DSC 102
Privacy and Security in Data Science

Today’s content will not
be covered in the exam.

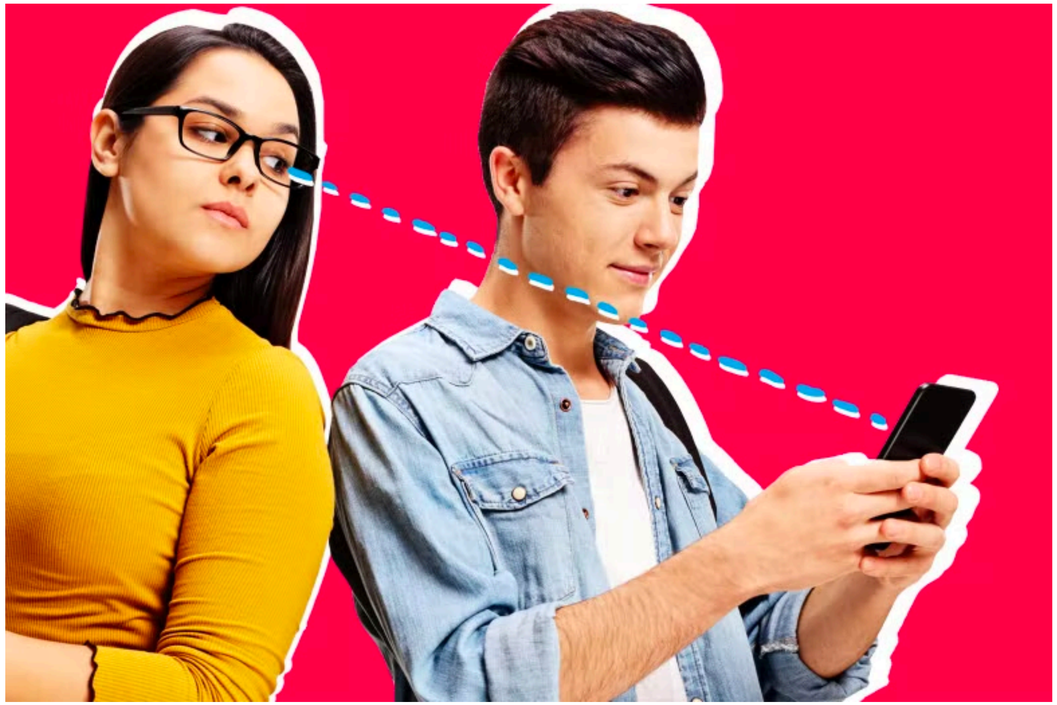
Agenda

1. Intro to S&P.
2. Research Examples.
    1. Problem and Results.
3. Future work and Capstone.

Intro to S&P

Privacy is a large umbrella for many different things.

Teen's privacy



Shoulder peeking

Privacy v.s. Security

- A user's bank account is hacked, and the hacker takes the user's money.
- A user's friend knows the password and logs into the user's bank account to check the spending history.
- The bank sells users' data to a third-party agency; the agency uses the user's shopping history to recommend something to that user, which may leverage the users' vulnerability.

Story #1 Walmart Beer and Diaper (1988)

Forbes 1988

- Unexpected correlation:
  - Sales of diapers and beer

https://www.forbes.com/forbes/1998/0406/6107128a.html?sh=2574a9316260

Story #2 Target Pregnancy (2012)

3,652,539 views | Feb 16, 2012, 11:02am

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did

Kashmir Hill Former Staff
Tech
Welcome to The Not-So Private Parts where technology & privacy collide

This article is more than 2 years old.

Every time you go shopping, you share intimate details about your consumption patterns with retailers. And many of those retailers are studying those details to figure out what you like, what you need, and which coupons are most likely to make you happy. Target TGT +0%, for example, has figured out how to data-mine its way into your womb, to figure out whether you have a baby on the way long before you need to start buying diapers.

Target has got you in its aim

Target predicted that a teenage girl might be pregnant and sent a diaper coupon to the girl.

How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did.
Kashmir Hill, Forbes, 2012

Story #3 Riot LoL ChatLogs

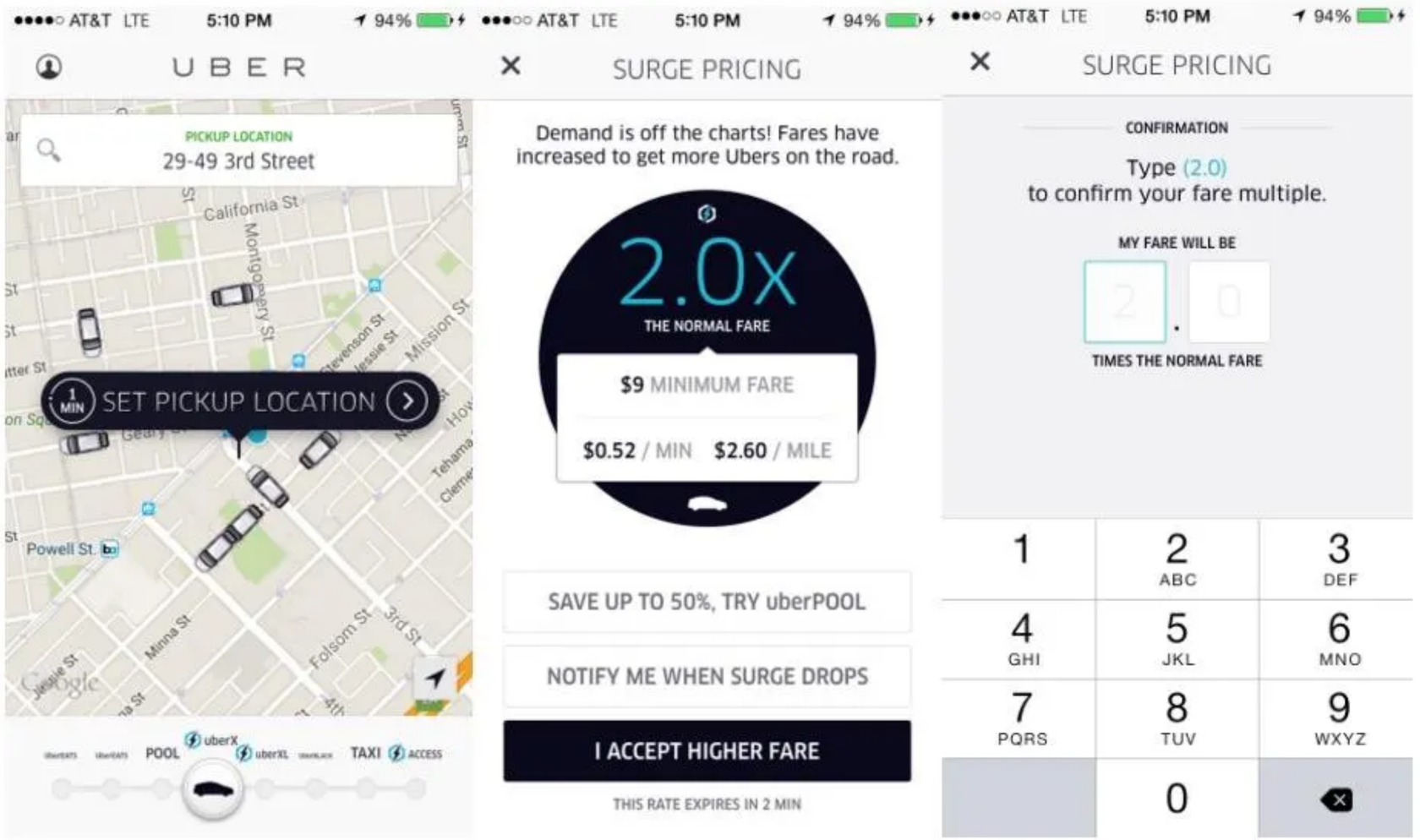
Riot Games uses its employee's League of Legends chat logs to spot bad behavior

By James Dator | Jun 12, 2016, 4:41pm EDT

SHARE

https://www.riftherald.com/2016/6/12/11914664/riot-league-of-legends-chat-log-bad-behavior-toxic-play

Story #4 Users Are More Likely To Pay Surge Pricing If Their Phone Battery Is Low



https://forbes.com/sites/amitchowdhry/2016/05/25/uber-low-battery/?sh=498982e774b3

A thought experiment: Data

"In our data-driven organization we collect real-time data streams and store them in our data warehouse. Our data scientists use advanced analytics and data processing in order to derive new insights."

Designing Data-Intensive Applications, p537

A thought experiment: Data → Surveillance

*"In our **surveillance**-driven organization we collect real-time **surveillance** streams and store them in our **surveillance** warehouse. Our **surveillance** scientists use advanced analytics and **surveillance** processing in order to derive new insights."*

Designing ***surveillance***-Intensive Applications, p537

DSC 291 Privacy-sensitive Data Systems (Winter 2025)

- Understand range of current problems and tensions around data privacy.
- Learn why privacy is hard.
- Learn the designs/proposals/methods to address privacy problems?
  - Not just for content but context
  - Why does this design/proposal/paper exist?
  - Why do they fail?
  - Can we do sth better? (My research & your course projects!)

Data Smith Lab

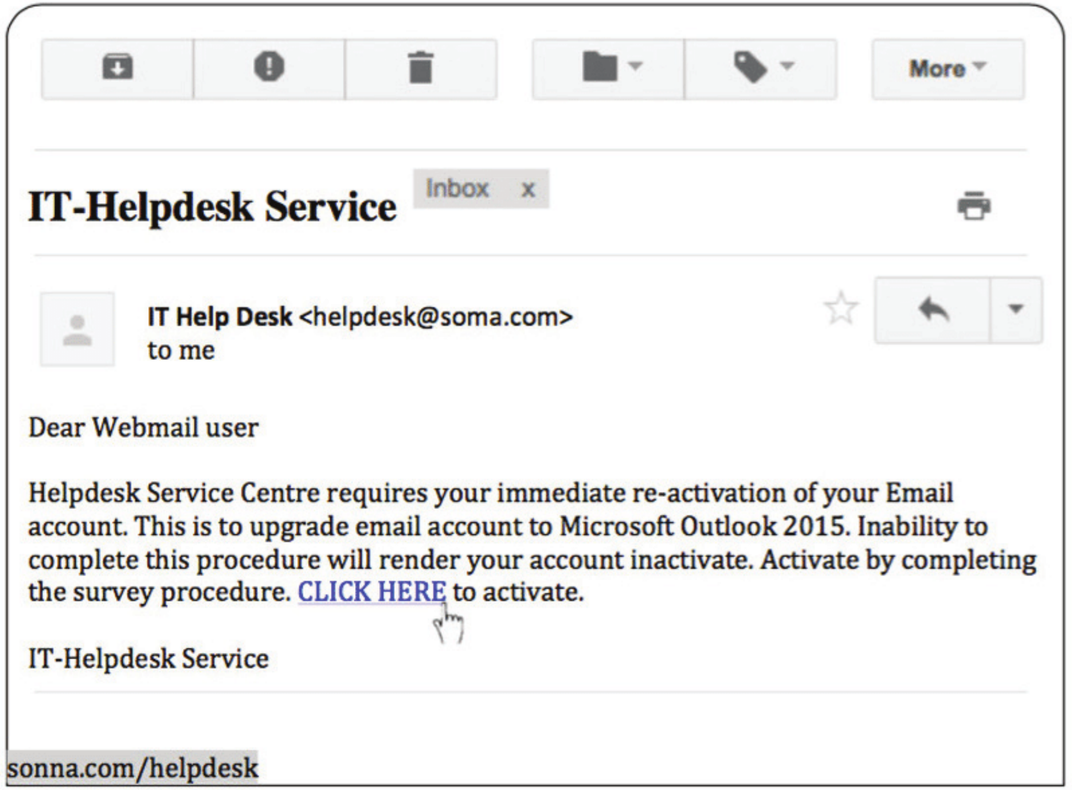
Human developers create risky computer systems that eventually affect human users.

1. Help developers create systems with enhanced privacy and security features.
2. Help users safeguard their privacy and security.

Research examples

Example #1

Problem - Phishing emails



POLICY / SECURITY

Uber's hack shows the stubborn power of social engineering

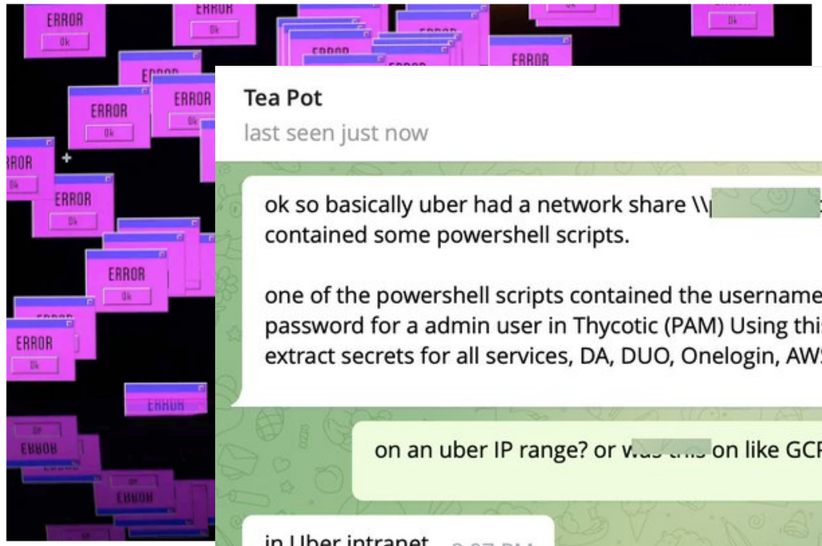


Photo by Amelia Holow

/ In corporate IT syst
weak

Tea Pot
last seen just now

ok so basically uber had a network share \\ ots. the share contained some powershell scripts.

one of the powershell scripts contained the username and password for a admin user in Thycotic (PAM) Using this i was able to extract secrets for all services, DA, DUO, Onelogin, AWS, GSuite 8:05 PM

on an uber IP range? or w on like GCP or AWS (*.uberinternal) edited 8:06 PM

in Uber intranet 8:07 PM

*.corp.uber.com edited 8:07 PM

How'd you get access to the intranet then? 8:08 PM

SE an employee -> access VPN -> scan intranet? 8:08 PM

yes! 8:08 PM

exactly 8:08 PM

nments (2 New

Example #1

Employees are the weakest link.

March 01, 2018

Proofpoint Acquires CMU spinoff Wombat Security for $225 Million

Strip District firm is industry leader in training employees to prevent cyber attacks

By Byron Spice

› Media Inquiries

Proofpoint Inc., a leading cybersecurity company, has completed its acquisition of a Carnegie Mellon University spinoff, Wombat Security Technologies Inc., for $225 million. The deal was announced by Proofpoint last month.

"Because threat actors target employees as the weakest link, companies need to continuously train employees and arm them with real-time threat data," said Gary Steele, CEO of Proofpoint in Sunnyvale, Calif. "The acquisition of Wombat gives us greater ability to help protect our customers from today's people-centric cyberattacks, as cybercriminals look for new ways to exploit the human factor."

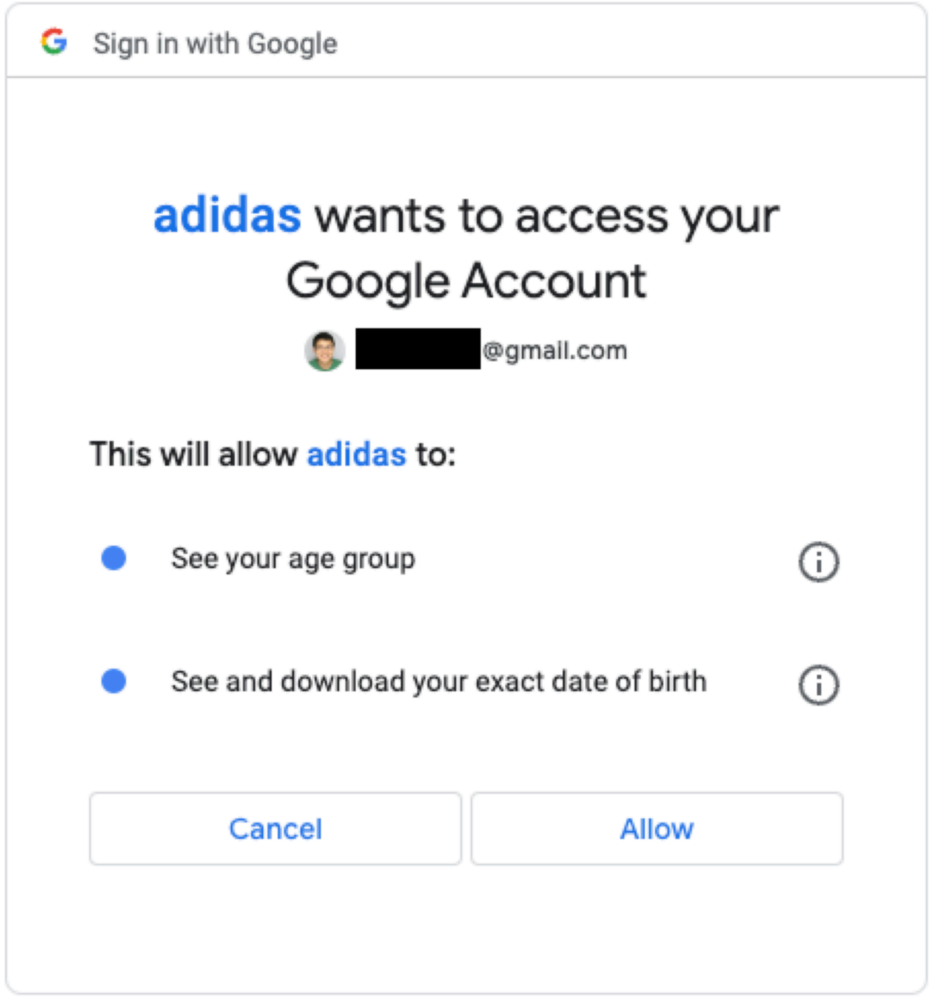
Wombat, founded 10 years ago by three CMU computer science professors to leverage innovative university research on preventing cyber attacks, is widely recognized as a leader in cybersecurity awareness training.

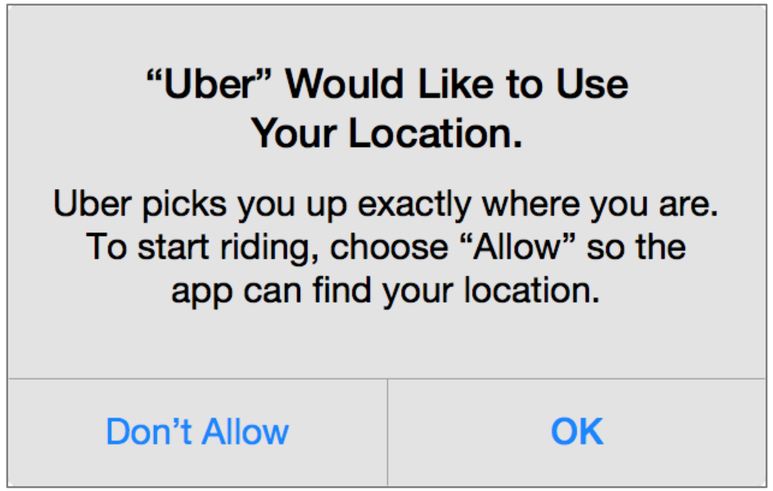
Example #1

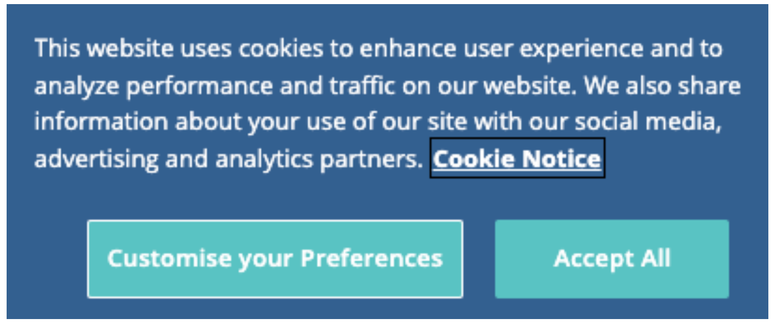
Employees are the weakest link.

Example #2

Problem - Permission popups





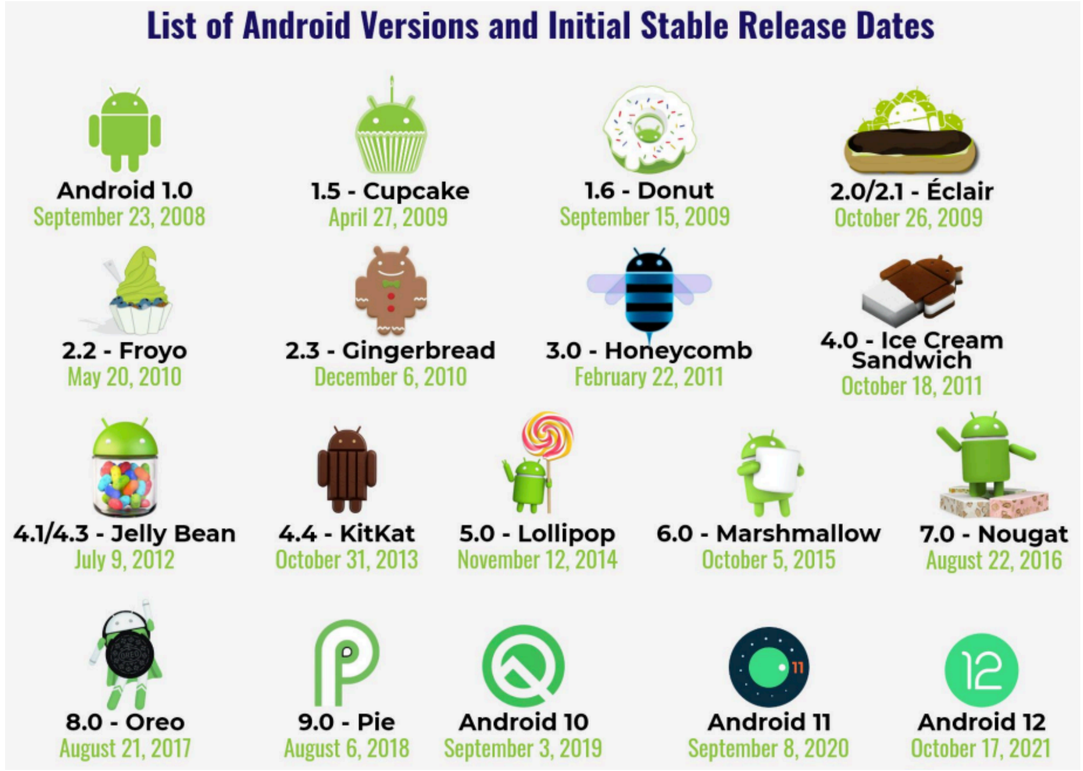


Notice and choice

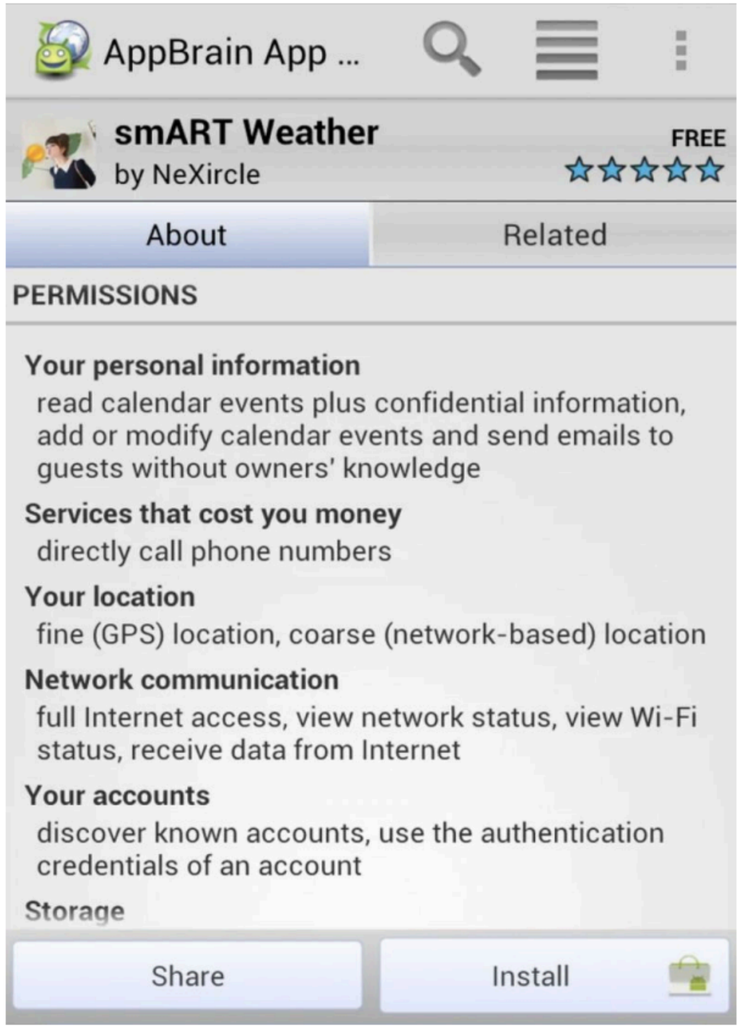
Informed decisions

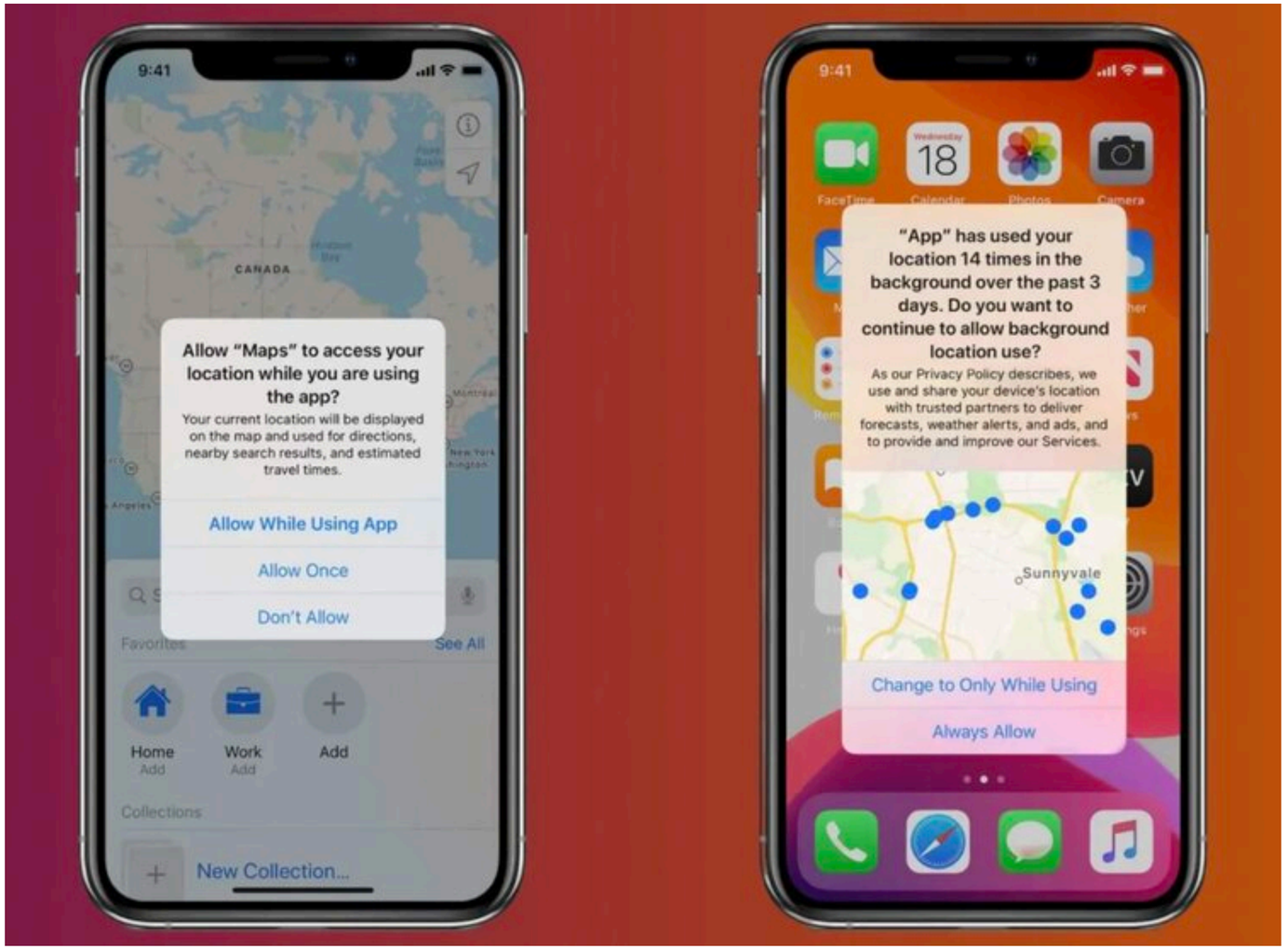
Example #2

Problem - Permission popups



2009 → 2023?


AppBrain App ...
smART Weather
by NeXircle
FREE
About
Related
PERMISSIONS
Your personal information
read calendar events plus confidential information, add or modify calendar events and send emails to guests without owners' knowledge
Services that cost you money
directly call phone numbers
Your location
fine (GPS) location, coarse (network-based) location
Network communication
full Internet access, view network status, view Wi-Fi status, receive data from Internet
Your accounts
discover known accounts, use the authentication credentials of an account
Storage
Share
Install

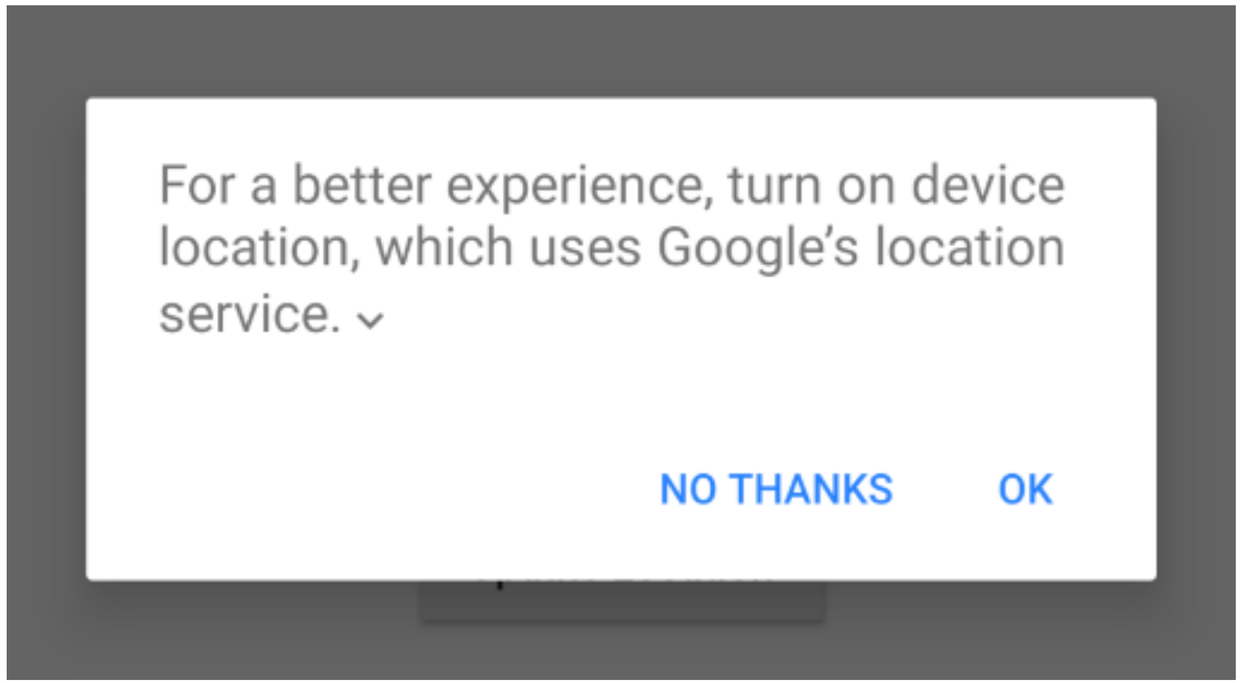

9:41
CANADA
Allow "Maps" to access your location while you are using the app?
Your current location will be displayed on the map and used for directions, nearby search results, and estimated travel times.
Allow While Using App
Allow Once
Don't Allow
Favorites
See All
Home
Add
Work
Add
Add
Collections
New Collection...
9:41
"App" has used your location 14 times in the background over the past 3 days. Do you want to continue to allow background location use?
As our Privacy Policy describes, we use and share your device's location with trusted partners to deliver forecasts, weather alerts, and ads, and to provide and improve our Services.
Sunnyvale
Change to Only While Using
Always Allow

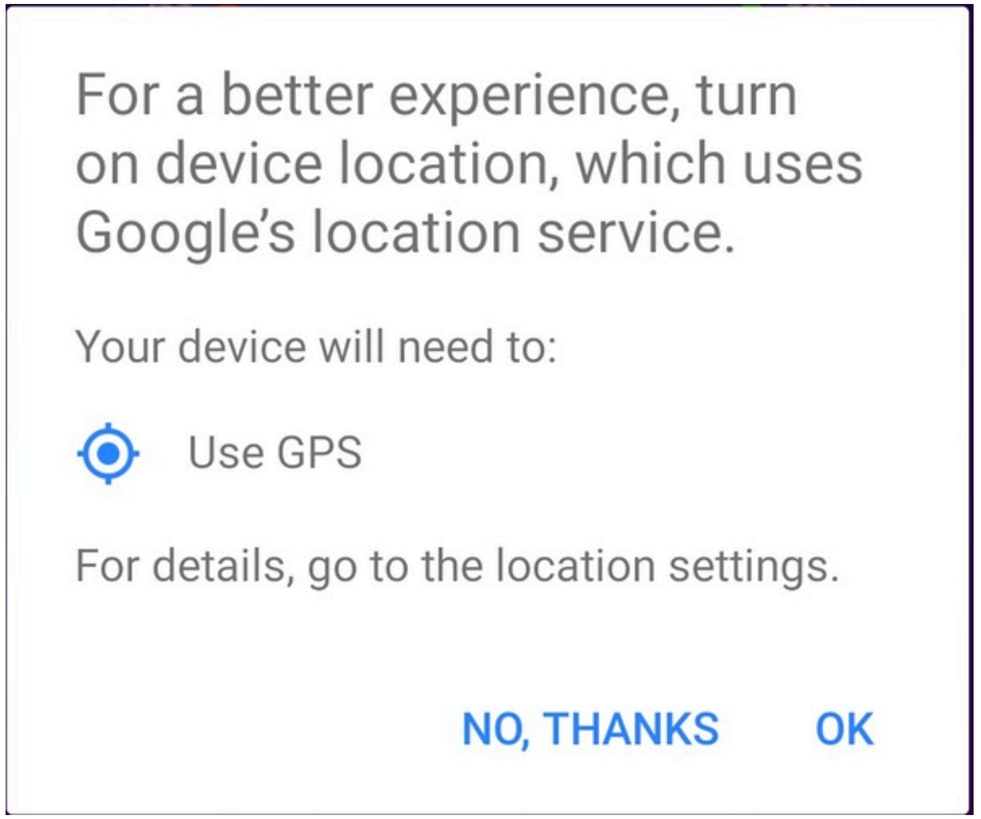
The permission granularity dilemma

More fine-grained permissions
→ Better privacy
→ More management burden for users
  Harder learning curve for app developers
  More implementation efforts for system builders

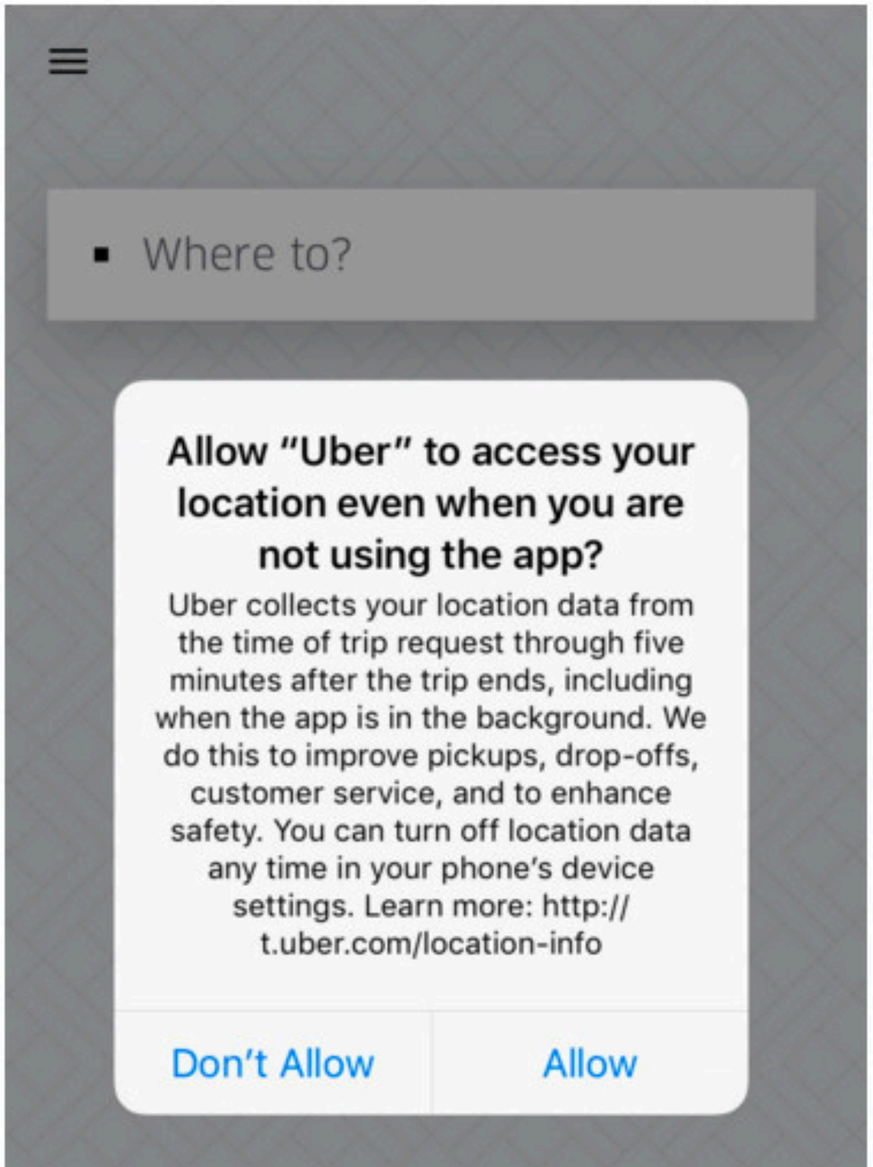
More coarse-grained permissions
→ Worse privacy
→ Overaccess risks
  More users deny data requests
  More complaints for system builders
  Hard to gain trust from users for app developers

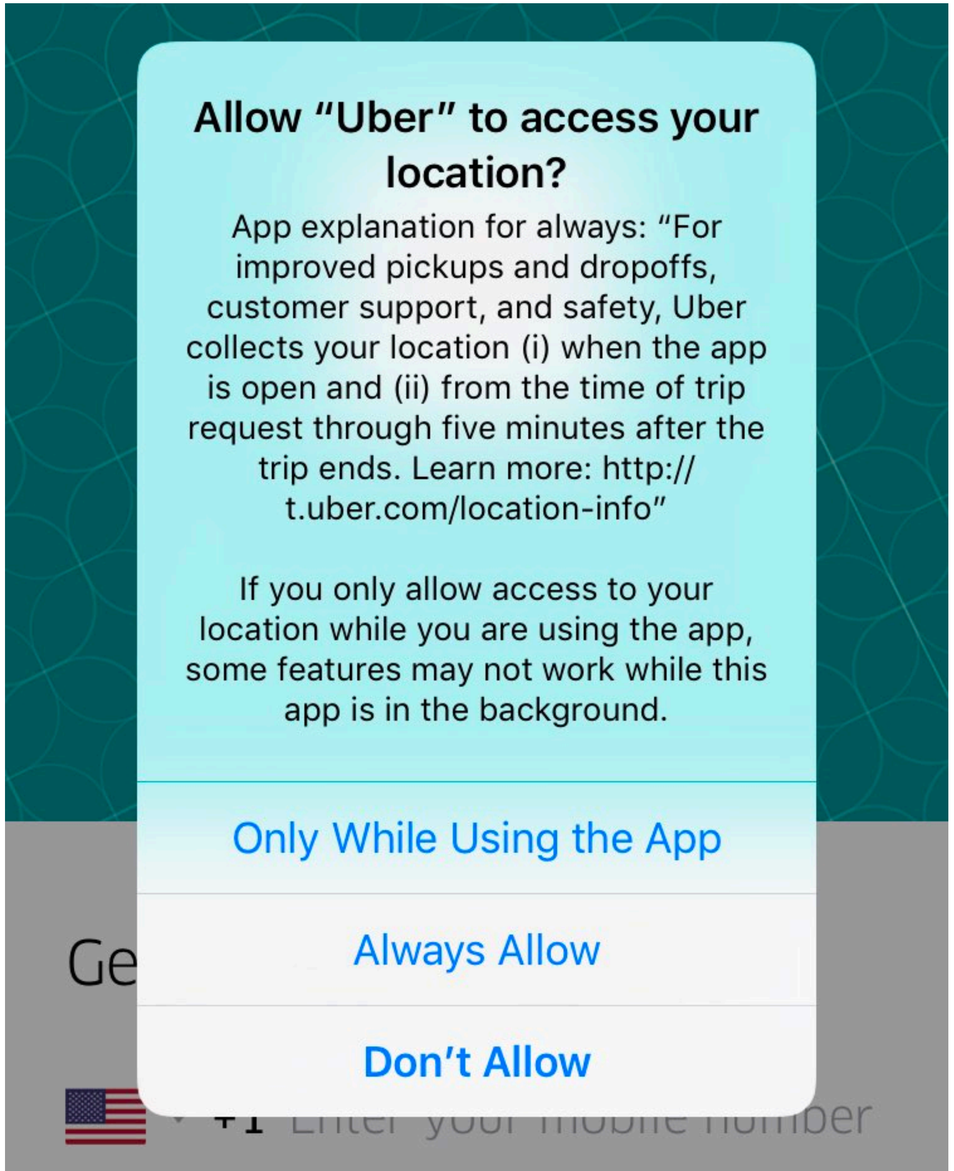
Challenges: Arbitrary Purpose strings



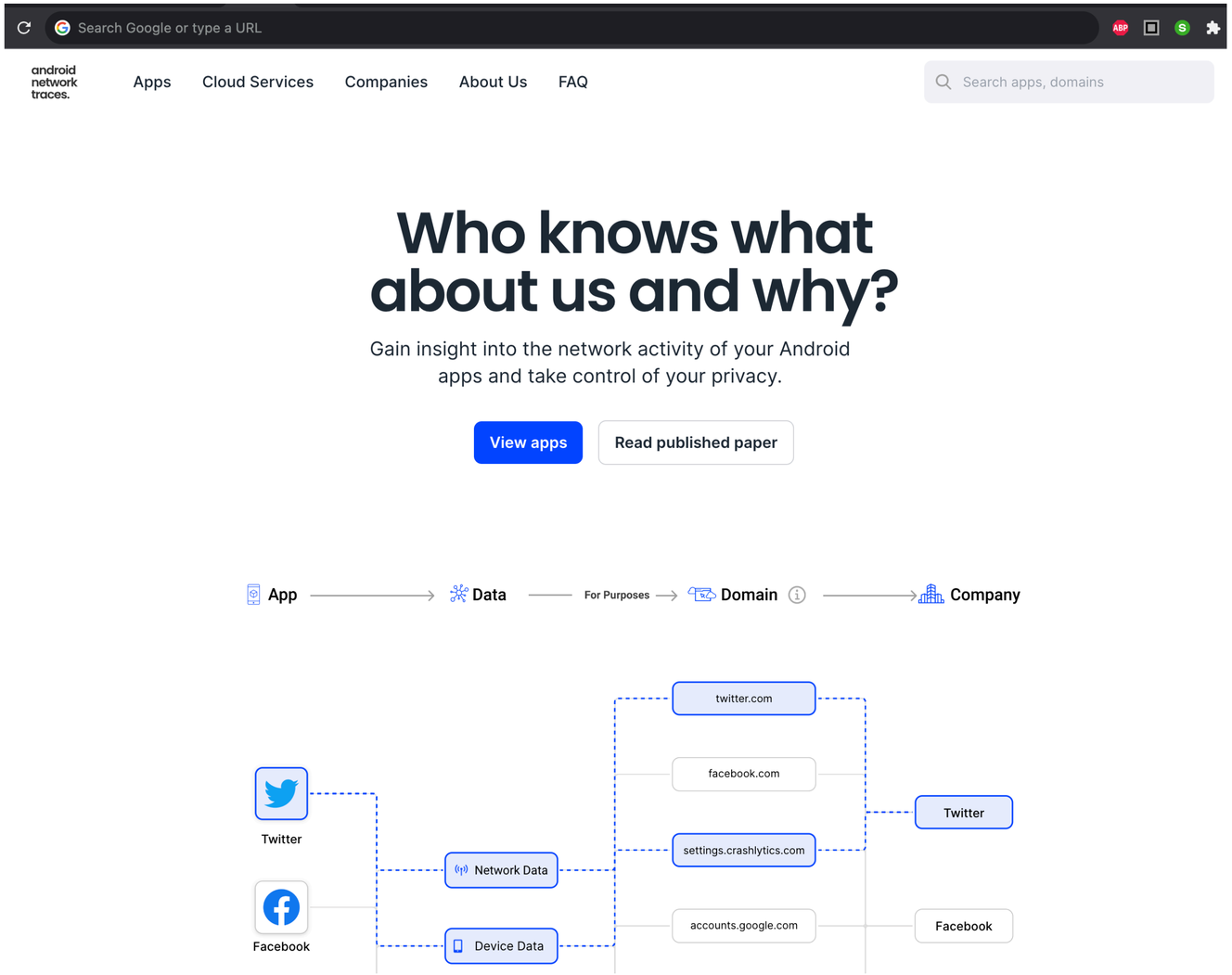


Challenges: Arbitrary Purpose strings

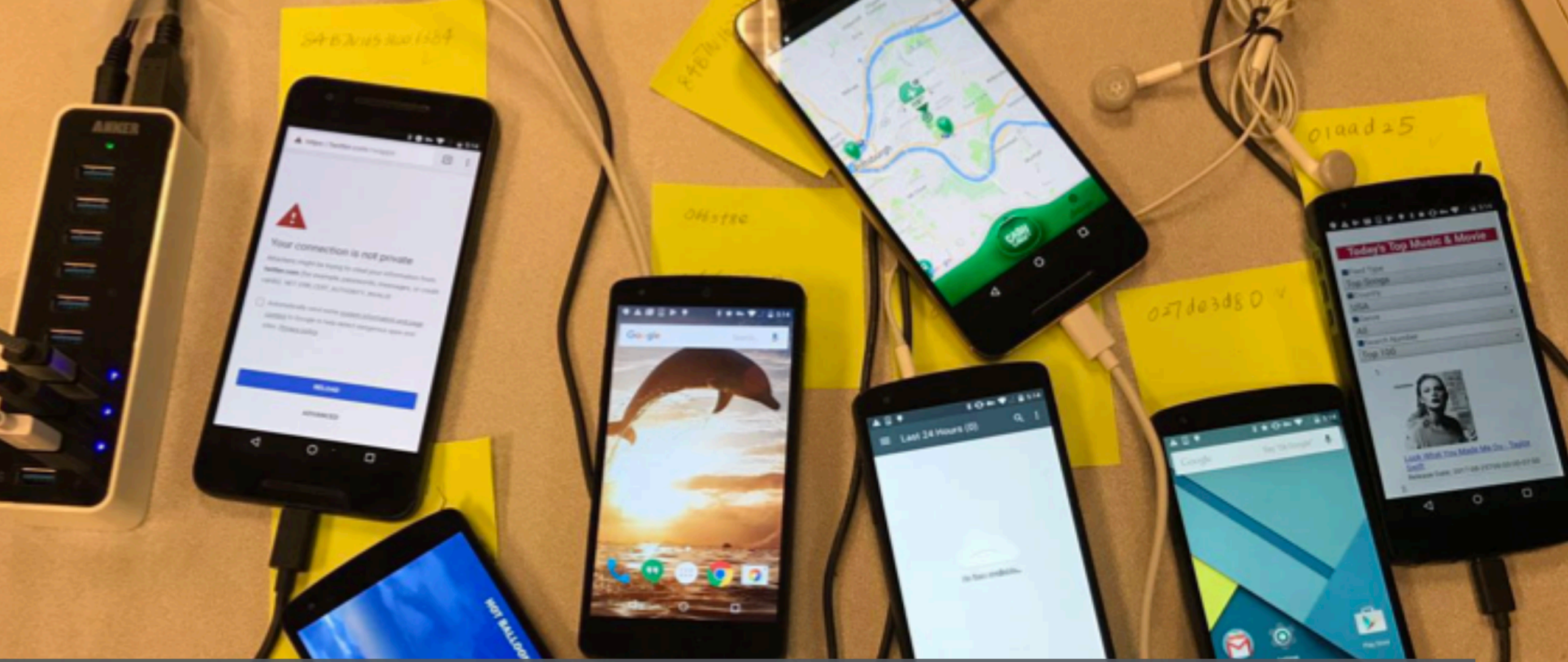




Categorized Purpose string (Ubicomp 2017)



http://android-network-tracing.herokuapp.com/

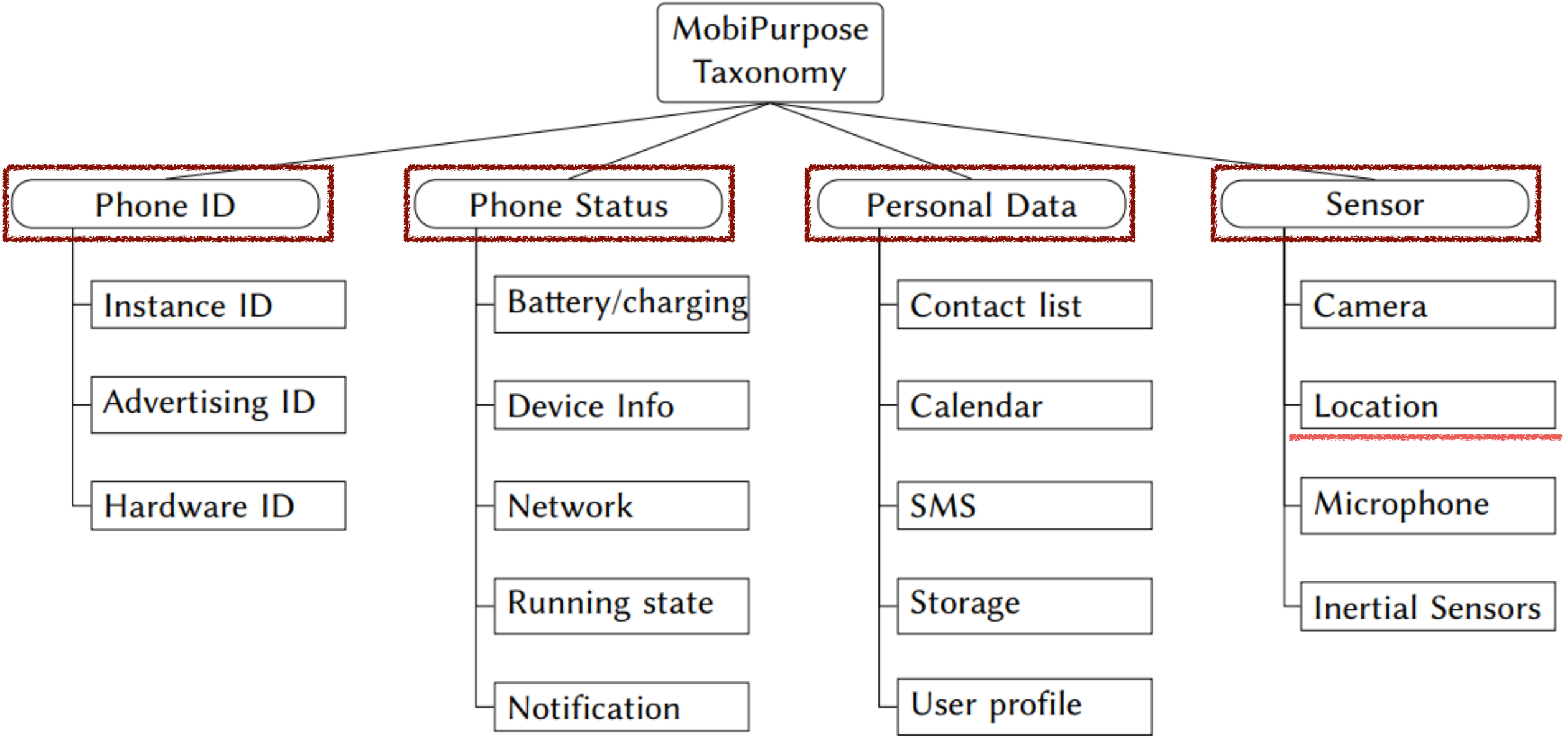


MobiPurpose is a **scalable in-lab** solution that can index **fine-grained** privacy attributes (**who**, **where**, **what**, **why**) of **outgoing** network requests.

Data purposes for location data

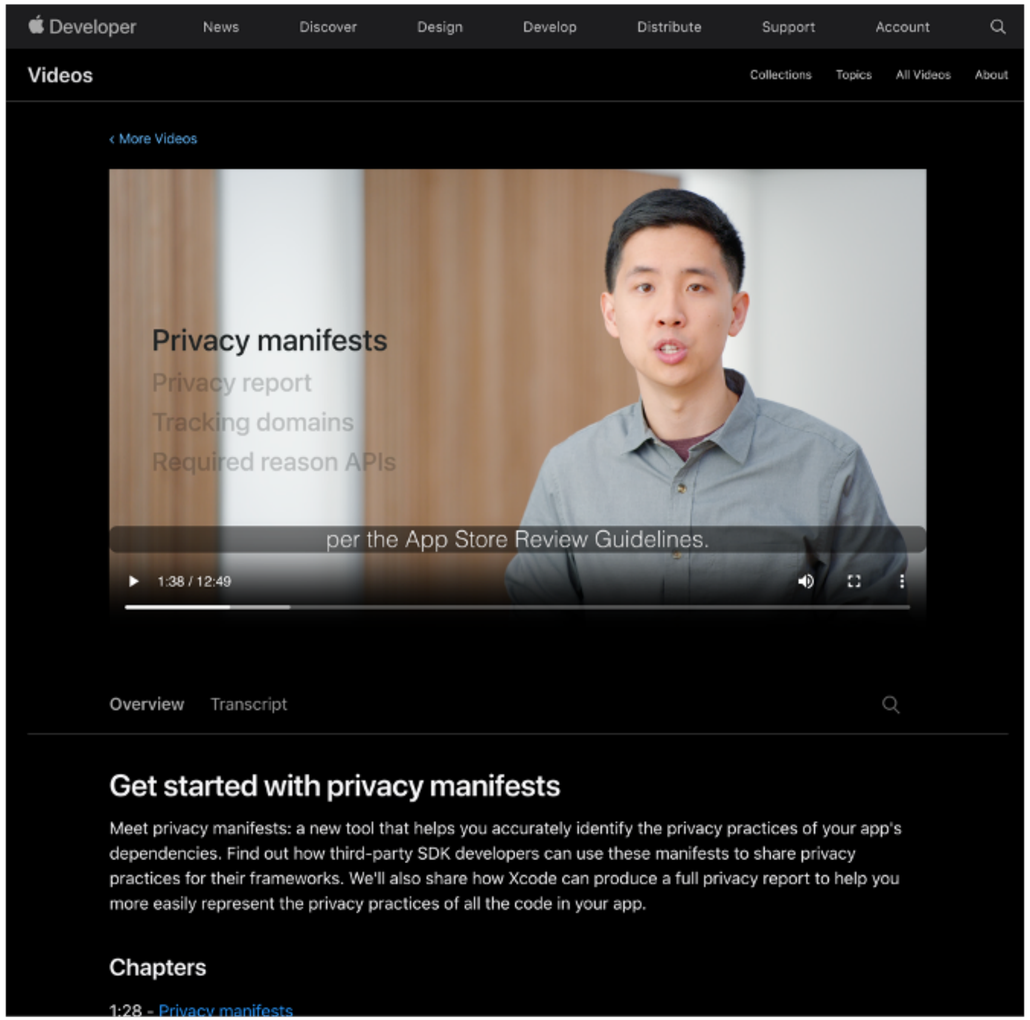
Location[7]	Nearby Search	Search nearby POIs/real estates
	Location-based Customization	Fetch local weather/radio information
	Query Transportation Information	Estimate the trip time through Uber API
	Recording	Track the running velocity
	Map and Navigation	Find the user location in Map apps
	Geosocial Networking	Find nearby users in the social network
	Geotagging	Tag photos with locations
	Location Spoofing	Set up fake GPS locations
	Alert and Remind	Remind location-based tasks
	Location-based game	Play games require users' physical location
	Reverse geocoding	Use the GPS coords to find the real world address.
	Data collection for analytics	Collect data for marketing analysis
	Data collection for ad	Collect data for ad personalization

See the complete taxonomy at:
http://bit.ly/mobitaxonomy


MobiPurpose Taxonomy
Phone ID
Instance ID
Advertising ID
Hardware ID
Phone Status
Battery/charging
Device Info
Network
Running state
Notification
Personal Data
Contact list
Calendar
SMS
Storage
User profile
Sensor
Camera
Location
Microphone
Inertial Sensors

data types

Adoptions



Categorized Purpose string (2017 → 2024)

Declared manifests (2020 → 2024)

Fine-grained data minimization (??)

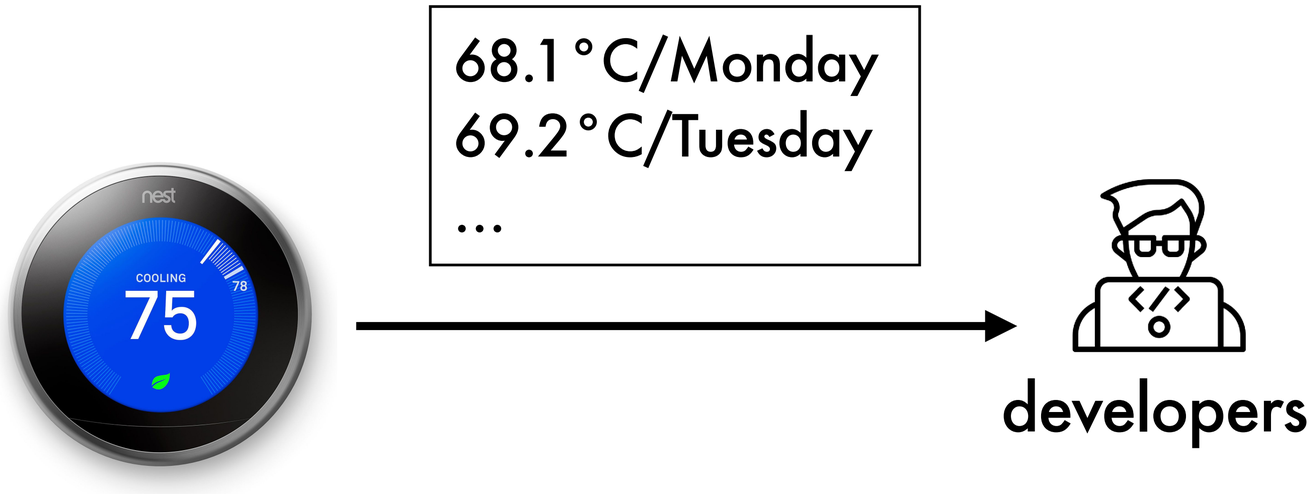
Operator-based API (?? postman api)

Machine-readable policies → User interfaces (??)

APPLE WWDC 2023

Example #3

How can Nest prove that they only collect aggregated data?

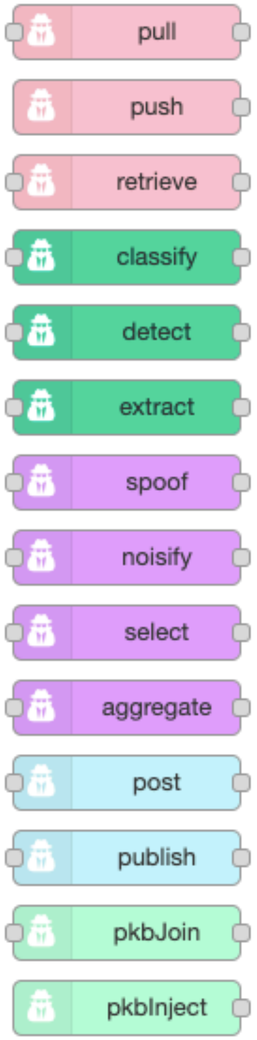


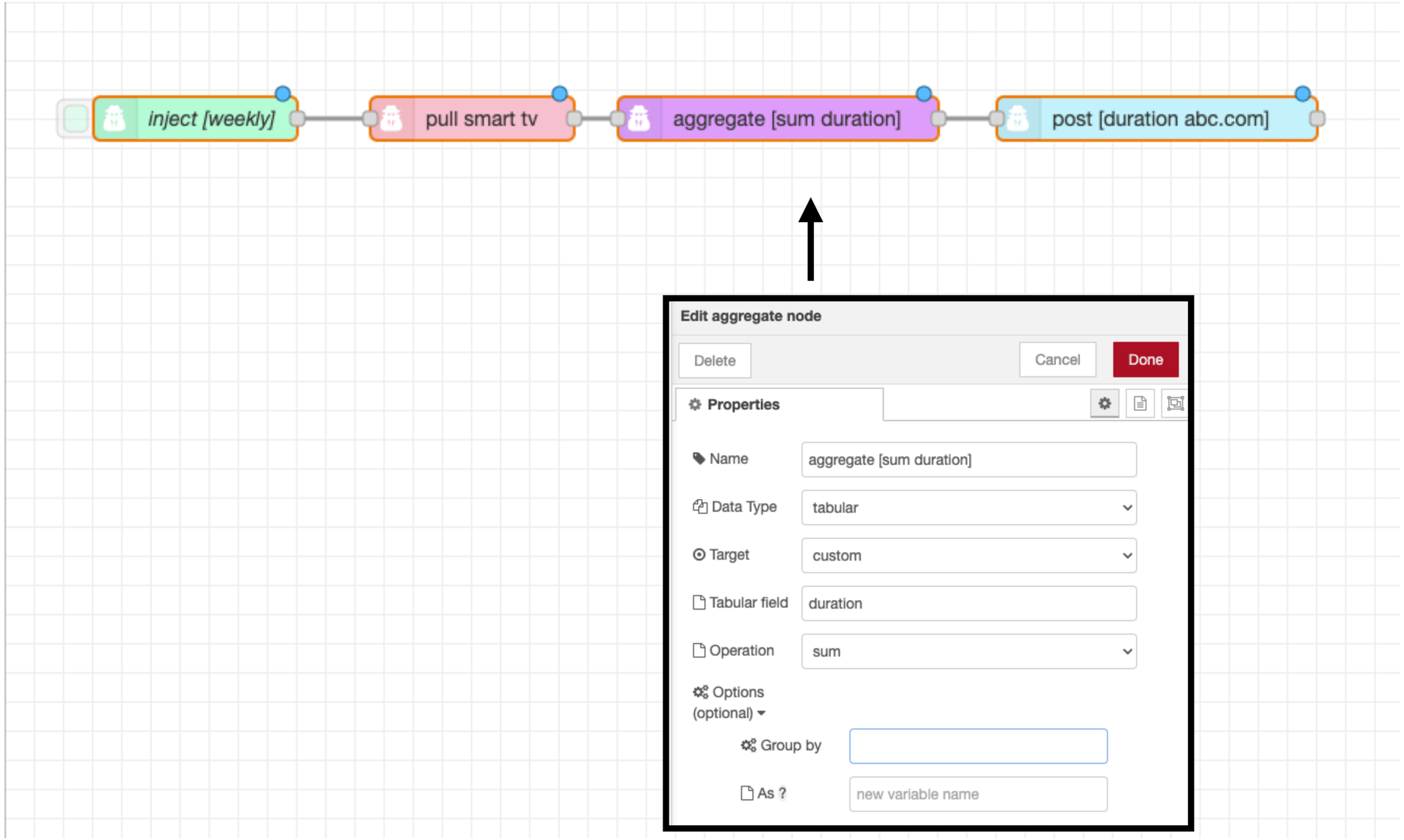
Open source?

[1] Jin et al., Peekaboo: A Hub-Based Approach to Enable Transparency in Data Processing within Smart Homes. S&P'22

Program pre-processing functions using chainable *operators*

A fixed set of operators





A text-based whitelist *manifest* (i.e., program representation)

How much time does the user spend on the TV?

```
@purpose: To measure device engagement.
WeeklyUsageHours{
  // operator [properties]
  inject [weekly] ->
  pull [smart TV driver] ->
  aggregate [sum duration] ->
  post [duration]
}
```

A trusted runtime with pre-loaded implementations

video #	duration	name	time	...
aaa	-	-	-	-
bbb	-	-	-	-
...	...	...	...	...

25 hours

How much time does the user spend on the TV?

A local hub

inject [weekly]

pull [smart tv]

video #	duration	name	time	...
aaa	-	-	-	-
bbb	-	-	-	-
...	...	...	...	...

aggregate [sum duration]

25 hours

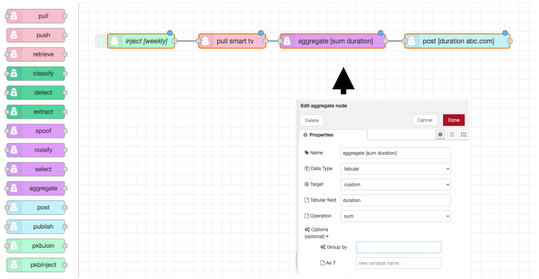
post [duration]

```
@purpose: To measure device engagement.
WeeklyUsageHours{
  // operator [properties]
  inject [weekly] ->
  pull [smart TV driver] ->
  aggregate [sum duration] ->
  post [duration]
}
```

A text-based manifest

A trusted runtime with pre-loaded, open-source implementations

Smart home app store



Programming environment with operators

Runtime with preloaded implementations

App developers

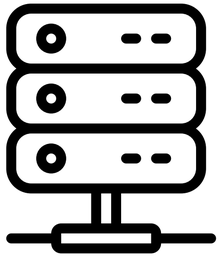
```
@purpose: To measure device engagement.
WeeklyUsageHours{
  // operator [properties]
  inject [weekly] ->
  pull [smart TV driver] ->
  aggregate [sum duration] ->
  post [duration]
}
```

Manifest

Smart home hub → privacy firewall

Smart home app →

```
@purpose: To measure device engagement.
WeeklyUsageHours{
  // operator [properties]
  inject [weekly] ->
  pull [smart TV driver] ->
  aggregate [sum duration] ->
  post [duration]
}
```



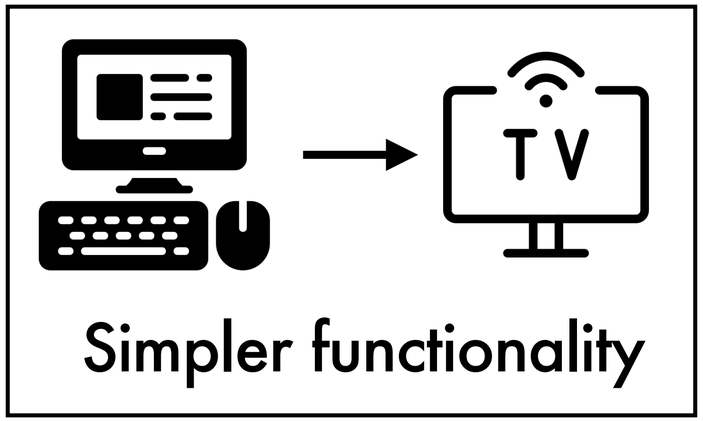
Edge devices

A local hub

Cloud

"Privacy firewall"

Peekaboo v.s. Firewall



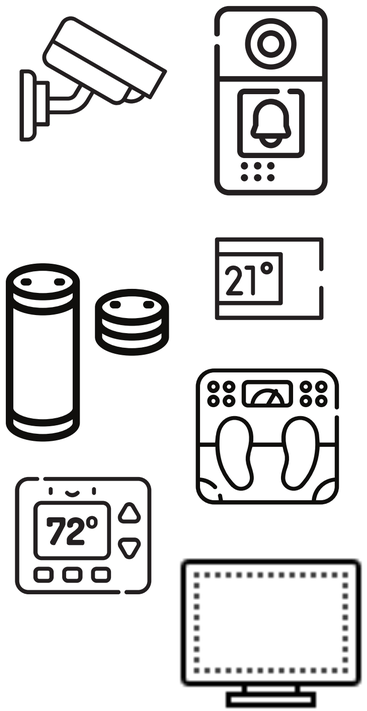
Whitelist-only

Developer-in-the-loop

77% Apps do not need raw data.

Pre-process users' data

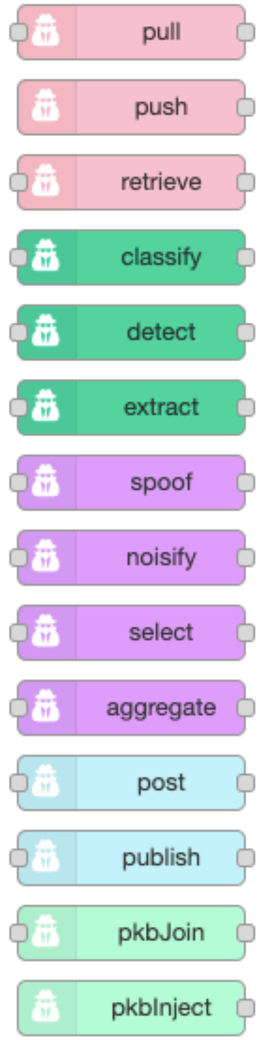
A fixed set of operators



Edge devices

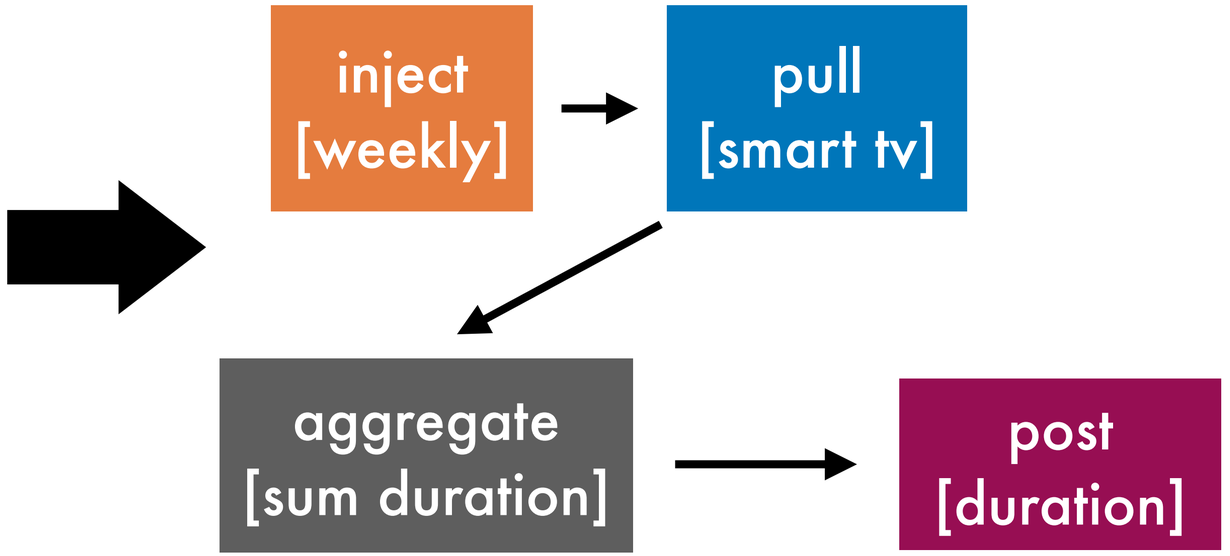
video, image, audio, tabular, scalar

A *fixed* set of operators



Manifests enforce fine-grained data collection

```
@purpose: To measure device engagement.
WeeklyUsageHours{
  // operator [properties]
  inject [weekly] ->
  pull [smart TV driver] ->
  aggregate [sum duration] ->
  post [duration]
}
```

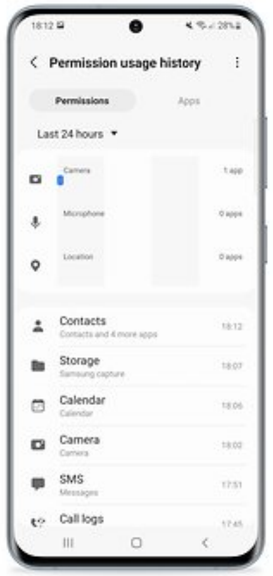


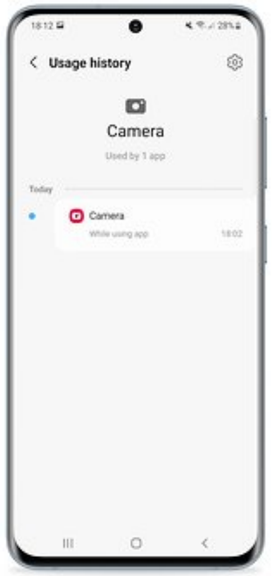
public, non-proprietary

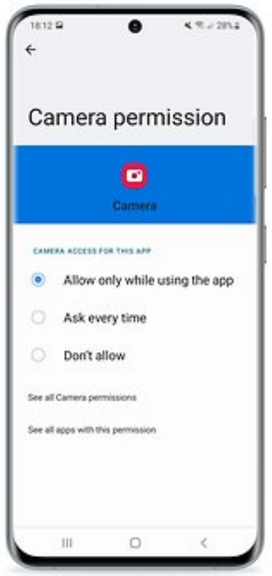
Advantages

Repetitive implementation and *distributed* interfaces

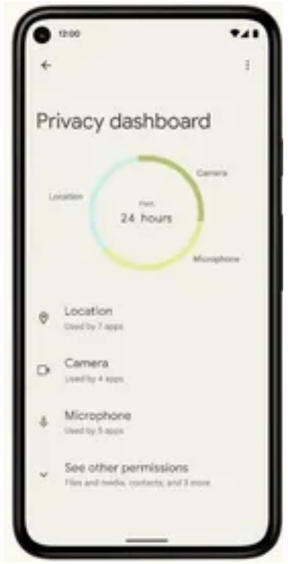
Samsung







Nest



Small developers?

Users?

Advantages

Manifests → *enforceable/dynamic* privacy nutrition labels

```
@purpose: To measure device engagement.
WeeklyUsageHours{
  // operator [properties]
  inject [weekly] ->
  pull [smart TV driver] ->
  aggregate [sum duration] ->
  post [duration]
}
```

[1]

Data Collection Disclosure

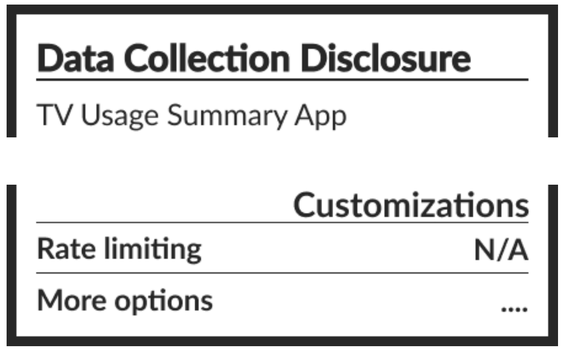
TV Usage Summary App

Running for	**20 days**
Total outgoing data packets **KBytes**	**80**
Sensor Type	**Smart TV**
Data type	**TV Watch history**
Granularity	**Weekly aggregated durations by content category**
Collection frequency	**Every wednesday 1:00 AM**
Destination	**www.abc.com**
Encryption	**HTTPS**
	Customizations
Rate limiting	**N/A**
More options	**....**

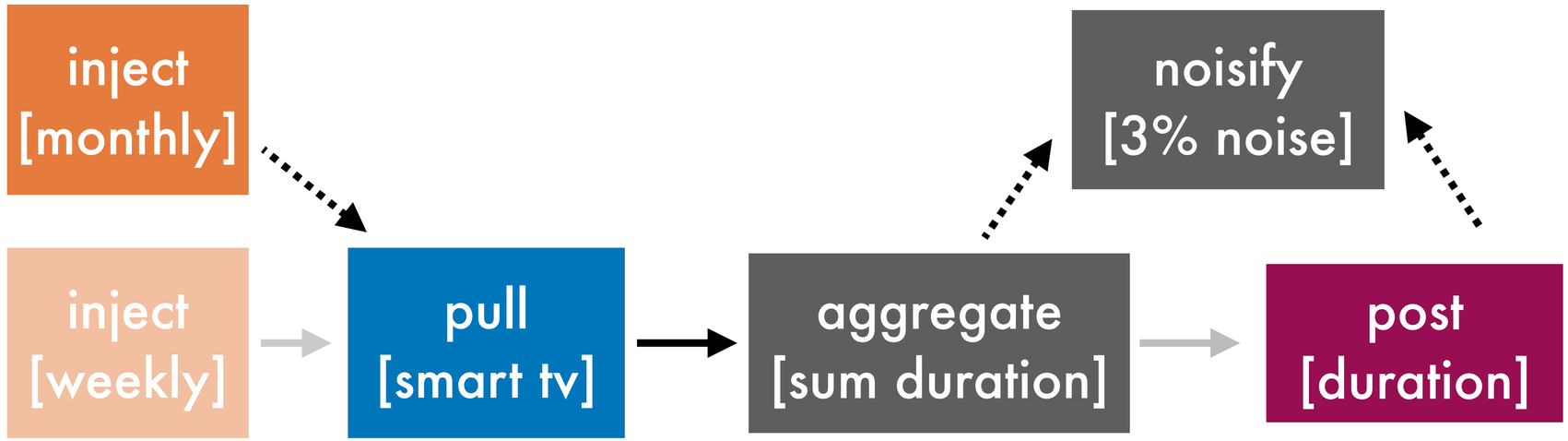
[1] Security and Privacy "Nutrition" Label, P. Emami-Naeini et al, IEEE S&P'20

Advantages

Built-in fine-grained control through manifest rewriting



Change the rate to monthly



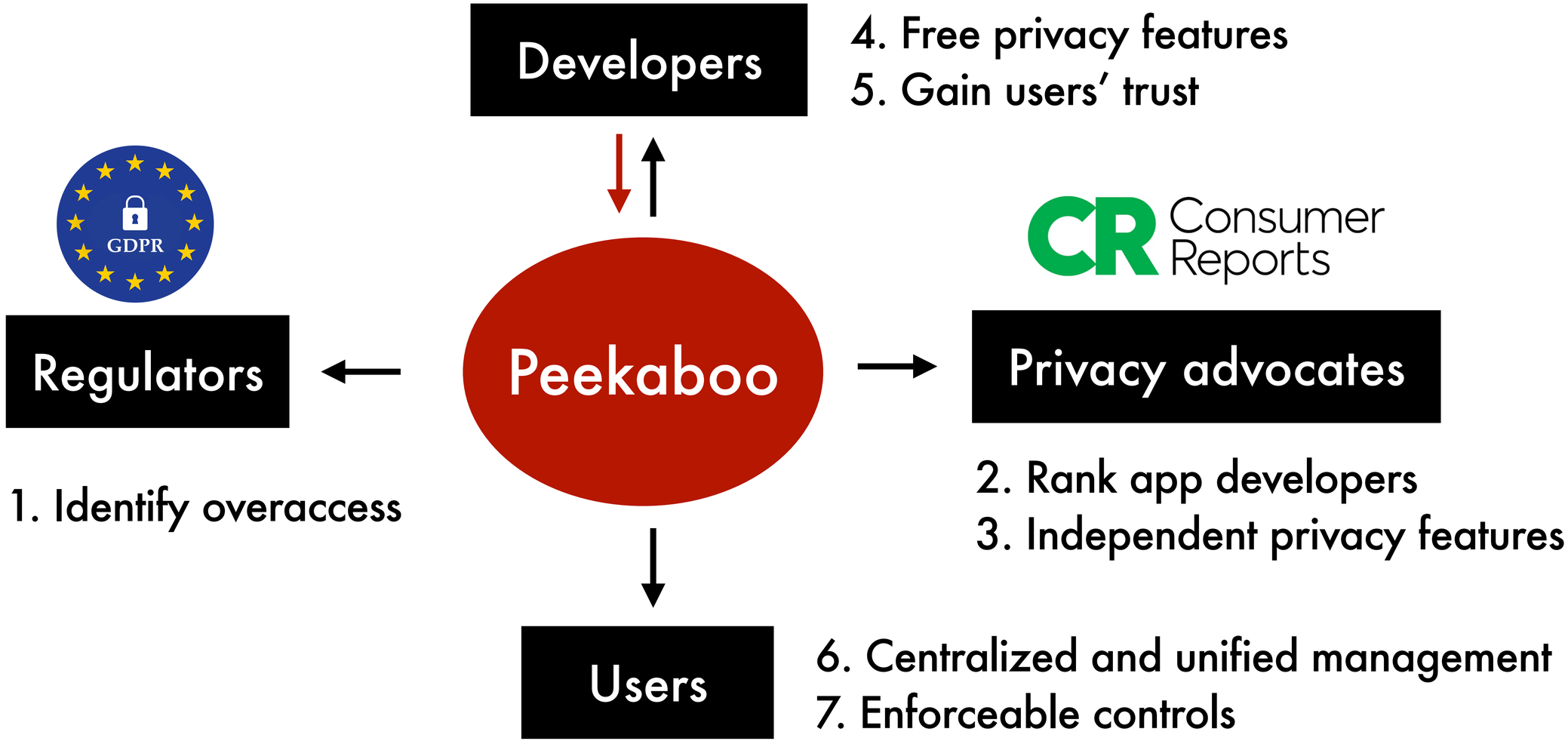
Revisit: The permission granularity dilemma

More fine-grained permissions.
→ Better default options.

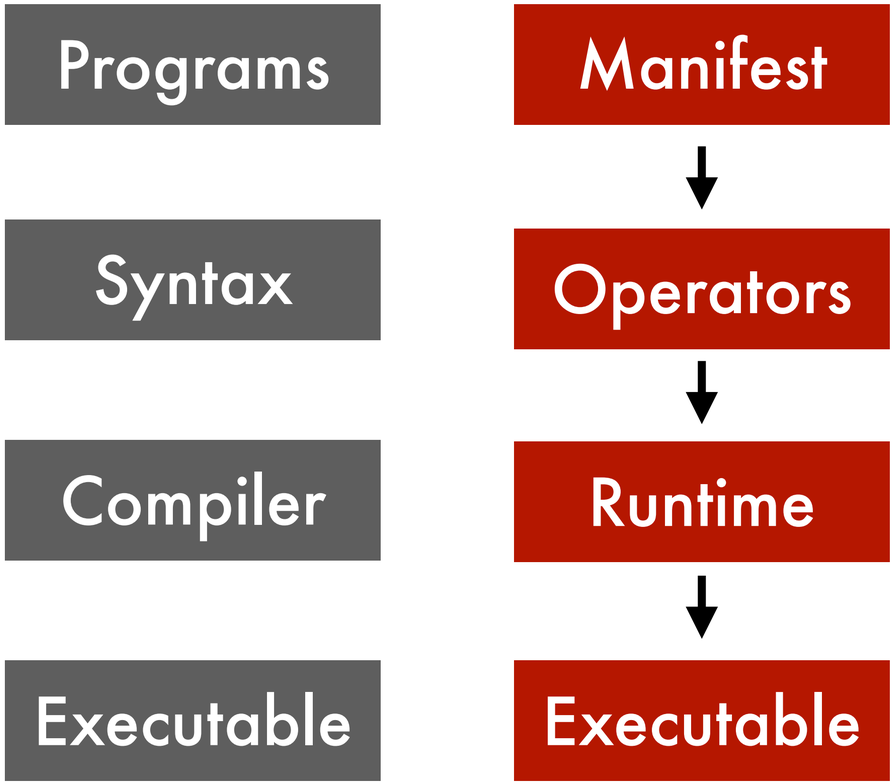
Machine-readable permissions
→ Easier to audit.
  → Better ecosystem. Good privacy drive-out bad privacy.
→ Aggregated management.

Decomposable (operator-based) permissions.
→ Fast development.

Let the good privacy drive out the bad privacy



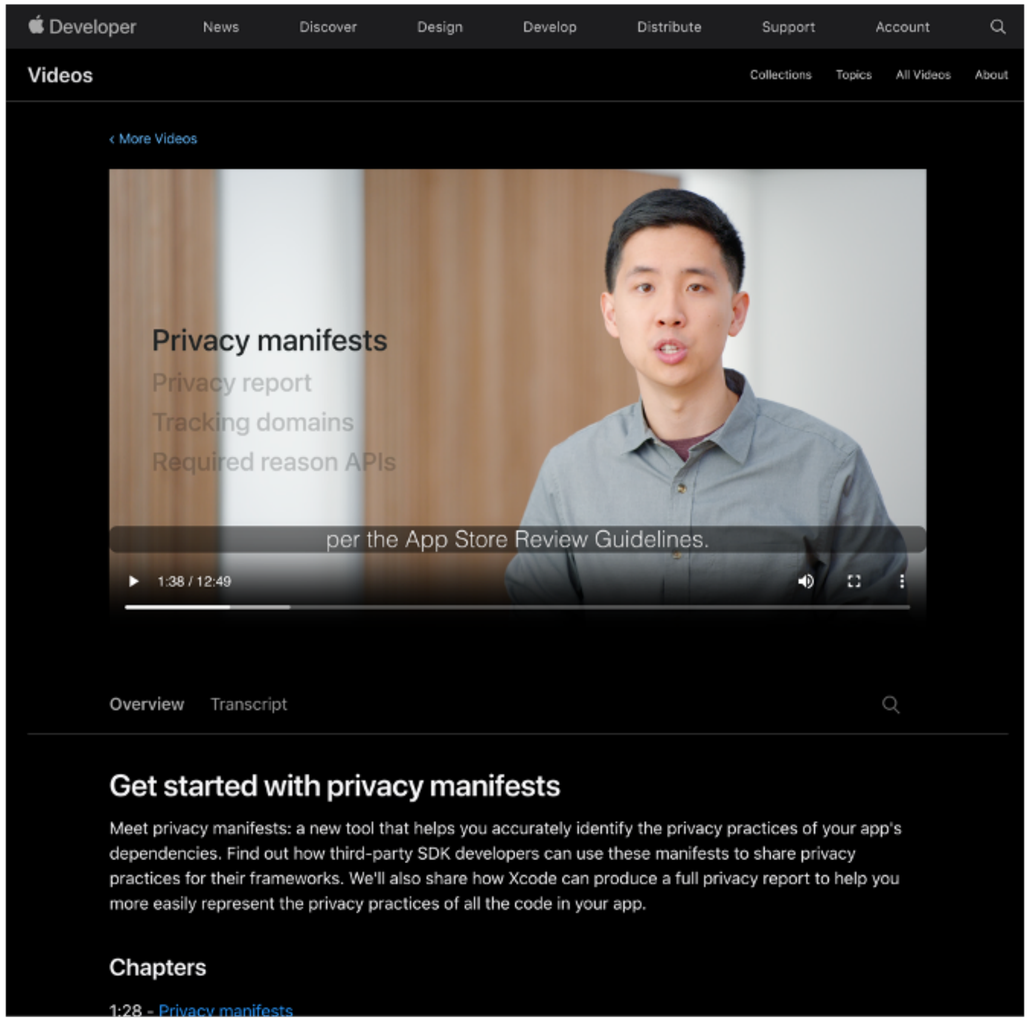
MPF is a simpler compiler architecture.



A fixed set of operators

A trusted runtime with a small set of pre-loaded implementations

Adoptions



Categorized Purpose string (2017 → 2024)

Declared manifests (2020 → 2024)

Fine-grained data minimization (??)

Operator-based API (?? postman api)

Machine-readable policies → User interfaces (??)

APPLE WWDC 2023

Example #4

Precision Medicine to Precision Privacy

modeling **individual** users' privacy expectations by understanding users' **underlying reasoning process** of forming privacy-related opinions.

Collective Privacy Norms

Companies should behave under their users' privacy expectations.

Individual Privacy Preferences

Users have **differing levels of sensitivity** to various types of contextual information across domains.

RQ2

How to capture contextual information and use it for privacy concern prediction?

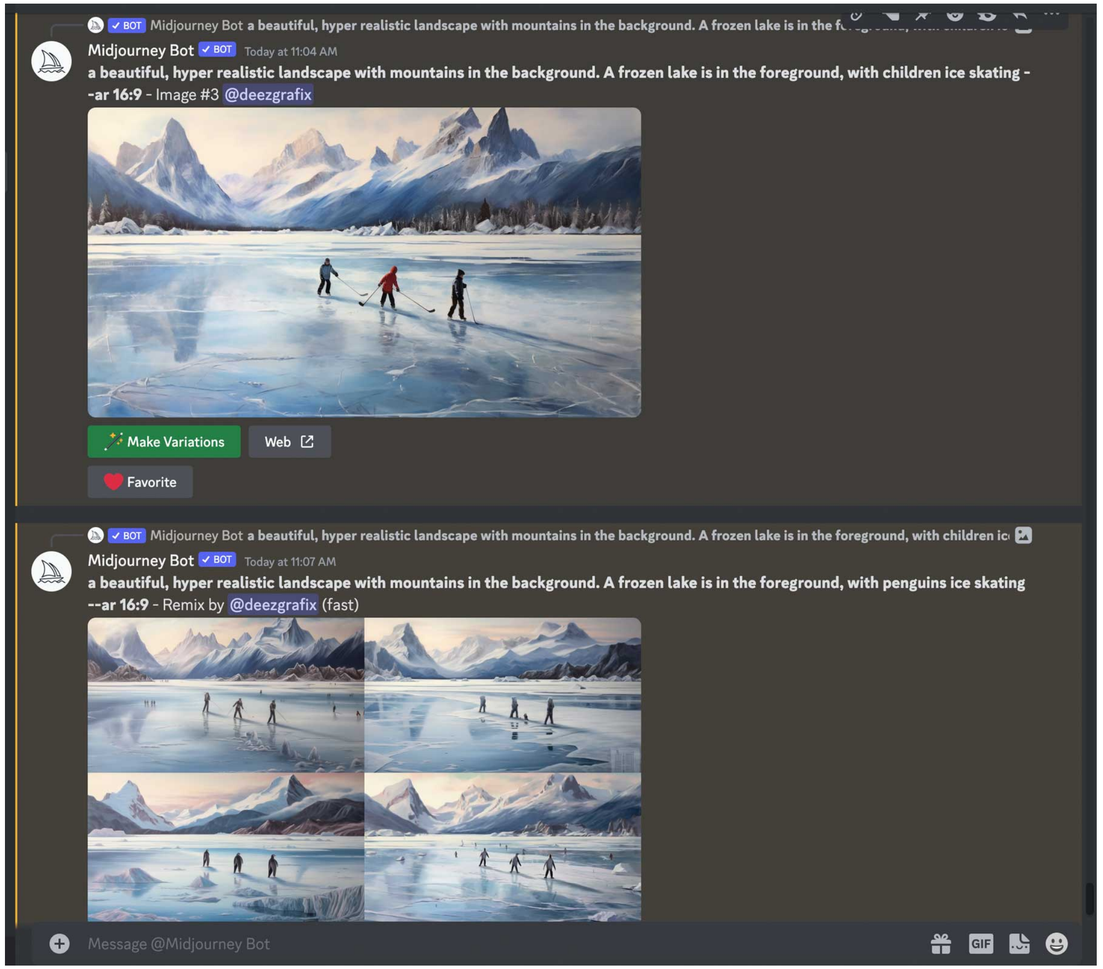
Example #5

Precision Medicine to Precision Privacy

modeling **individual** users' privacy expectations by understanding users' **underlying reasoning process** of forming privacy-related opinions.

Example #5

AI-Generated Content

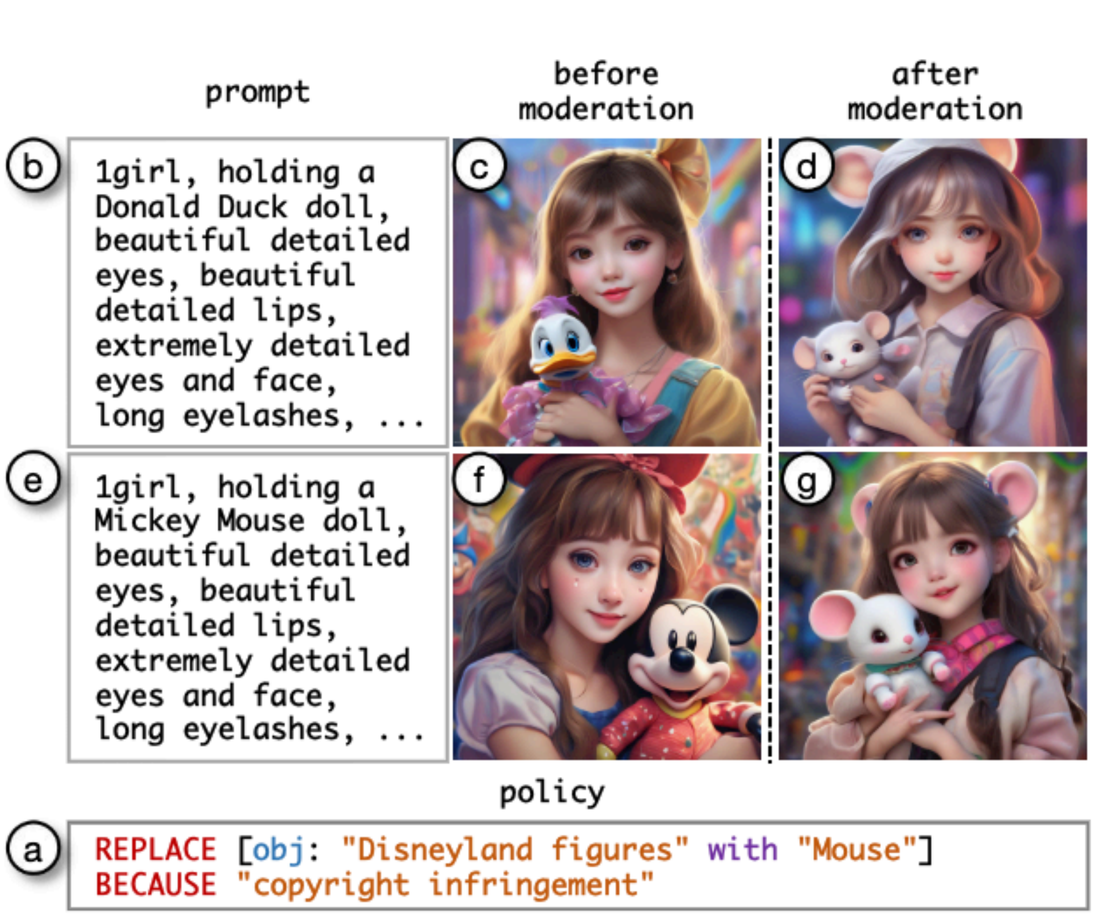


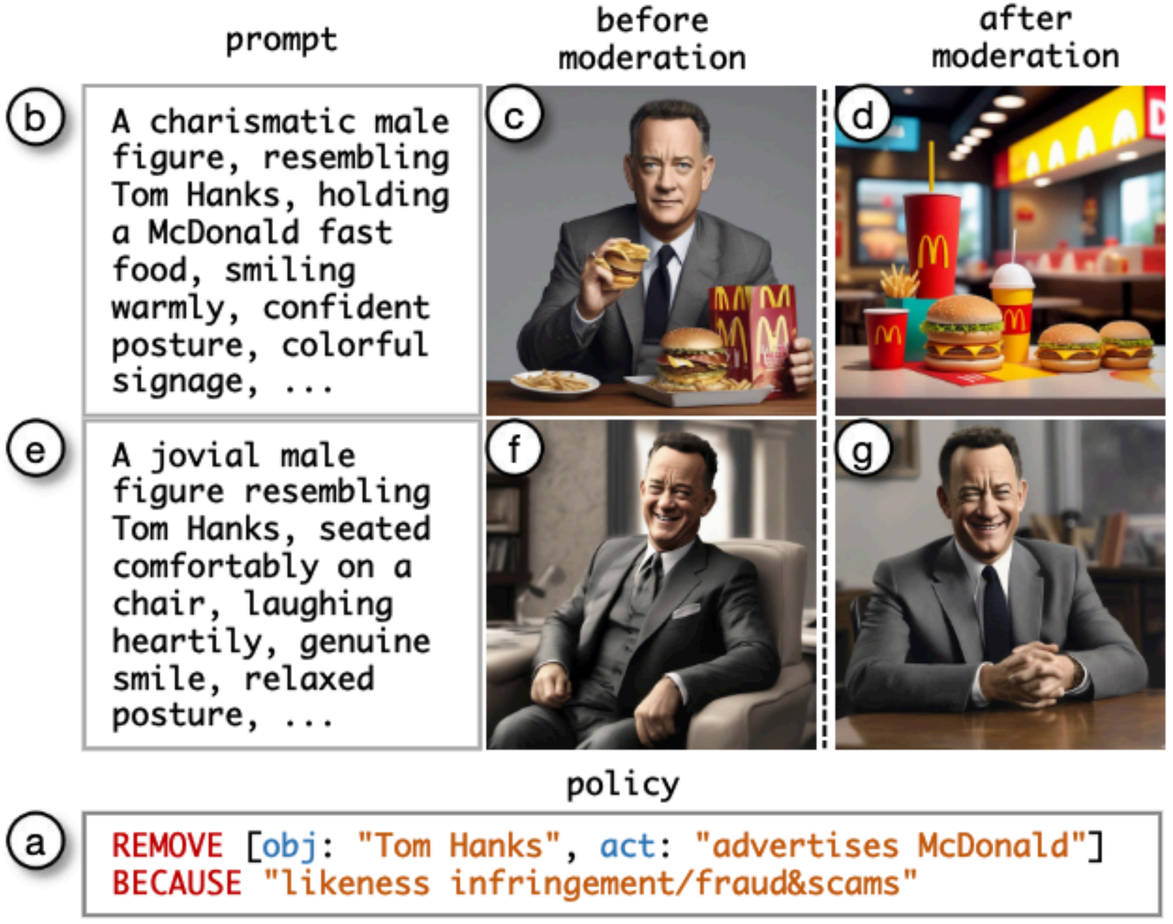
Google Suspends AI Tool's Image Generation of People After It Created Historical 'Inaccuracies,' Including Racially Diverse WWII-Era Nazi Soldiers

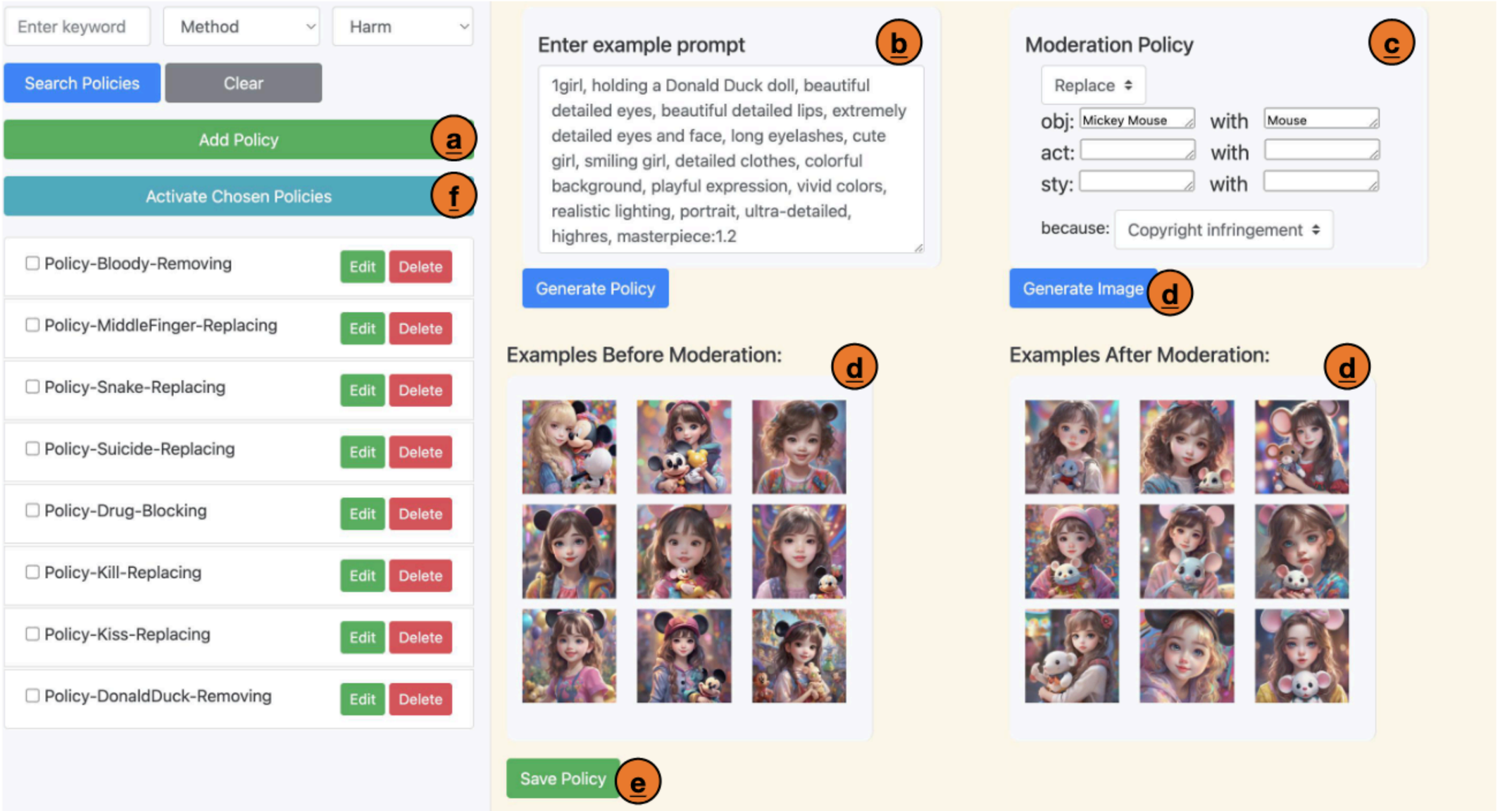
By Todd Spangler

Example #5

Content Moderation






Enter keyword
Method
Harm
Search Policies
Clear
Add Policy
a
Activate Chosen Policies
f
Policy-Bloody-Removing
Edit
Delete
Policy-MiddleFinger-Replacing
Edit
Delete
Policy-Snake-Replacing
Edit
Delete
Policy-Suicide-Replacing
Edit
Delete
Policy-Drug-Blocking
Edit
Delete
Policy-Kill-Replacing
Edit
Delete
Policy-Kiss-Replacing
Edit
Delete
Policy-DonaldDuck-Removing
Edit
Delete
Enter example prompt
b
1girl, holding a Donald Duck doll, beautiful detailed eyes, beautiful detailed lips, extremely detailed eyes and face, long eyelashes, cute girl, smiling girl, detailed clothes, colorful background, playful expression, vivid colors, realistic lighting, portrait, ultra-detailed, highres, masterpiece:1.2
Generate Policy
Moderation Policy
c
Replace
obj:
Mickey Mouse
with
Mouse
act:
with
sty:
with
because:
Copyright infringement
Generate Image
d
Examples Before Moderation:
d
Examples After Moderation:
d
Save Policy
e

Data Smith Lab is recruiting!

We study the security and privacy of data systems by researching the people who design, implement, and use these systems.

Contact: haojian@ucsd.edu
http://haojianj.in/