



PRIVACY CON

FEDERAL TRADE COMMISSION

📍 DC // 1.12.17

Opening Remarks

Chairwoman Edith Ramirez

Session 1: Internet of Things and Big Data

A Smart Home is No Castle: Privacy Vulnerabilities of Encrypted IoT Traffic

Noah Apthorpe, Dillon Reisman, Nick Feamster

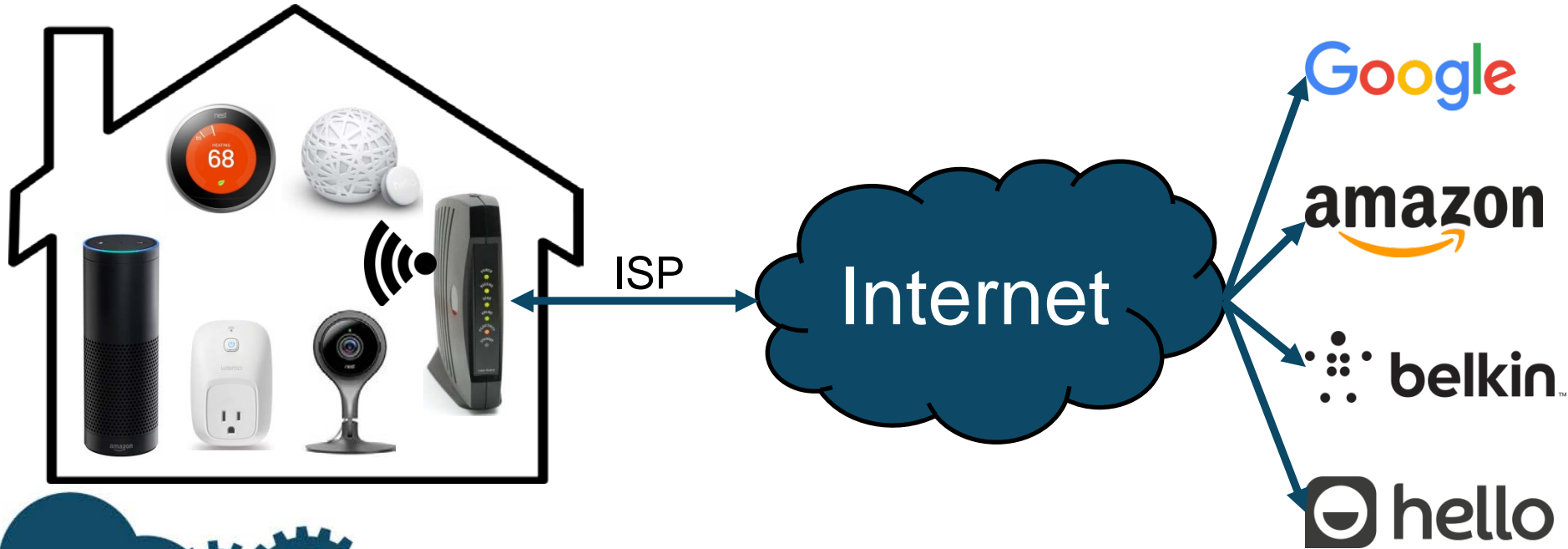
Center for Information Technology Policy, Princeton University

This research was funded by the Department of Defense through the National Defense Science & Engineering Graduate Fellowship (NDSEG) Program, a Google Faculty Research Award, and the National Science Foundation

Acknowledgements

- Arvind Narayanan, Princeton CITP
- Nina Taft, Google Inc.
- Alex Yue, Princeton CITP
- Caio Burgardt, Princeton CITP & Federal University of Pernambuco

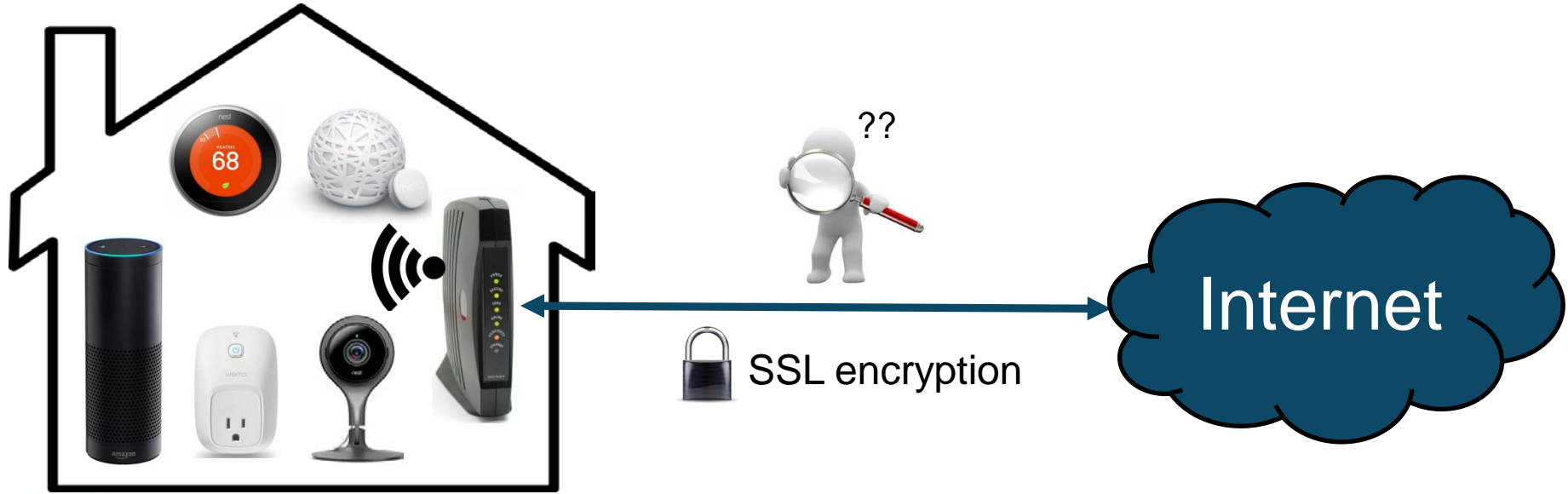
What is a smart home?



Smart home privacy

- Smart home Internet traffic can contain sensitive consumer information
 - Physical presence in home
 - Sleeping habits
 - Media consumption
 - Appliance usage

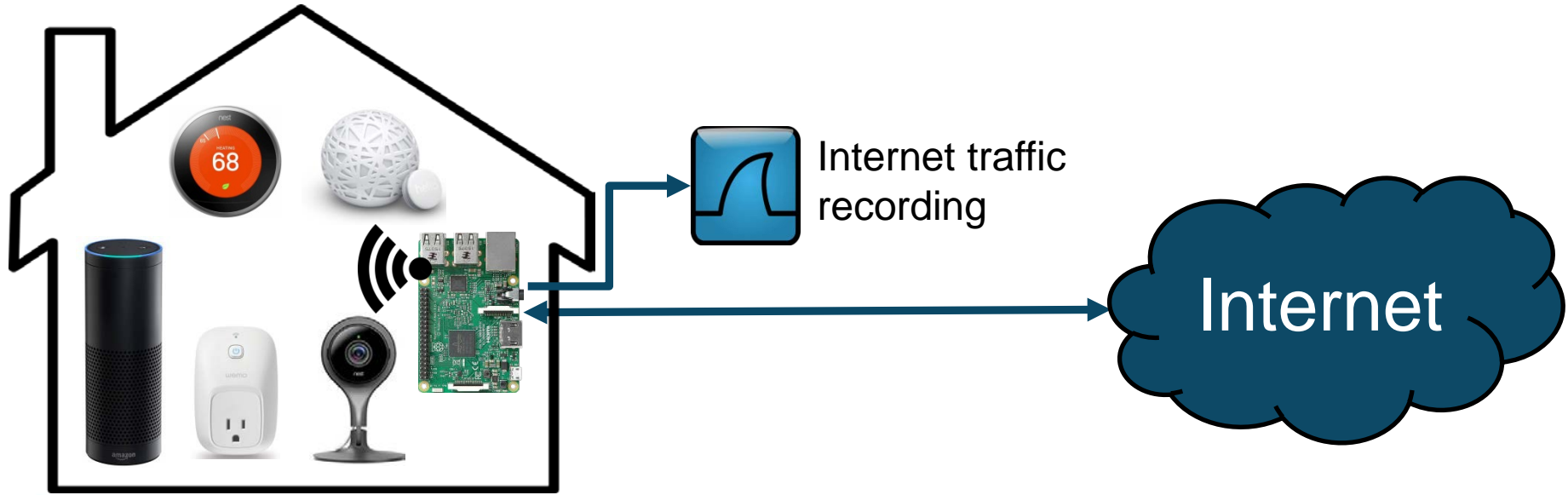
Smart home privacy



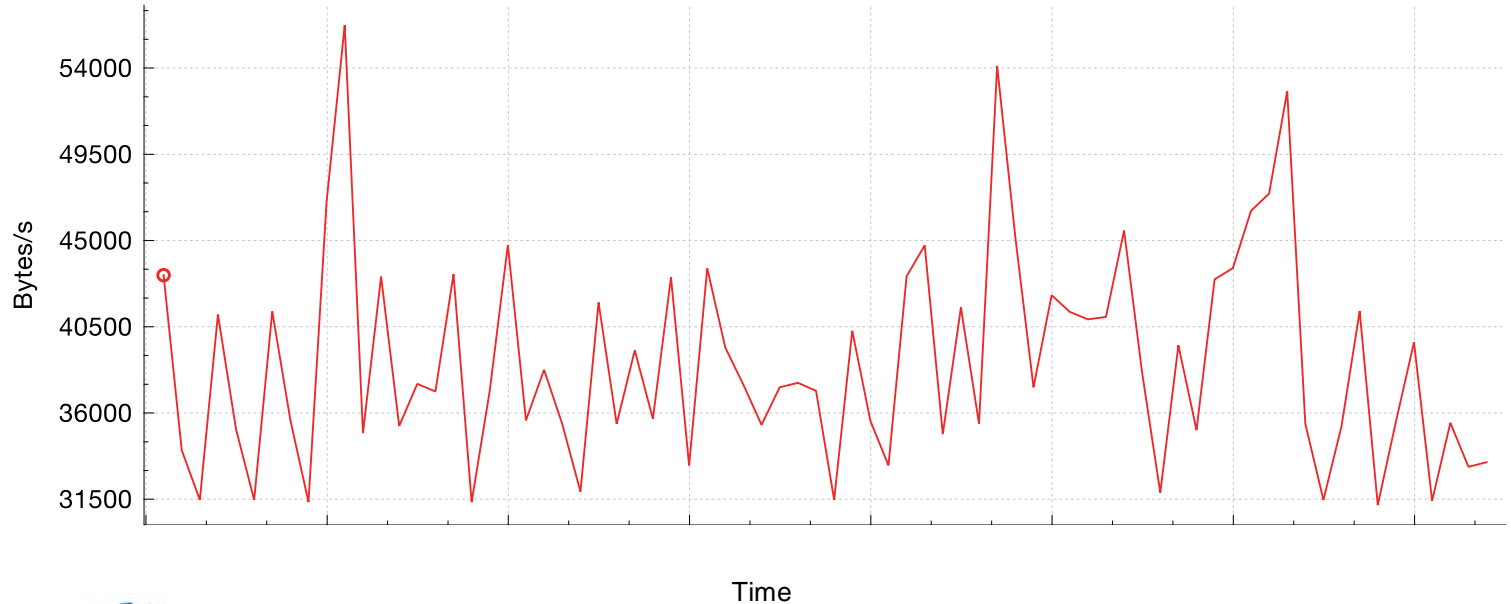
Smart home privacy

Smart home Internet traffic patterns reveal consumers' private in-home behaviors
even when traffic is encrypted

Smart home laboratory

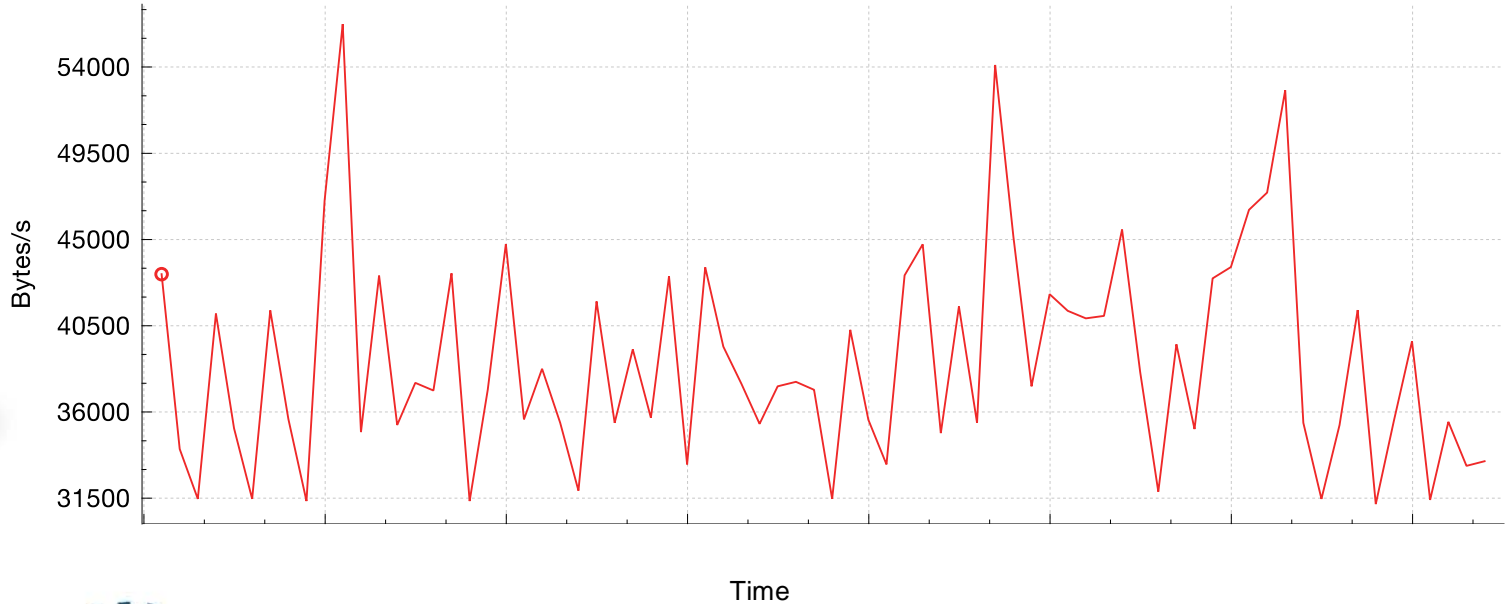


1. Obtain Internet traffic from device



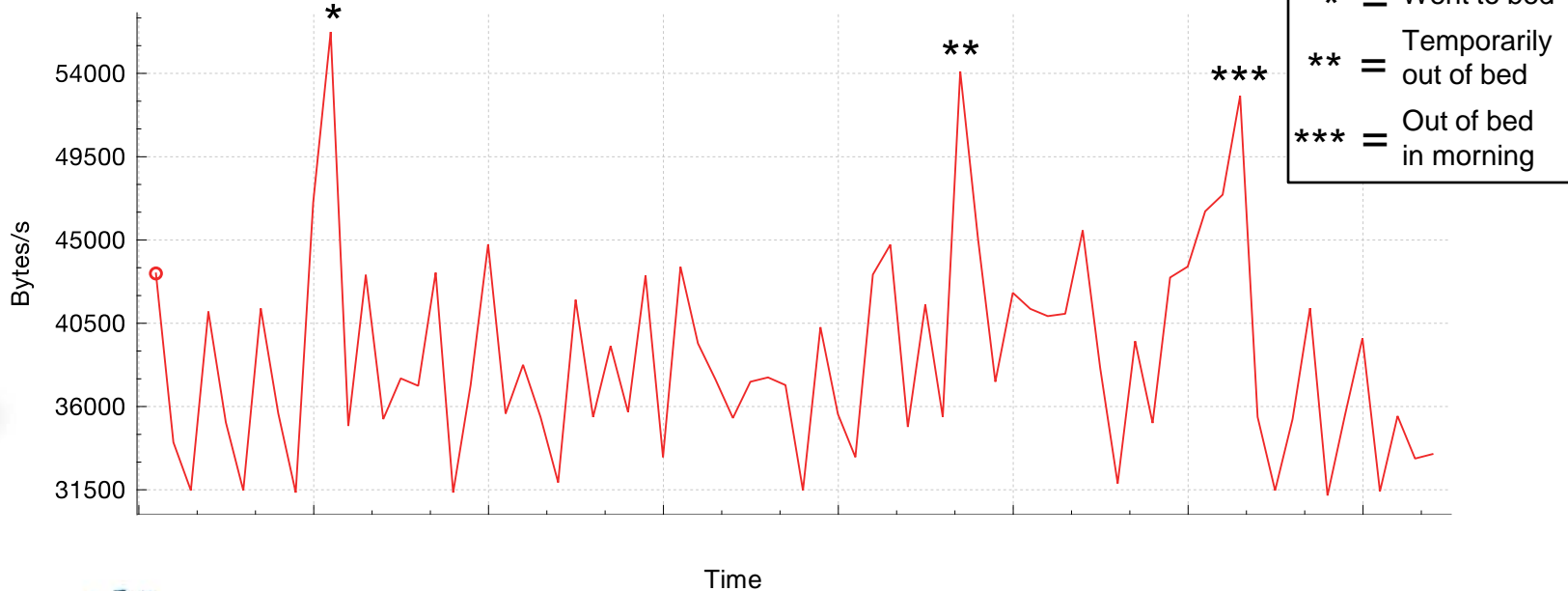
2. Identify device

Sleep monitor

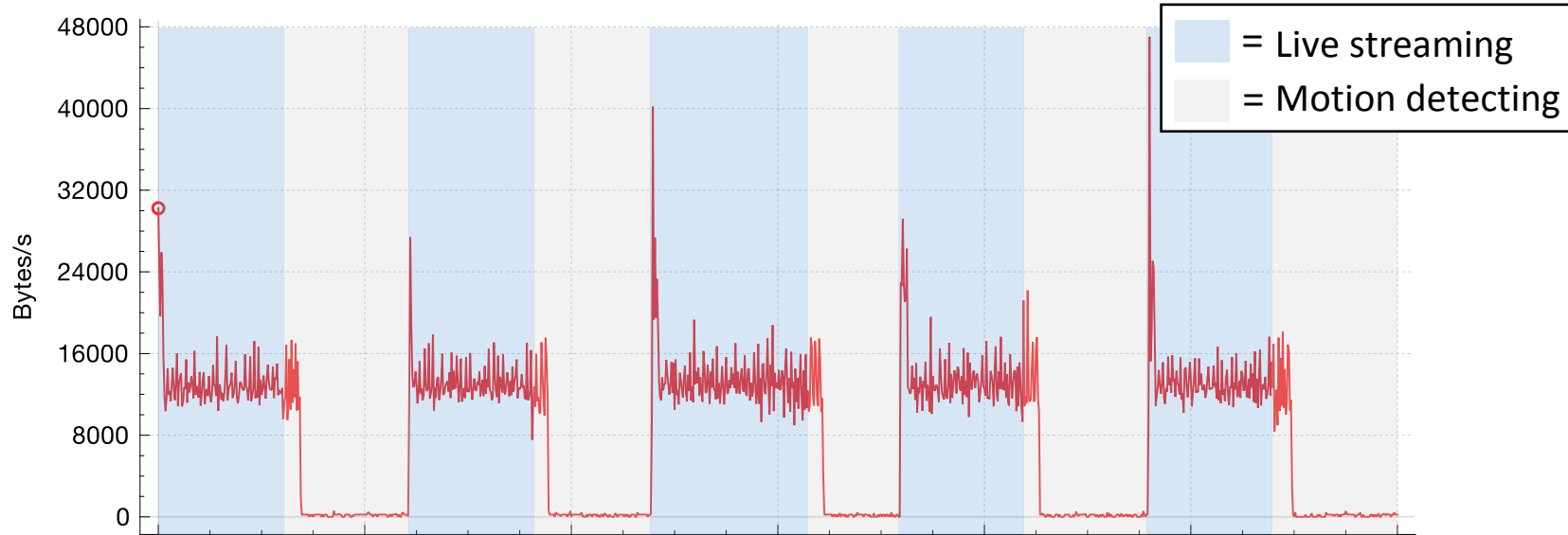


3. Infer behaviors from traffic patterns

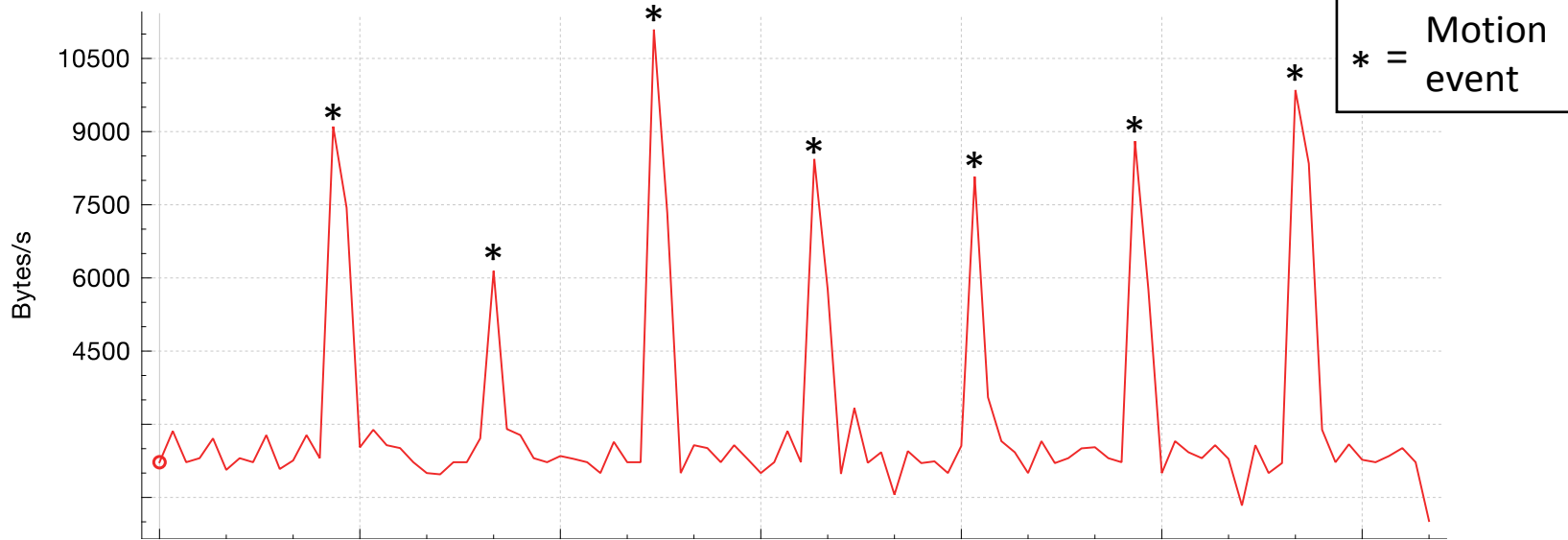
Sleep monitor



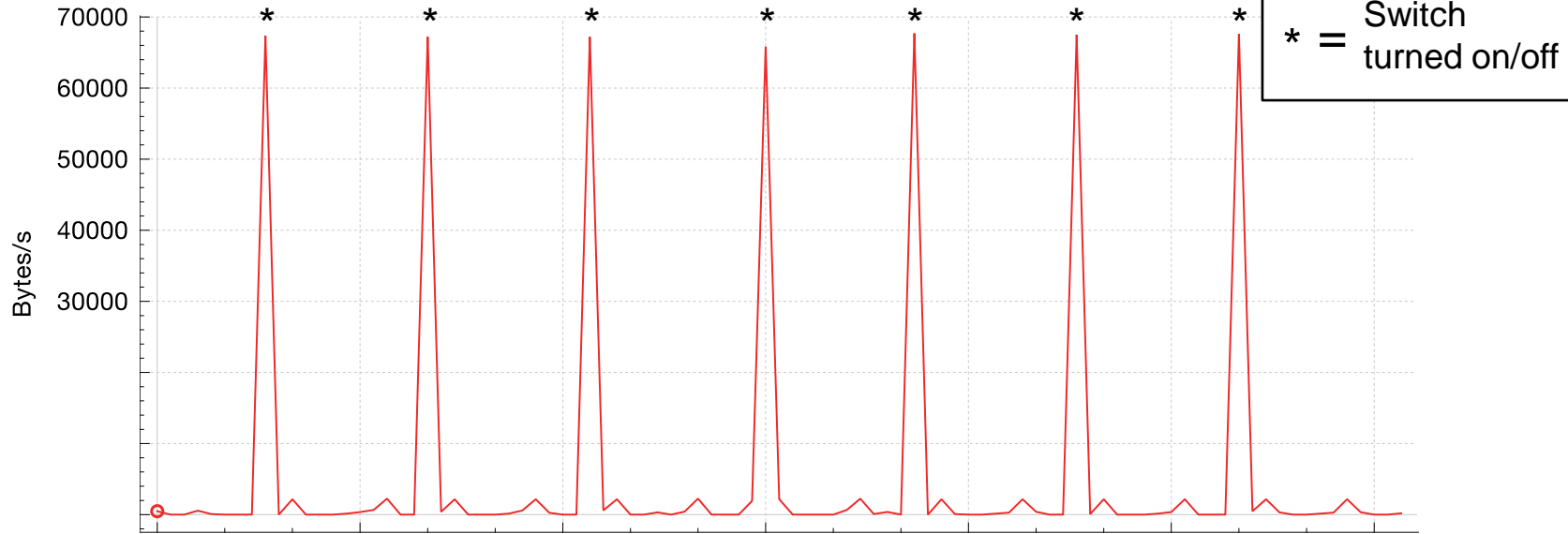
Security camera monitoring



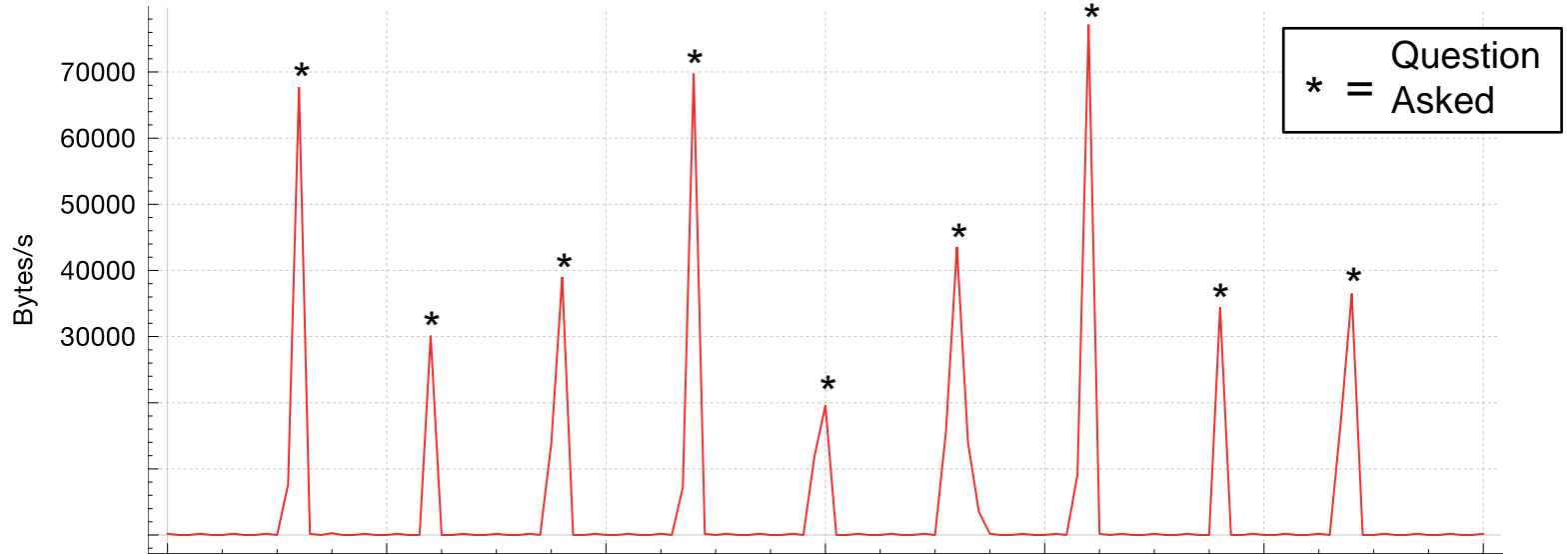
Presence of motion in home



Power to physical appliance



Interactions with personal assistant



Future questions

- How widespread is this privacy risk?
- Can we design privacy preservation methods that address metadata?
 - e.g. probabilistic traffic injection

Conclusion

- Encryption alone does not provide adequate privacy protection for smart home IoT devices
- Link to paper:
<http://datworkshop.org/papers/dat16-final37.pdf>

Cross-App Tracking via Nearby Bluetooth Devices

Aleksandra Korolova

University of Southern California

Joint work with Vinod Sharma, USC

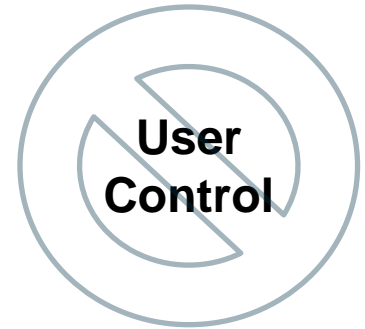
Bluetooth-enabled Devices Everywhere



What are the Privacy Implications?

New channel for:

- Profiling the user
- Tracking across apps



The Bluetooth LE Protocol

Devices transmit info	Example
MAC address	A4:77:32:4E:43:92
Name	Joe's Chromecast
Manufacturer data	16 bit id
Service UUIDs	0000fea0-0000-1000-8000-00805f9b34fb

Frequency: Every 20ms-10s

Range: up to 100m

App Developers

Can request info of all nearby devices from OS

- Unlimited frequency
- User permission not needed in iOS & Android 5
 - iOS modifies MAC addresses
 - Android 6 requires location permission

How does BLE enable Profiling?

interest

users
name



Dan Jo's FitBit

door
lock type



Kevo

Livingroom
size



[TV] Samsung 9 Series (65)

Income

parents of
infant



mamaRoo

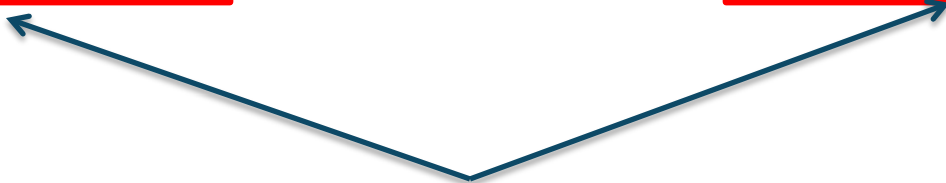
How does BLE enable Tracking?

APP 1

USER 1	USER 2
AA:BB:CC:DD:EE	FF:FF:FF:FF:FF
A1:B1:C1:D1:E1	55:55:55:55:55
AA:AA:AA:AA:AA	BB:BB:BB:BB:BB

APP 2

USER X	USER Y
AA:BB:CC:DD:EE	CC:CC:CC:CC:CC
A1:B1:C1:D1:E1	66:66:66:66:66
AA:AA:AA:AA:AA	DB:DB:DB:DB:DB



Likely the same user

Our Study

70 volunteers collect nearby Bluetooth-enabled device data every 10 minutes for 1 week in June 2016

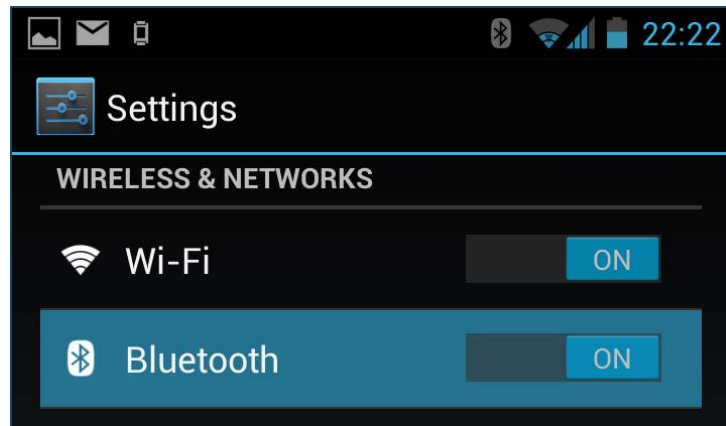
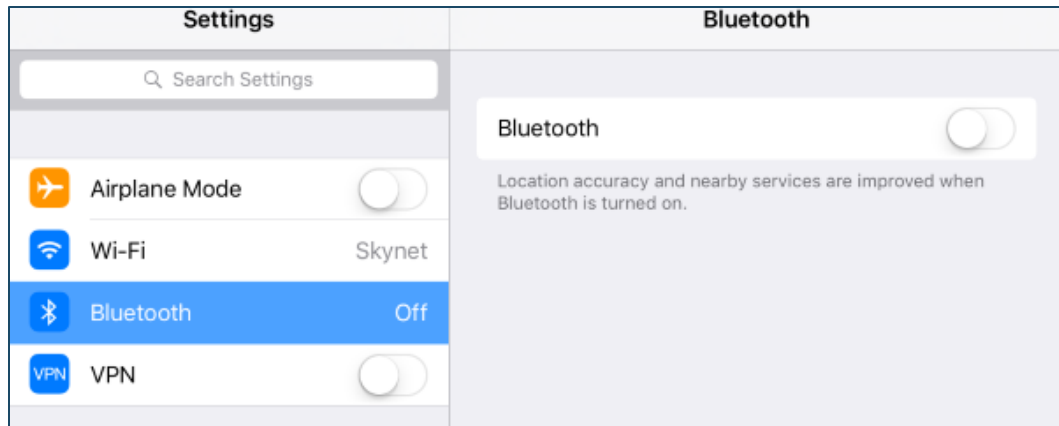
Findings:

- **1,000+** distinct device names
- **87%** uniquely identifiable by apps used every 5 hours
- **60%** uniquely identifiable by apps used once a day

Is BLE-based Profiling & Tracking Happening?

- Hard to tell, which is a problem in itself!
- What we know:
 - increasing # of apps declaring Bluetooth use
 - some apps access Bluetooth quite often
 - nothing stops them from using obtained info for profiling & tracking

Controls Available to Individuals



Device-level Bluetooth ON / OFF

- Hardly a meaningful choice long-term

Conclusions – Changes are Needed

- I. Profiling & Tracking using nearby BLE devices feasible

- I. Can increase privacy without hurting functionality, but changes needed by:
 - Bluetooth Special Interest Group
 - Apple, Google
 - Device manufacturers

A role for FTC?

Cross-App Tracking via Nearby Bluetooth Devices

Aleksandra Korolova

University of Southern California

Study details: <http://bit.ly/BluetoothPrivacy>

Joint work with Vinod Sharma, USC

Rating Products & Services for Privacy, Security & Data Practices

Maria Rerecich
Consumer Reports

This research was funded by the Ford Foundation



PRIVACYCON

Testing Philosophy

- Comparative Testing -> Informed choice
- Defined protocols and procedures
- Consumer-focused
- Companies compete
- Products improve
- Industry standards and regulations advance

Developing a Standard: Why Now?

- Shift from hardware-only to software-enabled and connected, i.e. Internet of Things
- Uncharted territory for consumers
- No easy way to navigate the privacy and security of this new digital world
- Need for a consistent, accessible standard to measure these products

Organizing Principles

- Security – “Is it safe?”
- Privacy – “Is it private?”
- Governance and Compliance – “Are the policies strong for consumers?”
- Ownership – “Is it mine?”

Example

- Criterion: The product is protected from known software vulnerabilities that present a danger from attackers.
- Indicator: The software is secure against known bugs and types of attacks.
- Procedure Overview: Launch activities from user interface. Monitor communication to/from device.

Next Steps

- Create an openly sourced digital standard that can be used to hold manufacturers and providers accountable for how they manage consumers' privacy, security, and data.
- To provide any comments or feedback, please email us at externalrelations@cr.consumer.org

A User-Centered Perspective on Algorithmic Personalization

Alethea Lange, Rena Coen, Emily Paul, Pavel Vanegas, & G.S. Hans
Center for Democracy & Technology
UC Berkeley School of Information

This research was funded by the Berkeley Center for Technology, Society, and Policy and the Berkeley Center for Long-Term Cybersecurity

Personalization Practices

The screenshot shows the Staples.com website with a personalized price for a Swingline Standard Stapler Value Pack. The price is \$11.49, which is significantly lower than the \$15.79 price shown for a similar product elsewhere. The article text explains that this is due to personalization based on user information.

STAPLES

THE WALL STREET JOURNAL

Subscribe | Sign In

KEYWORDS: Yelp, Google Hold Printers to Fix Governments | Live-Video Search Coming to Periscope

What They Know

Websites Vary Prices, Deals Based on Users' Information

By JENNIFER VALENTINO-DEVRIES, JEREMY SINGER-VINE and ASHKAN SOLTANI
December 24, 2012

It was the same Swingline stapler, on the same [Staples.com](#) website. But for Kim Wamble, the price was \$15.79, while the price on Trude Frizzell's screen, just a few miles away, was \$14.29.

Swingline Standard Stapler Value Pack, 15 Sheets, Black, Premium Staples and Remover Included
\$11.49

The screenshot shows the ProPublica website header. The logo features a magnifying glass over the word 'PRO'. The tagline is 'Journalism in the Public Interest'. There is a search bar and a 'Receive our top stories' button.

PROPUBLICA | Journalism in the Public Interest

Home | Investigations | Data | MuckReads | Get Involved | About Us

Search ProPublica

HUD Has 'Serious Concerns' About Facebook's Ethnic Targeting

Federal officials are taking a close look at a sales practice that allows advertisers on the social network to include or exclude people who have an "affinity" with specific ethnic groups.

by *Stephen Engelberg*
ProPublica, Nov. 7, 2016, 3:27 p.m.

The screenshot shows the Fandango website with movie listings for 'Rogue One: A Star Wars Story' and 'Sing'. The 'Sing' listing includes a 'SING' logo and the text 'Drama film...'.

movie showtimes

All Shopping Maps News

Movies playing near Washington

Rogue One: A Star Wars Story
Science ficti...

Sing
Drama film/...

Movie Times and Movie Theater
[www.fandango.com/washington_dc_mo](#)
Looking for local movie times and movie theaters?

Fandango: Movie Tickets & More
[www.fandango.com/](#)

Buy movie tickets in advance, find movie times, watch trailer
Fandango.

Rogue One: A Star Wars Story - Now Playing - Fantastic Beas

The screenshot shows a Facebook advertisement for a movie theater. The ad features a large blue thumbs-up icon and the text 'facebook 1601 Willow Road'. On the right side, there is a sidebar with social media sharing options: 'Follow ProPublica', 'Twitter', 'Podcast', and 'Updates by email'. There is also a 'SUBSCRIBE' button.

Follow ProPublica

Twitter

Podcast

Updates by email

Email address

Zip-code

SUBSCRIBE

From left, Aldis Hodge, Neil Brown Jr, Jason Mitchell, O'Shea Jackson Jr, and Corey Hawkins in a scene from the film, *Straight Outta Compton*. Photograph: [Jaimie Trueblood/AP](#)



Research Design

DOMAIN

Targeted Advertising

Filtered Search Results

Differential Retail Pricing

DATA TYPE

Personal Information

City/Town of Residence

Gender

Household Income

Race

SOURCE

Provided

Accurately Inferred

Inaccurately Inferred

CONTEXT

INFERENCE &
ACCURACY

Research Design

DOMAIN

Targeted Advertising
Filtered Search Results
Differential Retail Pricing

DATA TYPE

Personal Information
City/Town of Residence
Gender
Household Income
Race

SOURCE

Provided
Accurately
Inferred
Inaccurately
Inferred

*You are reading an article on a website. The **ad** is shown to you based on your **race** which was **inferred** from the webpages you visit and is **accurate**.*



Survey Instrument



Berkeley
UNIVERSITY OF CALIFORNIA

How often do you use the internet either on a computer or on a mobile device like a smartphone or tablet?

Several times a day
 About once a day
 A few times a week
 A few times a month
 A few times a year
 Never

Valid N = 748

How often do you send or check email?

Several times a day
 About once a day
 A few times a week
 A few times a month
 A few times a year
 Never

How often do you use social media websites?

Several times a day
 About once a day
 A few times a week
 A few times a month
 A few times a year
 Never

How often do you use apps on a mobile device such as a smartphone or tablet?

Several times a day
 About once a day
 A few times a week
 A few times a month
 A few times a year
 Never

Race	N	%
American Indian or Alaska Native	10	1.34%
Asian	70	9.36%
Black or African American	62	8.29%
Hispanic or Latino	50	6.68%
Native Hawaiian or Other Pacific Islander	3	0.40%
White	597	79.81%
Other	9	1.20%

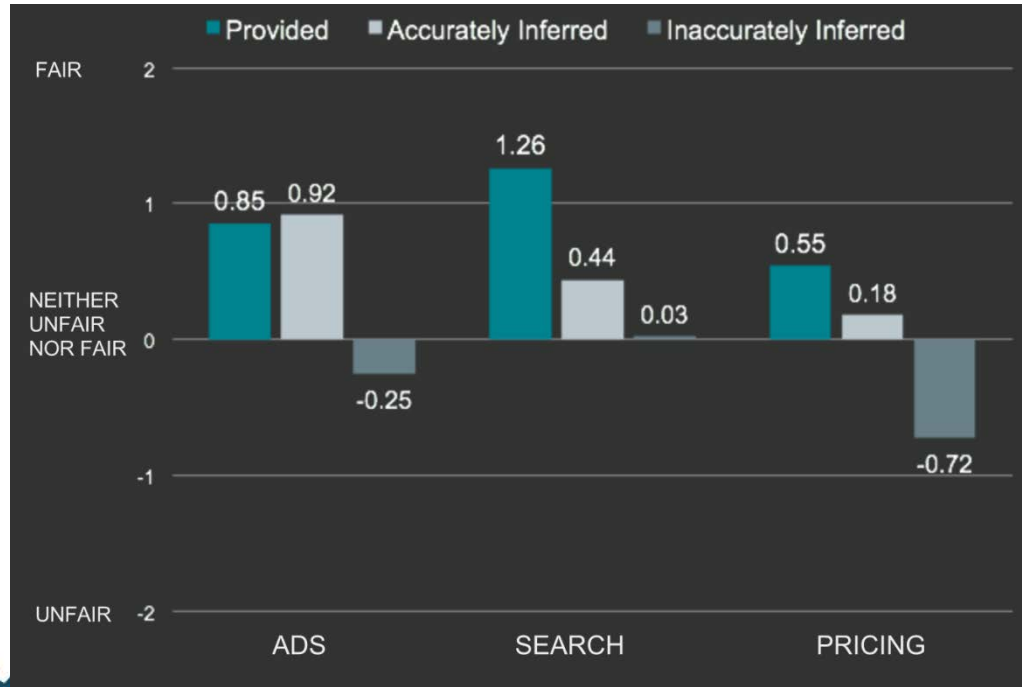
Gender	N	%
Male	347	46.39%
Female	392	52.41%
Female-to-Male transgender	1	0.13%
Male-to-Female transgender	0	0.00%
Genderqueer	5	0.67%
Other	0	0.00%
Prefer not to answer	3	0.40%

Household Income	N	%
Less than \$20,000	118	15.78%
\$20,000 - \$39,999	211	28.21%
\$40,000 - \$59,999	175	23.40%
\$60,000 - \$79,999	106	14.17%
\$80,000 - \$99,999	60	8.02%
\$100,000 +	77	10.29%

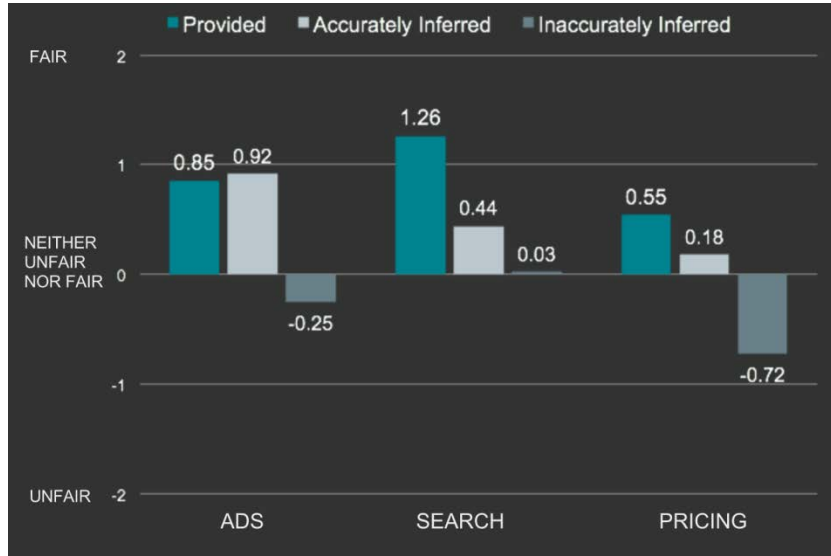
Age	N	%
18-33	406	54.28%
34-49	235	31.42%
50-68	95	12.70%
69 and older	11	1.47%

Median Age = 33

City or Town of Residence



City or Town of Residence

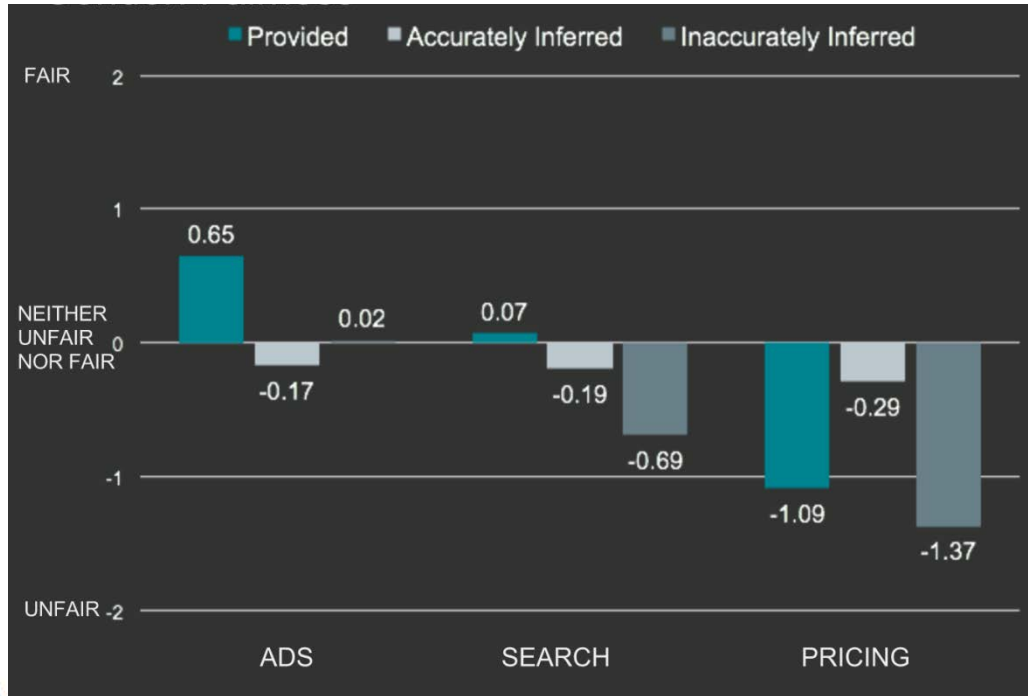


“Getting an **ad** about a product or store in my town is perfectly acceptable and beneficial to me.”

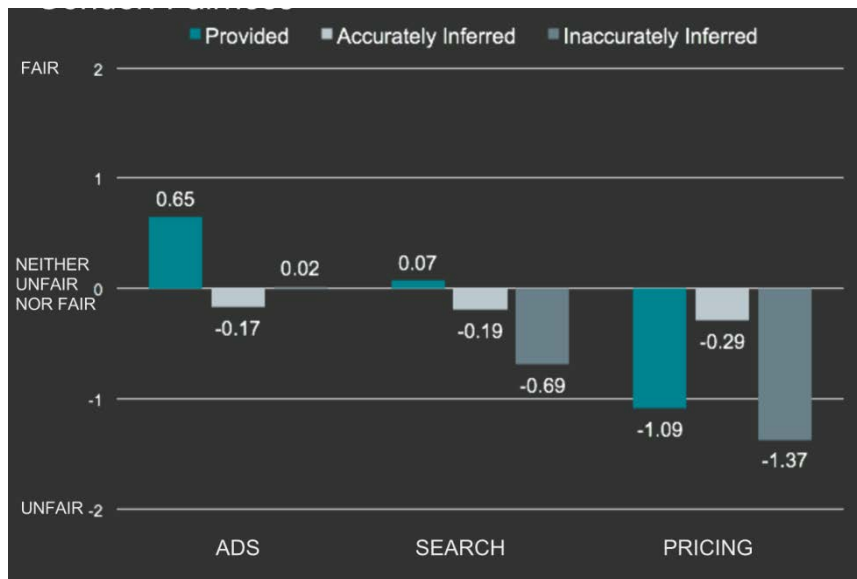
“I would find this acceptable for some things. If I was **searching** for a book or a movie plot . . . it wouldn't be helpful, but if I wanted the weather or a nearby restaurant, it would save time.”

“My initial reaction is that **price** discrimination by geography is unfair. . . . After further thought, this effectively mimics the physical world where prices in areas with higher costs and typically higher salaries tend to be more.”

Gender



Gender

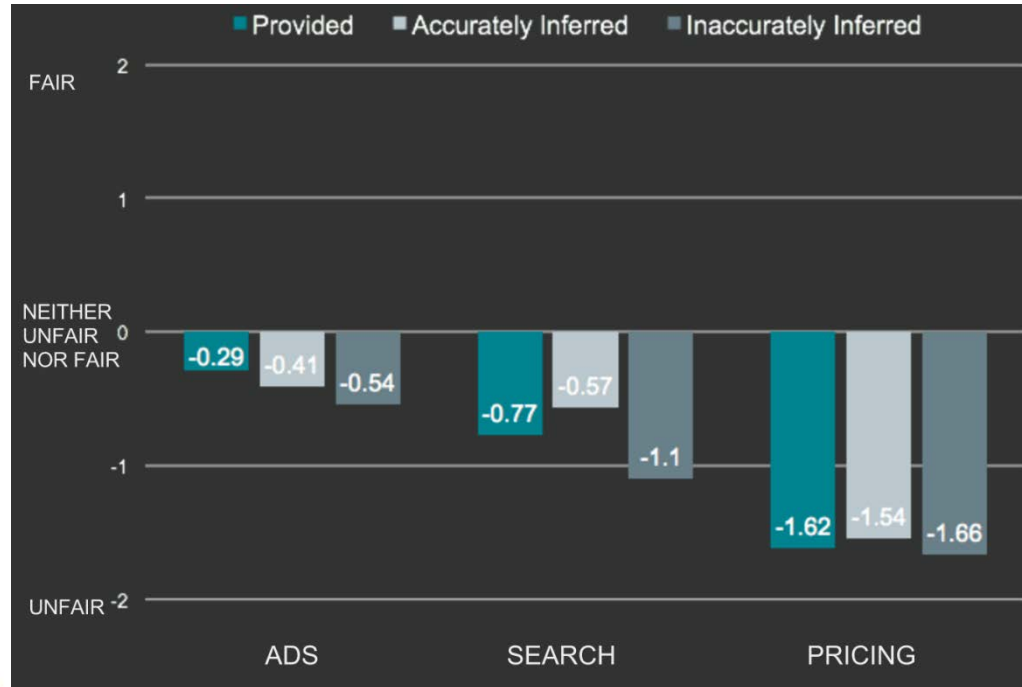


“I don't love the idea of targeted **ads** in general but something based on my gender seems relatively harmless.”

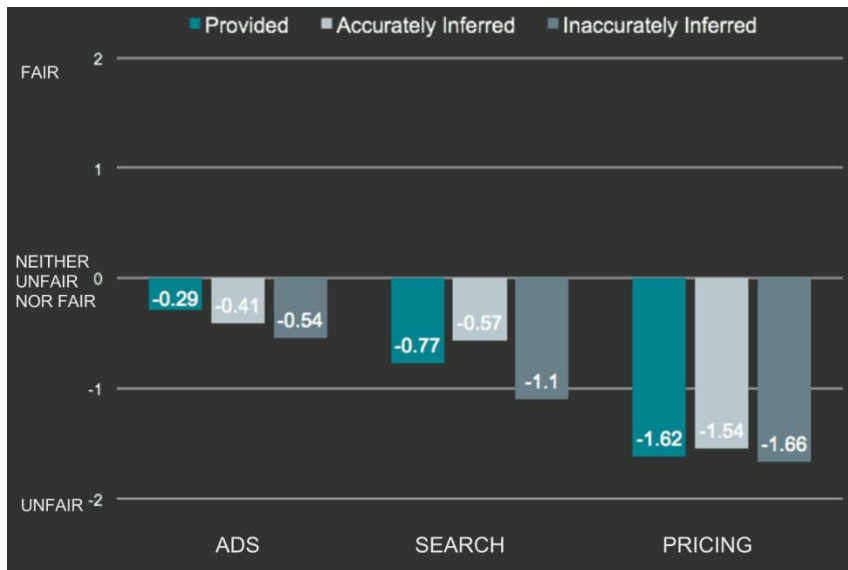
“I don't think my gender provides enough information to improve **[search]** results, and I worry that the filtering will . . . lead to people of different genders having access to different information.”

“That seems very unfair. Products should **cost** the same regardless of gender. . . I don't trust a website that would pull something like this.”

Race



Race



“I cannot imagine a scenario where the **[ad]** presented, using this metric, would be anything more than indicative of stereotypes and racism.”

“I don't like my **search** results being filtered by my race. I feel like I may be missing out on relevant information that I could use.”

“My race shouldn't influence personal product **pricing** regardless of whether the information the company has about me is correct or not”

Key Takeaways

- Reconsider Personalizing in High-Stakes Domains
- Personalization Based on Location Data (City or Town of Residence) is Acceptable Across Contexts
- Data Quality is Meaningful
- Personalized Pricing Should Mirror Offline Practices
- Avoid Personalization Based on Race

Discussion of Session 1

Presenters:

- **Noah Apthorpe** and **Dillon Reisman**, Princeton University
- **Aleksandra Korolova**, University of Southern California
- **Maria Rerecich**, Consumer Reports
- **Alethea Lange**, Center for Democracy & Technology

Moderator:

- **Peder Magee**, Federal Trade Commission

BREAK



PRIVACYCON