name="dynamic.cookies" category="state"/>
    <DATA name="dynamic.miscdata" category="preference"/>
    <DATA name="user.gender"/>
    <DATA name="user.home." optional="yes"/>
  </DATA-GROUP>
  <STATEMENT>
    <RECIPIENT>ours</RECIPIENT>
    <PURPOSE>admin/><develop/></PURPOSE>
    <RETENTION>indefinitely</RETENTION>
  </STATEMENT>
  <DATA-GROUP>
    <DATA name="dynamic.clickstream.server"/>
    <DATA name="dynamic.http.useragent"/>
  </DATA-GROUP>
</POLICY>
```

USABLE PRIVACY.ORG

# Project objectives

- **Semi-automatically analyze natural language privacy policies to extract key data practices**
- Combine **crowdsourcing, machine learning natural language processing** to enable **large-scale analysis** of privacy policies
- **Model users' privacy preferences** to focus on those practices they care about
- **Develop effective user interfaces** that convey relevant and actionable information to users

# Tightly interconnected threads



Sadeh et al., *The Usable Privacy Policy Project: Combining Crowdsourcing, Machine Learning and Natural Language Processing to Semi-Automatically Answer Those Privacy Questions Users Care About*, CMU Tech Report, 2013.

USABLE PRIVACY.ORG

# Identifying data practices of interest

- **Legal analysis**
  - Analysis of privacy harms addressed through litigation
- **User modeling**
  - Studies on privacy preferences & concerns
- **Policy content analysis**
  - Analysis of how practices are described in privacy policies
  - Ambiguity and vagueness in privacy policies

Reidenberg et al., *Privacy Harms and the Effectiveness of the Notice and Choice Framework*. I/S Journal of Law & Policy for the Information Society. vol. 11, 2015.  
Wilson et al., *Crowdsourcing Annotations for Websites' Privacy Policies: Can It Really work?* WWW'16: Intl. Worldwide Web Conference, April 2016.

# Crowdsourcing policy annotations

The screenshot shows the usableprivacy website interface. At the top, there is a navigation bar with links for 'User Profile', 'Task', 'Settings', and 'Logout'. Below this is a search bar labeled 'Search this policy'. The main content area is divided into two columns. The left column displays the 'time.com' privacy policy table of contents, including sections like 'The Information We Collect', 'How We Use the Information', 'Privacy Options', and 'Your California Privacy Rights'. The right column is titled 'Answer the following questions' and contains a question: 'Does the policy state that the website might collect contact information about its users?'. Below the question are two buttons: 'Select sentence from policy and click' and 'Remove last selection'. A text box contains a snippet of the policy: 'Your personally identifiable information may be required to engage in these activities as well as to receive products and services that you may have requested.' Below this are four radio button options: 'No', 'Yes', 'Unclear', and 'Not applicable'. A 'Next' button is located at the bottom right of the question area. At the bottom of the interface, there is a 'Your Progress' bar and a 'Jump directly to question' dropdown menu.

Wilson et al., *Crowdsourcing Annotations for Websites' Privacy Policies: Can It Really work?* WWW'16: Intl. Worldwide Web Conference, April 2016.

USABLE PRIVACY.ORG

# Crowdsourcing policy annotations

## collection of contact information

**2x** **Yes:** The policy explicitly states that the website might collect contact information

**6x** **Unclear:** The policy does not explicitly state whether the website might collect contact information or not

### The Information We Collect

At some Turner Network sites, you can order products, enter contests, vote in polls or otherwise express an opinion, subscribe to one of our services such as our online newsletters, or participate in one of our online forums or communities. In the course of these various offerings, we often seek to collect from you various forms of personal information. Examples of the types of personally identifiable information that may be collected at these pages include: name, address, e-mail address, telephone number, fax number, credit card information, and information about your interests in and use of various products, programs, and services.

At some Turner Network sites, you may also be able to submit information about other people. For example, you might submit a person's name and e-mail address to send an electronic greeting

# How good are crowdworkers?

- **Studies to compare performance of**
  - privacy policy experts
  - grad students in law & public policy
  - MTurk crowdworkers
- **Annotation of 26 policies**
  - 26 policies annotated by crowdworkers & skilled annotators
  - 6 policies also annotated by experts



www.shutterstock.com · 209001508



Reidenberg et al., *Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding*. Berkeley Technology Law Journal, vol. 30, 1, pp.39-88, May 2015

Wilson et al., *Crowdsourcing Annotations for Websites' Privacy Policies: Can It Really work?* WWW'16: Intl. Worldwide Web Conference, April 2016.

**USABLE PRIVACY.ORG**

# How good are crowdworkers?

- **Results highlights**

- Even experts do not always agree
- Data collection relatively easy to identify
- Data sharing practices more difficult
- Finer nuances difficult to extract

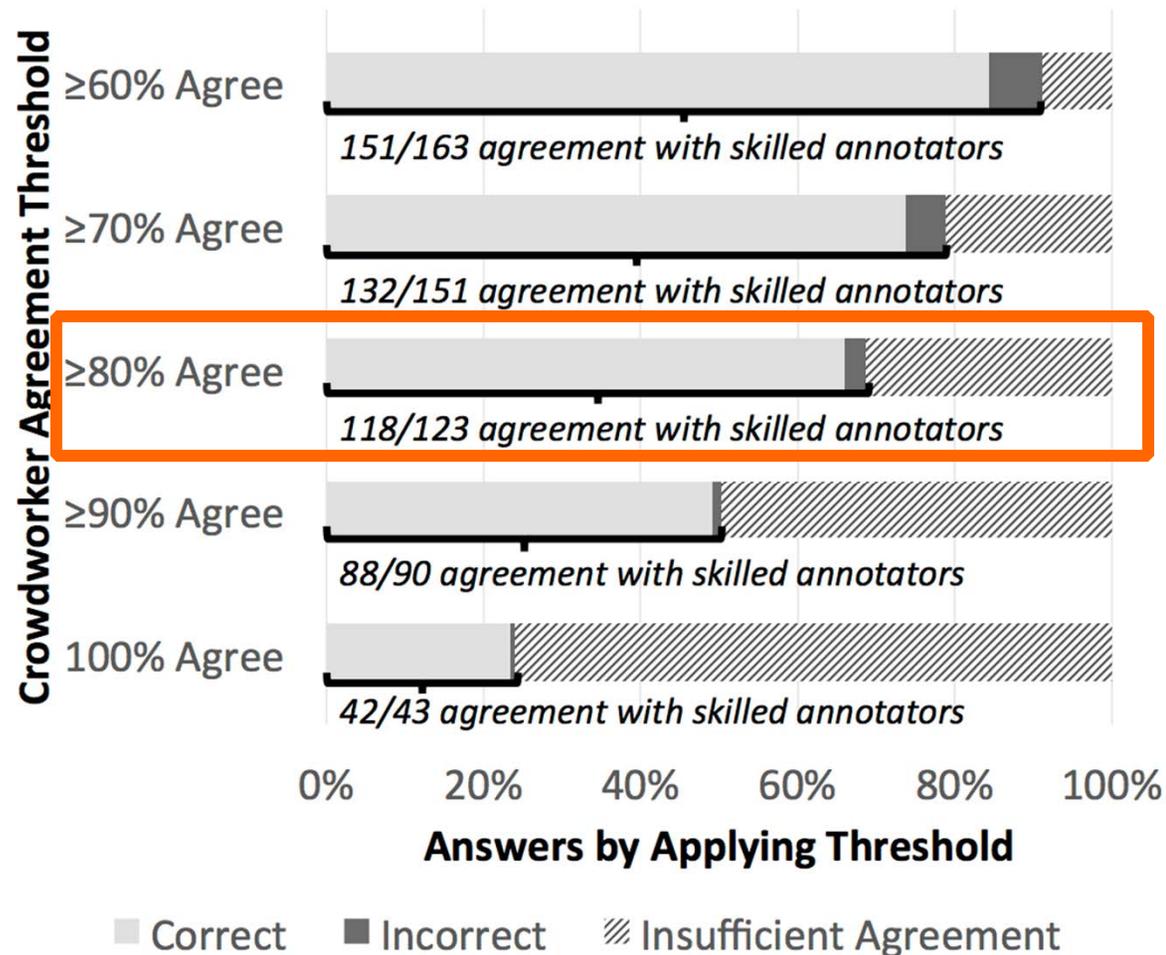


Reidenberg et al., *Disagreeable Privacy Policies: Mismatches between Meaning and Users' Understanding*. Berkeley Technology Law Journal, vol. 30, 1, pp.39-88, May 2015

**USABLE PRIVACY.ORG**

# Accuracy of crowdworker annotations

Compared to skilled annotators on 26 policies



# Enhancing extraction tasks with Machine Learning and NLP

- Accurate crowdsourcing of policy annotations is feasible
- But privacy policies are still long and complex
- Goal: Help crowdworkers **read selectively** (thus working more rapidly) without loss of accuracy

# Predicting & highlighting relevant paragraphs

Skip to highlighted paragraph: [Previous](#) [Next](#)

privacy practices specific to the website or online service.

This Privacy Statement describes the types of personal information we collect on the Site, how we may use that information and with whom we may share it. The Privacy Statement also describes the measures we take to protect the security of the personal information. We also tell you how you can reach us to ask us to update your preferences regarding how we communicate with you or answer any questions you may have about our privacy practices.

### Information We Collect

You may choose to provide us with personal information (such as name, contact details and payment information), such as:

Contact information, such as your name, address, telephone number, and email address, and your title or occupation.

Login and access credentials (such as username and password) for Lowe's accounts.

Payment information, such as your payment card number and expiration date.

Date of birth.

The geolocation of your device (such as if you opt to use the "Find Near Me" feature of the mobile-optimized portion of our websites or our Mobile Applications).

The unique ID number associated with certain Lowe's accounts.

## Answer the following questions

[Click here to view the instructions again](#)

**Question 2:**  
Does the policy state that the **website** might collect **financial information** about its users?

[Select sentence from policy and click](#) [Remove last selection](#)

Find the answer in the document, highlight the sentences containing the answer, and click the blue button above to paste the text here

**No** - the policy explicitly states that the **website** will not collect **financial information**.

**Yes** - the policy explicitly states that the website might collect financial information.

**Unclear** - the policy does not explicitly state whether the website might collect financial information or not, but the selected sentences could mean that financial information might be collected.

**Not applicable** - this question is not addressed by this policy.

[Previous](#) [Next](#)

11% Your Progress

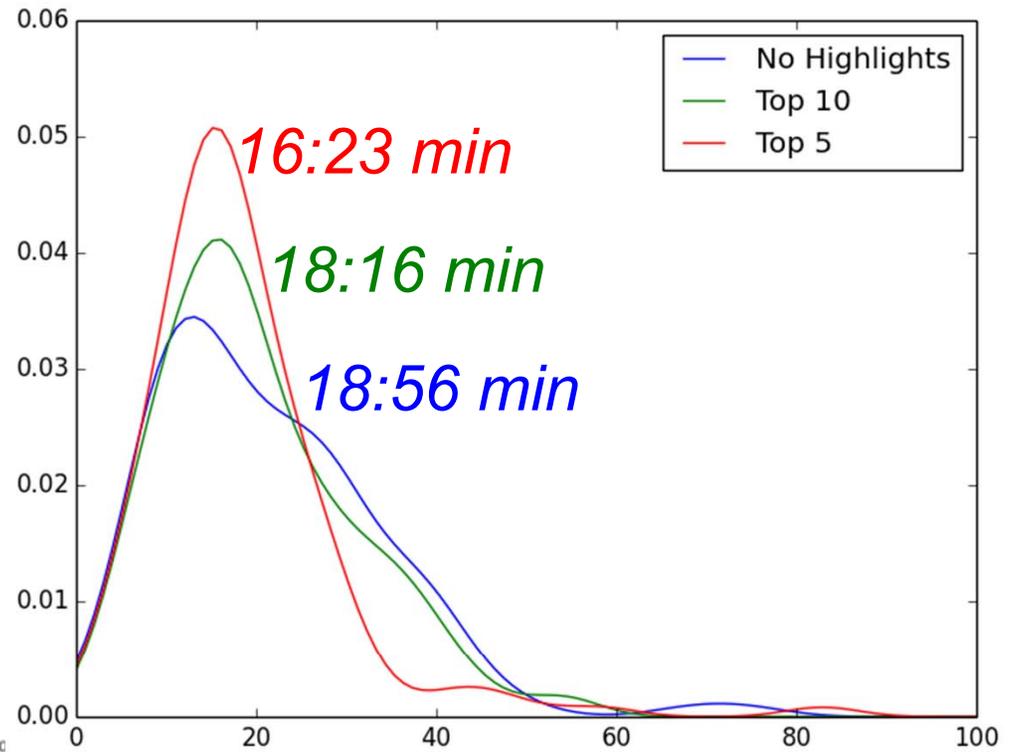
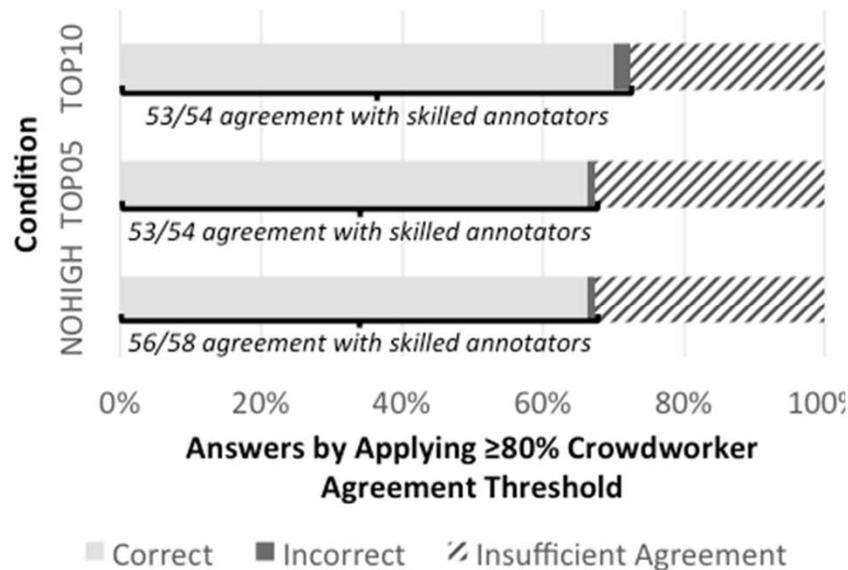
[Jump directly to question ▾](#)

Logistic regression based relevance models

Highlight X paragraphs most relevant for current question

# Predicting & highlighting relevant paragraphs

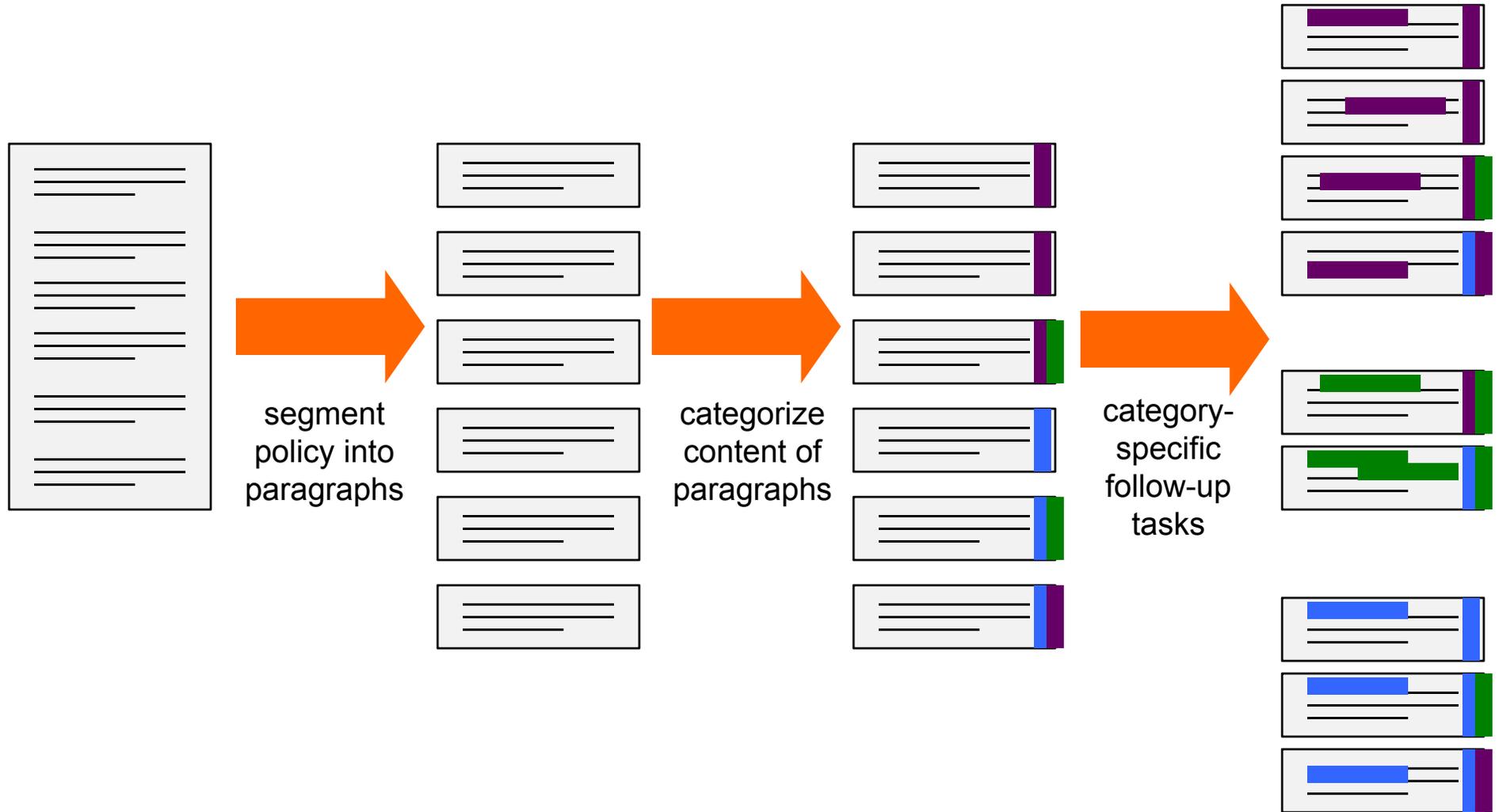
Crowdworkers can be induced to label privacy policies **faster without affecting accuracy.**



Wilson et al., *Crowdsourcing Annotations for Websites' Privacy Policies: Can It Really work?* WWW'16: Intl. Worldwide Web Conference, April 2016.

**USABLE PRIVACY.ORG**

# Multi-step annotation workflow



# Simplified but fine-grained tasks

[Click here to read the expanded instructions with an example.](#)

Response options for categorization

**Short Instructions:** Select the action verbs with your mouse cursor and then press one of the following keys to indicate when the verb describes an act to:

- Press 'c' for **collect** - any act by Zynga to collect information from another party, including the user
- Press 'u' for **use** - any act by Zynga or another party to use or modify information for a particular purpose
- Press 't' for **transfer** - any act by Zynga to transfer or share information with another party, including the user
- Press 'r' for **retain** - any act by Zynga to retain, store or delete information

Select relevant words and press button

In the following paragraph, any pronouns "We" or "Us" refer to the game company Zynga, and "you" refers to the Zynga user.

**Paragraph:**

We may **collect** or **receive** information from other sources including (i) other Zynga users who choose to **upload** their email contacts; and (ii) third party information providers.

Submit Query

Clear Last

Clear All

# Annotation dataset

The screenshot shows the usableprivacy.org interface. At the top, there's a navigation bar with 'usableprivacy', 'User Profile', 'Task', 'Visualize', 'Settings', and 'Logout'. Below this, the current policy is identified as 'www.imdb.com-privacypolicy-05-2014.csv'. A series of tabs allows navigation between different policy sections: 'First Party Collection/Use', 'Third Party Sharing/Collection', 'User Choice/Control', 'User Access, Edit and Deletion', 'Data Retention', 'Data Security', 'Policy Change', 'Do Not Track', 'International and Specific Audiences', and 'Other'. The 'First Party Collection/Use' tab is active, showing a paragraph of text with various annotations. To the right of the text is a legend for these annotations, including categories like 'Does/Does Not', 'Implicit/Explicit', 'Action First-Party', 'Identifiability', 'Personal Information Type', 'Purpose', 'User Type', 'Choice Type', 'Choice Scope', and 'References another place in the policy'. Each category has a corresponding dropdown menu. A 'Save' button is located at the bottom right of the annotation area. Below the text, there's a section titled 'Practices of this paragraph' which lists the categories used in the annotation and provides 'Clone' and 'Delete' buttons for each.

usableprivacy User Profile Task Visualize Settings Logout

Current Policy: www.imdb.com-privacypolicy-05-2014.csv

First Party Collection/Use Third Party Sharing/Collection User Choice/Control

User Access, Edit and Deletion Data Retention Data Security

Policy Change Do Not Track International and Specific Audiences Other

4/29

Previous Next

Information You Give Us: We receive and store any information you enter on our Web site or give us in any other way. Click here to see examples of what we collect. You can choose not to provide certain information, but then you might not be able to take advantage of many of our features. We use the information that you provide for such purposes as responding to your requests, customizing future browsing for you, improving our site, and communicating with you.

Please write your comments for this paragraph

### Practices of this paragraph

#### First Party Collection/Use

- Does Explicit Collect on website not-selected Generic personal information Basic service/feature not-selected Don't use service/feature not-selected [Clone](#) [Delete](#)

#### Third Party Sharing/Collection

#### User Choice/Control

#### User Access, Edit and Deletion

creating corpus of >100 privacy policies annotated by law students

gold standard data for ML/NLP research

# Annotation dataset

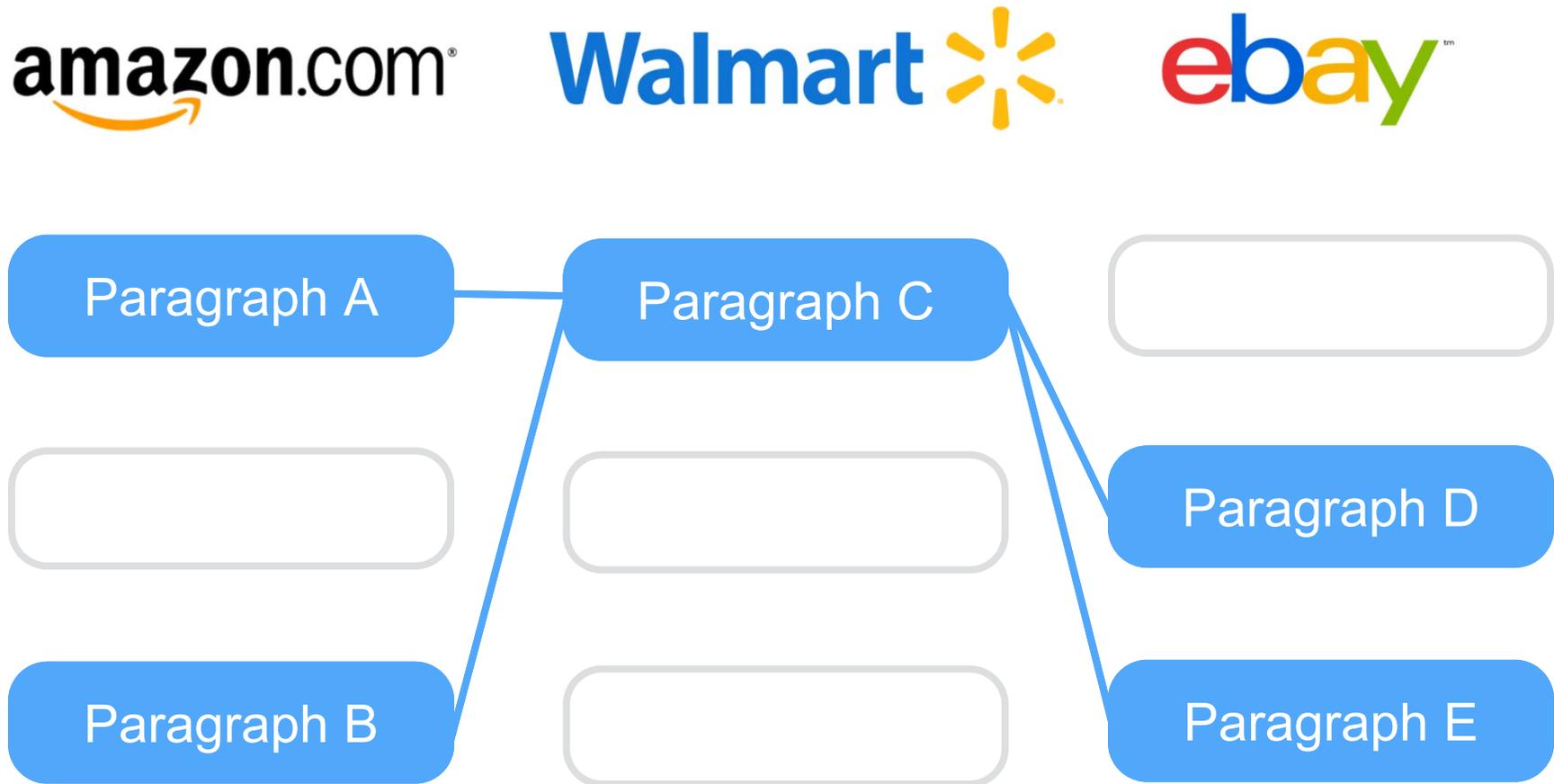
The screenshot shows the Google Privacy Policy page with an annotation interface. On the left, a 'Practices' sidebar lists categories with counts: First Party Collection/Use (50), Third Party Sharing/Collection (25), User Choice/Control (8), User Access, Edit and Deletion (5), Data Security (5), Data Retention (0), International and Specific Audiences (0), Do Not Track (0), Policy Change (6), and Other (20). The main content area is titled 'Privacy Policy' and includes an 'Annotator' section with counts 127, 131, and 132. The text of the policy is visible, including sections like 'Welcome to the Google Privacy Policy', 'Privacy Policy', and 'Information we collect'. A vertical bar on the right side of the page is filled with colored segments, representing the annotations made by different users.

creating corpus of >100 privacy policies annotated by law students

gold standard data for ML/NLP research

# Towards automated extraction

Paragraph sequence alignment



# Providing notice to users

- **Relevant information**
  - highlight practices users care about
  - emphasize unexpected practices
  - usable and intuitive interface
- **Actionable information**
  - show available privacy choices
  - help users find privacy-friendly alternatives
  - enable users to express dislike of practices
- Development of **Privacy Browser Plugin**
  - provide information independent of website

# Browser plugin design

- Display limited set of relevant practices
- User-centered iterative design
  - Focus groups
  - Online studies
  - Field studies
- Public release: Summer 2016

**amorenw.us's Privacy Practices**  
Based on the amorenw.us privacy policy from July 26, 2015.  
Last checked August 4, 2015.

6 Friendly  
4 Unfriendly

Our analysis of the amorenw.us privacy policy suggests the following privacy practices:

- ▶ How is my information collected and used? 2 FRIENDLY / 0 UNFRIENDLY PRACTICES
- ▶ How is my information shared? 1 FRIENDLY / 1 UNFRIENDLY PRACTICES
- ▶ How are my online activities tracked? 1 FRIENDLY / 1 UNFRIENDLY PRACTICES
- ▶ Can I access and delete my information? 1 FRIENDLY / 1 UNFRIENDLY PRACTICES
- ▶ How long is my information kept? 0 FRIENDLY / 1 UNFRIENDLY PRACTICES
- ▶ How can the privacy policy change? 1 FRIENDLY / 0 UNFRIENDLY PRACTICES

Privacy Practices for Similar Sites:

Site	Friendly	Unfriendly
LoveMatch	2	8
LoveNow	8	2
DateToday	6	4

Find more sites →

**Practices**  
From July 26, 2015.

6/10

Our analysis of the amorenw.us privacy policy suggests the following privacy practices:

Practice	Points
How is my information collected and used?	+2 Points
How is my information shared?	+1 Points
How are my online activities tracked?	+1 Points
Can I access and delete my information?	+1 Points
How long is my information kept?	+0 Points
How can the privacy policy change?	+1 Points

USABLE PRIVACY.ORG

# Conclusions

- **Semi-automatic analysis of privacy policies** with crowdsourcing, natural language processing and machine learning
- Enable **large-scale analysis** of privacy policies
- **Modeling users' privacy preferences** to identify unexpected and relevant practices
- **Development of effective user interfaces** that convey relevant and actionable information to users

**Florian Schaub**  
fschaub@cmu.edu

**Norman Sadeh**  
Lead PI | sadeh@cmu.edu

**USABLE PRIVACY.ORG**

# Norman Sadeh

Carnegie Mellon University

## *To Deny, or Not to Deny: A Personalized Privacy Assistant for Mobile App Permissions*

Co-authors: Bin Liu, Mads Schaarup Andersen, Florian Schaub, Hazim Almuhiemedi, Yuvraj Agarwal, Alessandro Acquisti (Carnegie Mellon University)





# ***Personalized Privacy Assistants***

*From Android Apps to the Internet of Things*

**Norman Sadeh**

Professor, School of Computer Science

Co-Director, MSIT Program in Privacy Engineering

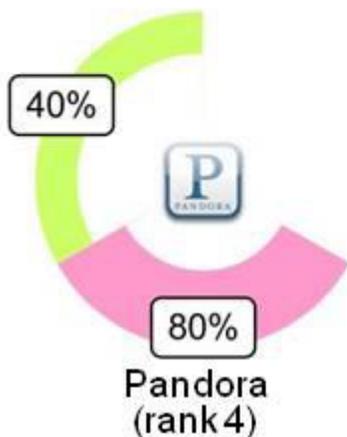
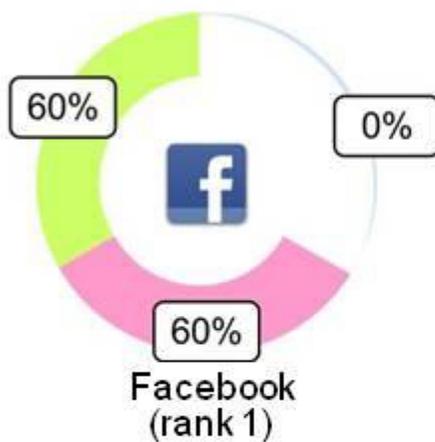
Carnegie Mellon University

[www.normsadeh.org](http://www.normsadeh.org) --- [sadeh AT cs.cmu.edu](mailto:sadeh AT cs.cmu.edu)



# People Care About Privacy...

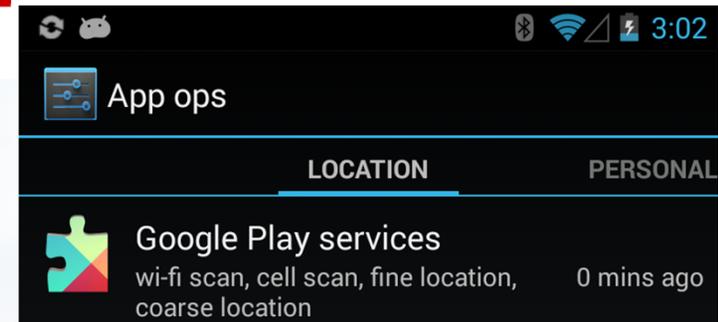
Percentages of people surprised by an App's Permission Requests



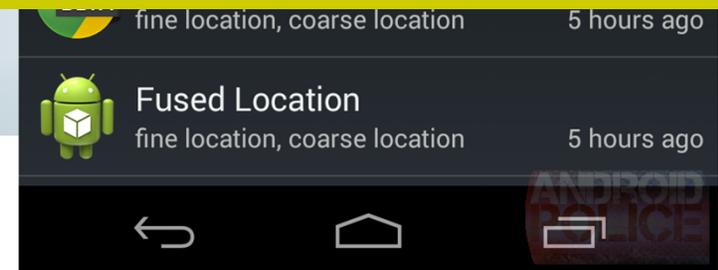
J. Lin, S. Amini, J. Hong, N. Sadeh, J. Lindqvist, J. Zhang, "Expectation and Purpose: Understanding Users' Mental Models of Mobile App Privacy through Crowdsourcing", Proc. of the 14th ACM International Conference on Ubiquitous Computing, Pittsburgh, USA, Sept. 2012

## ...But They Are Feeling Helpless...

- *Privacy policies are too long and too complex*



If this has failed on the fixed Web, what are the chances it will work on smartphones or in IoT?

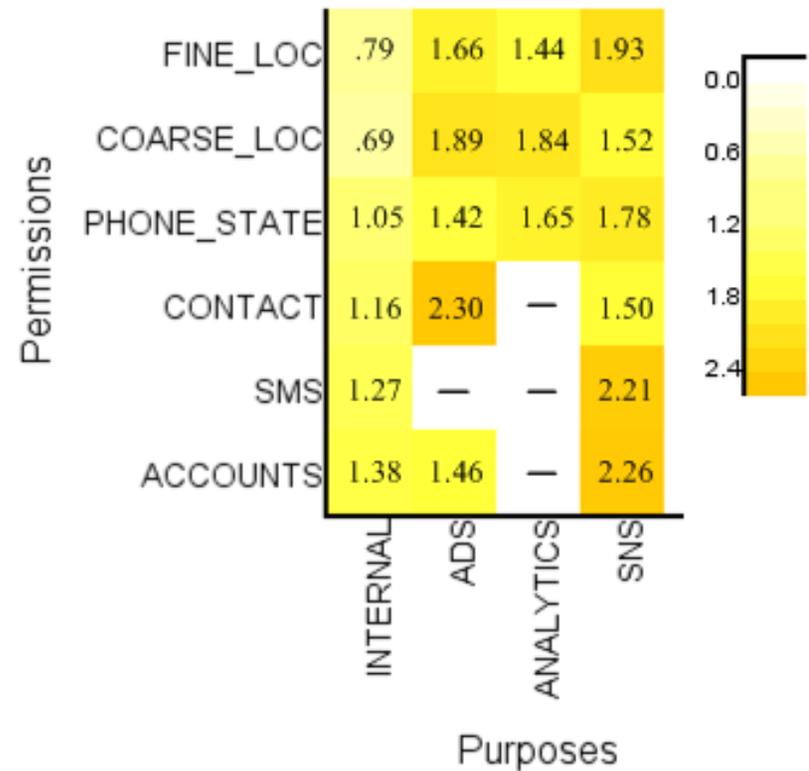
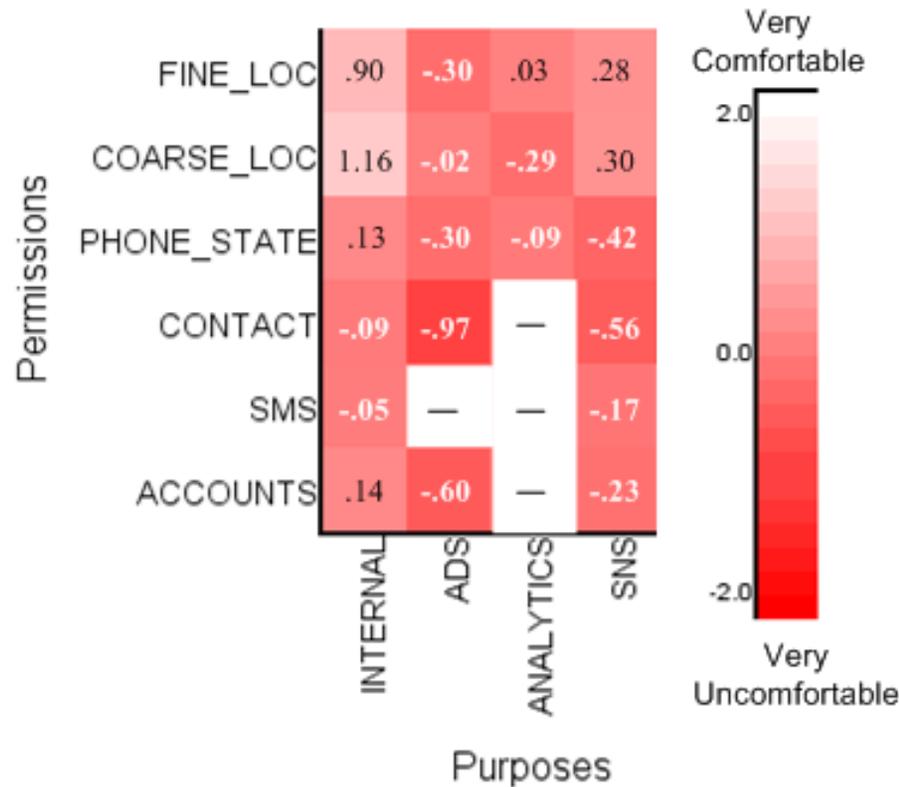


# Personalized Privacy Assistants

---

- ❑ **Selectively inform** us about privacy practices we may **not be expecting, yet care about**
- ❑ **Learn** many of our privacy preferences and **semi-automatically configure** many settings on our behalf
- ❑ **Motivate us** to occasionally revisit some of our preferences and decisions
- ❑ The assistants should ideally work across any number of environment and be **minimally disruptive**

# One Size-Fits-All Defaults Doesn't Work



## Users' Average Preferences

White → comfortable

Red → uncomfortable

## Variance among Users

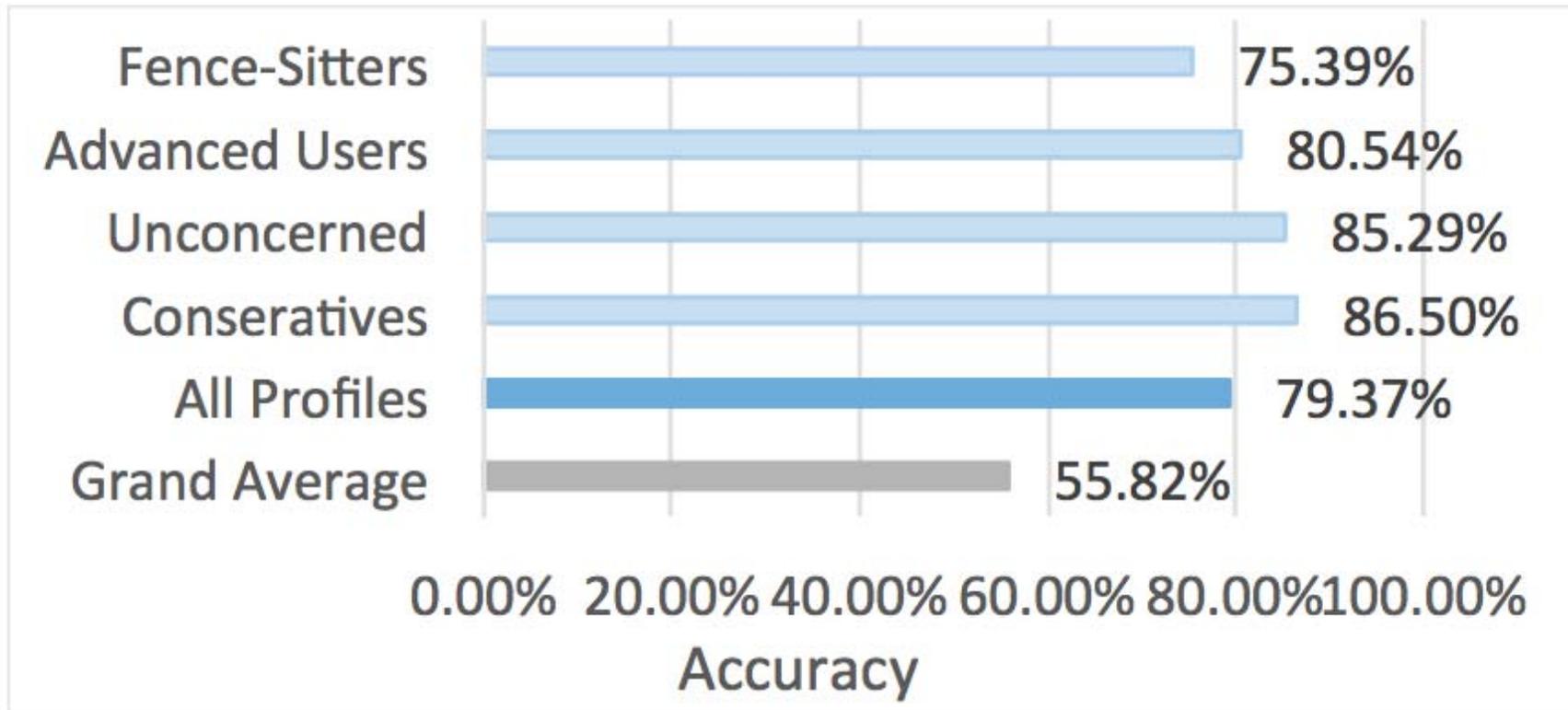
Darker yellow → larger variance

**Data based on 725 users and 837 apps (>21,000 HITs)**

# Mobile App Privacy Preferences

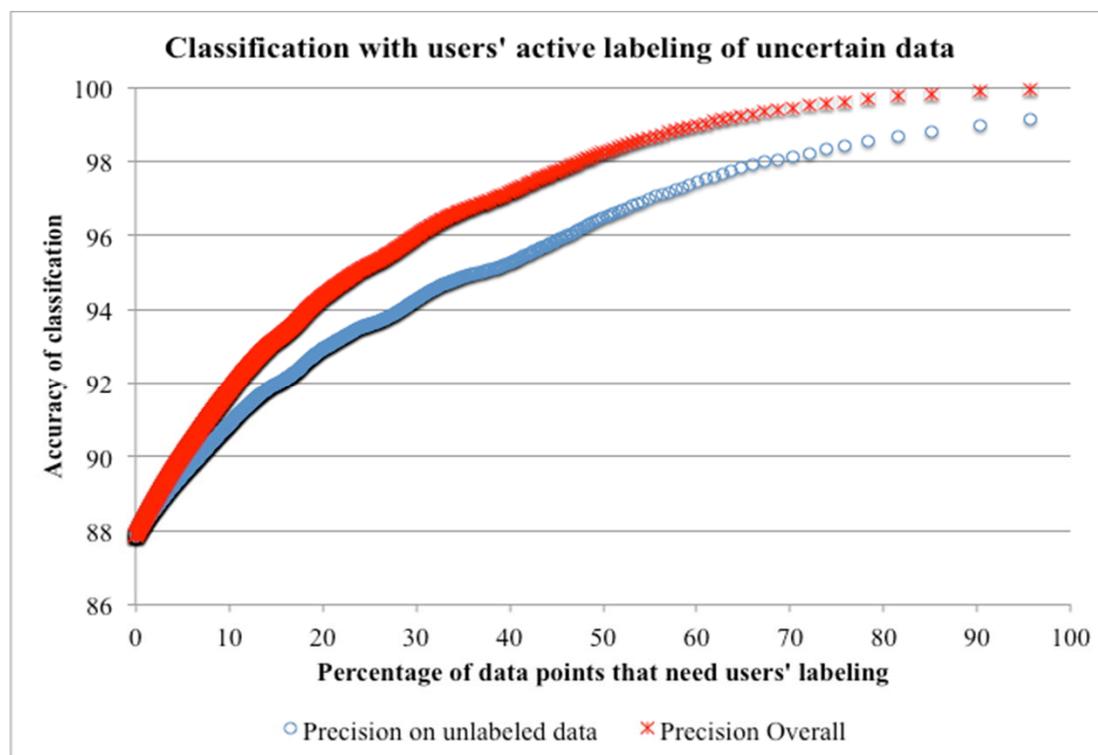
---

**A small number of privacy profiles can go a long way**



“Grand Average”: Results obtained with “one-size-fits-all” profile

# Pure Prediction vs. Interactive Model



## Learning personalized privacy preference models

If users can label an additional 10% of their permission decisions, the **prediction accuracy will climb from 87.8% to 91.8%...and that's only 6 questions...**

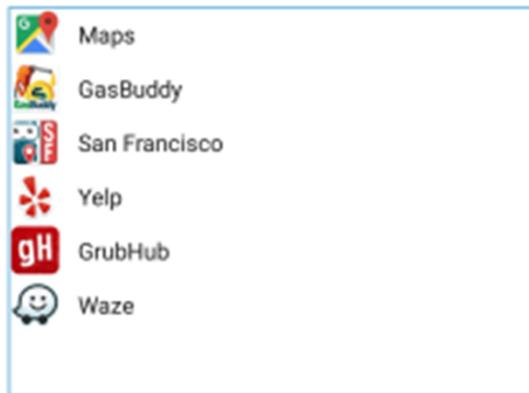
**At 20% (about 12 questions), accuracy climbs to 94%!**

**Data from about 240,000 LBE users, 12,000 apps, 14.5M records**

B. Liu, J. Lin, N. Sadeh, "Reconciling Mobile App Privacy and Usability on Smartphones: Could User Privacy Profiles Help?", WWW 2014. [http://www.normsadeh.com/file\\_download/168](http://www.normsadeh.com/file_download/168)

# Personalized Privacy Assistant for Android Permissions

These **TRAVEL & LOCAL** apps accessed your **LOCATION** **102 TIMES** over the past 2 days:



In general, are you OK with **TRAVEL & LOCAL** apps accessing your **LOCATION**?

YES

NO

Thank you! Based on your answers, we recommend restricting the following 11 app(s):

Click category to view/change recommendations



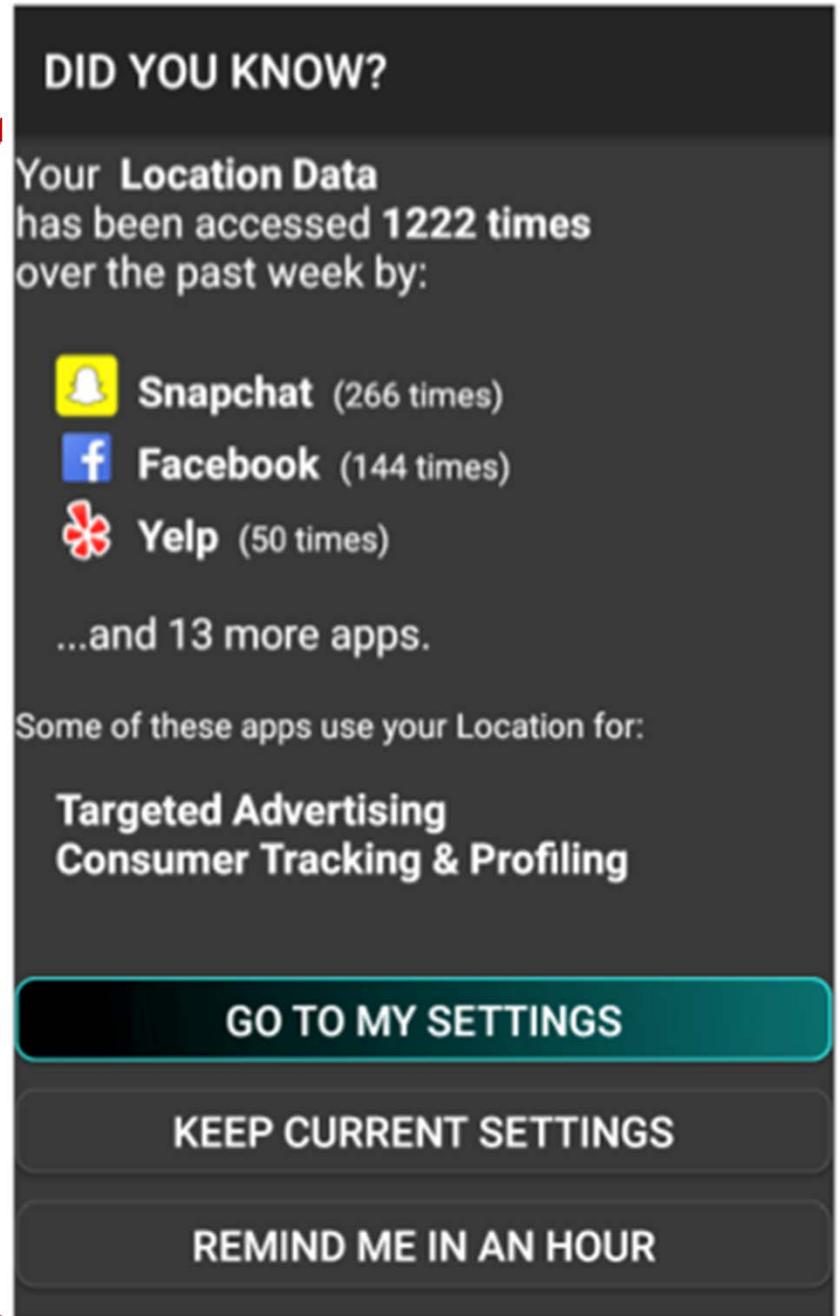
Do you want to make these changes?

YES, DENY THE 8 APP(S) SELECTED

NO, DO NOT MAKE ANY CHANGES

# Nudging Users for 6 days

Are users just being nice or is this truly reflecting their preferences?



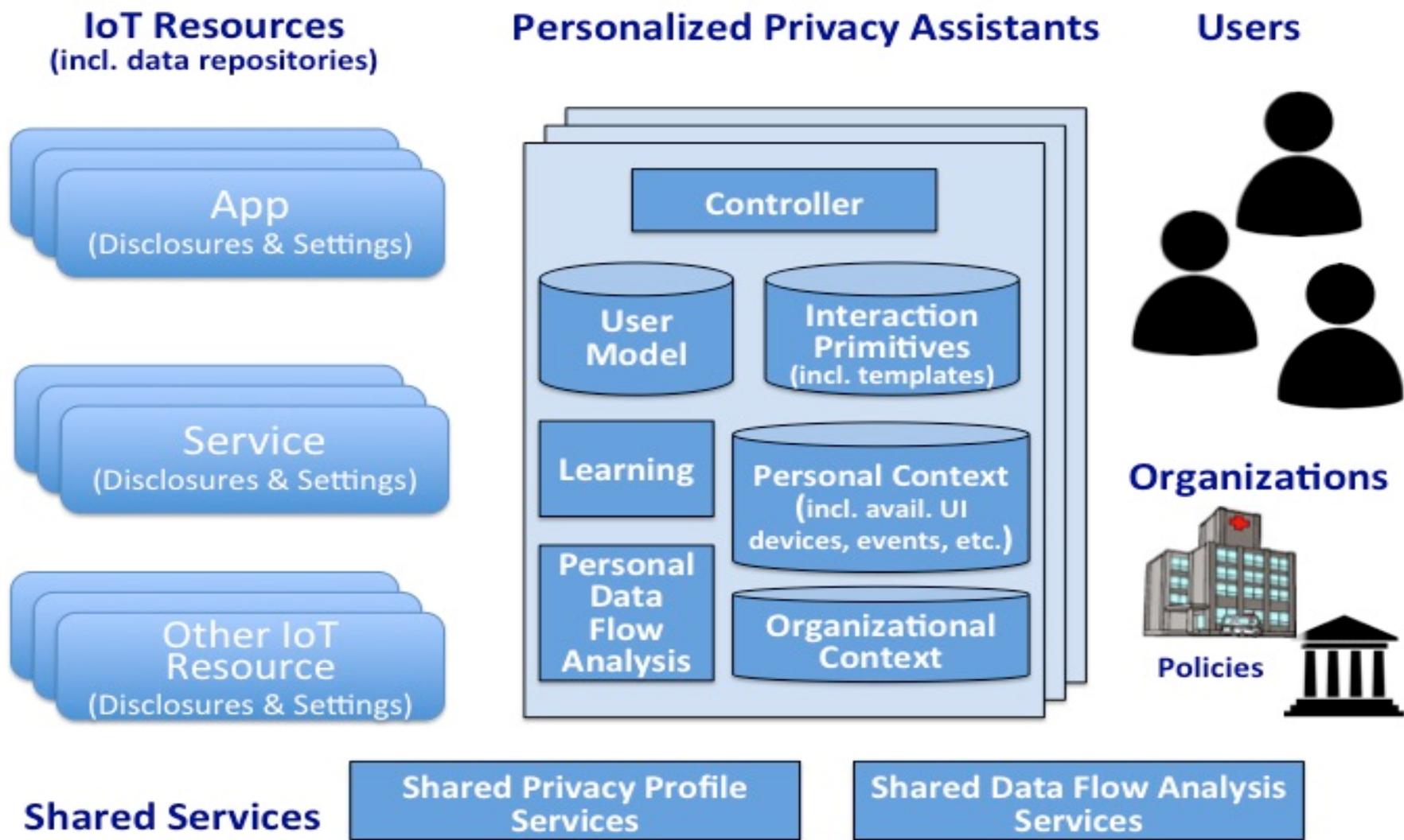
## Successfully Piloted with Android Users

---

- ❑ Piloted with 29 Android users – 10 day study
- ❑ **Users accepted 73.7% of our recommendations**
- ❑ Only **5.6% of accepted recommendations were modified over the next 6 days**, despite nudges to revisit earlier decisions
  - Users showed great engagement, modifying many settings not covered in the recommendations
- ❑ Users are comfortable with the recommendations and see the value of the assistants

*"To Deny, or Not to Deny: A Personalized Privacy Assistant for Mobile App Permissions,"* Bin Liu, Mads Skaarup Andersen, Florian Schaub, Norman Sadeh, Hazim Almuhiemedi, Yuvraj Agarwal, Alessandro Acquisti - working paper, 2016

# Extending this to IoT



# Personalized Privacy Assistants for IoT

---

- Registries enable owners to **register their IoT resources**
  - Resources associated with locations/areas
  - Menus lead to automated **generation of machine-readable privacy policies**
- PPA's **discover relevant resources** by consulting registries & compare policies against user profiles (**expectations and preferences**)
  - Selective **alerts & semi-automated configuration** of available privacy settings

## Concluding Remarks- I

---

- PPAs aim to provide a **pragmatic approach to notice and choice**
  - Leveraging machine learning and privacy profiles
  - Learning people's privacy preferences and expectations to **minimize user burden**, yet ensure that **users are informed** about those issues they care about and **retain sufficient control over their settings**

## Concluding Remarks - II

---

- ❑ **Assumption:** Privacy profiles and learned preferences should **only be used for the purpose of managing user privacy**
- ❑ PPAs have to come with **strong privacy guarantees**
  - Could be offered by entities controlling specific ecosystems
  - Could be offered by **3<sup>rd</sup> parties dedicated to privacy management**
    - ❑ Opens the door to PPAs that cut across multiple ecosystems/environments but [requires open APIs](#)

---

**Contact:** *sadeh AT cs.cmu.edu*

**Acknowledgement:** *Funding provided under DARPA's Brandeis initiative, NSF SaTC/SBE Program, Google Web of Things Expedition*

*Contact: sadeh AT cs.cmu.edu*

**Collaborators:** *Bin Liu, Jialiu Lin, Mads Scharup Andersen, Florian Schaub, Alessandro Acquisti, Yuvraj Agarwal, Lujo Bauer, Lorrie Cranor*



# Discussion of Session 5

## Discussants:

- **Aaron Alva**, Federal Trade Commission
- **Geoffrey Manne**, International Center for Law and Economics
- **Davi Ottenheimer**, Institute for Applied Network Security

## Presenters:

- **Sarthak Grover**, Princeton University
- **Vitaly Shmatikov**, Cornell Tech
- **Florian Schaub**, Carnegie Mellon University
- **Norman Sadeh**, Carnegie Mellon University





# Closing Remarks

Lorrie Cranor, Chief Technologist



**PRIVACY** CON  
FEDERAL TRADE COMMISSION