Watching IoTs That Watch Us

Danny Y. Huang

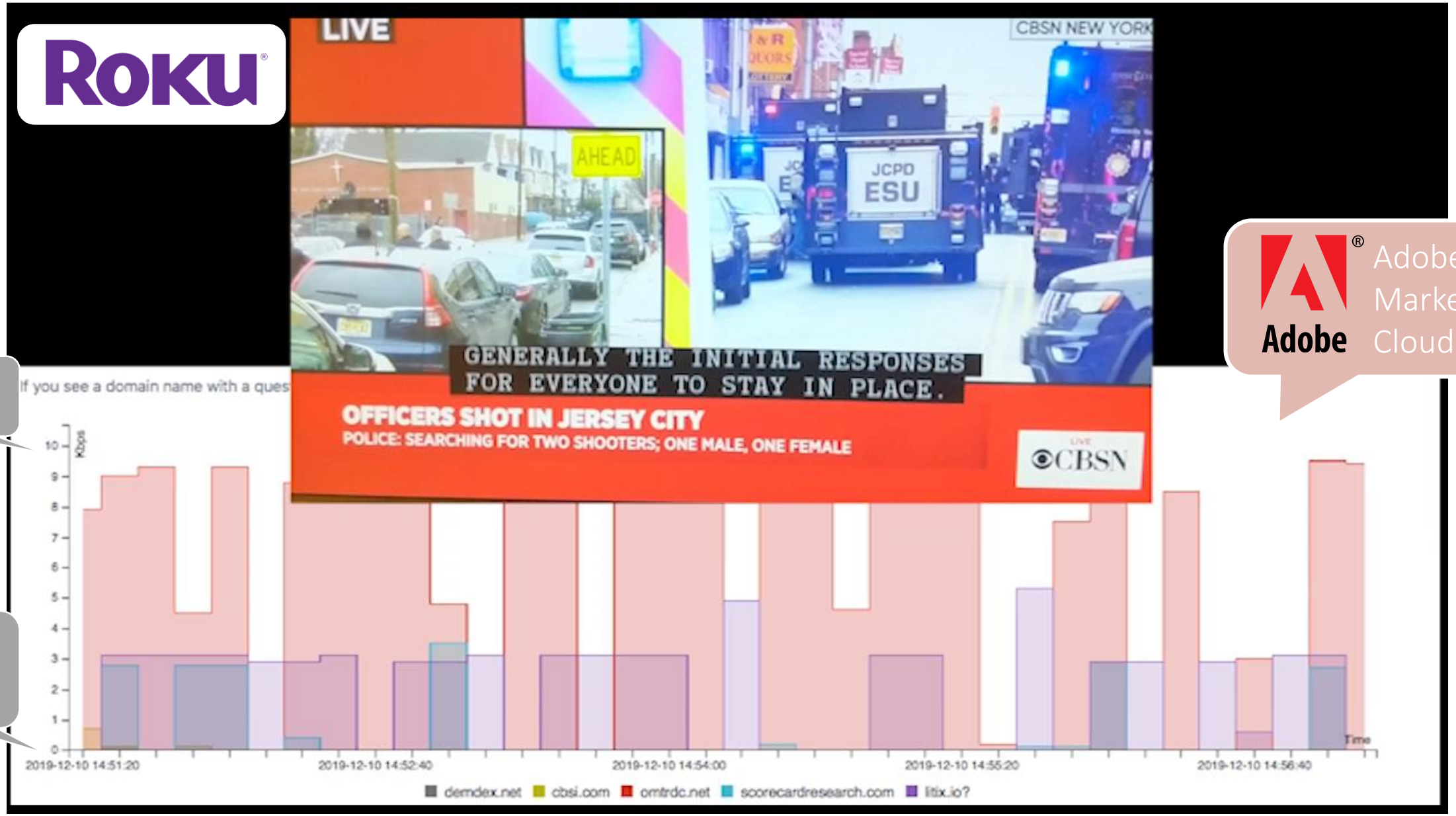
Assistant Professor

NYU TANDON SCHOOL OF ENGINEERING

Video: I’m watching my TV while it is watching me

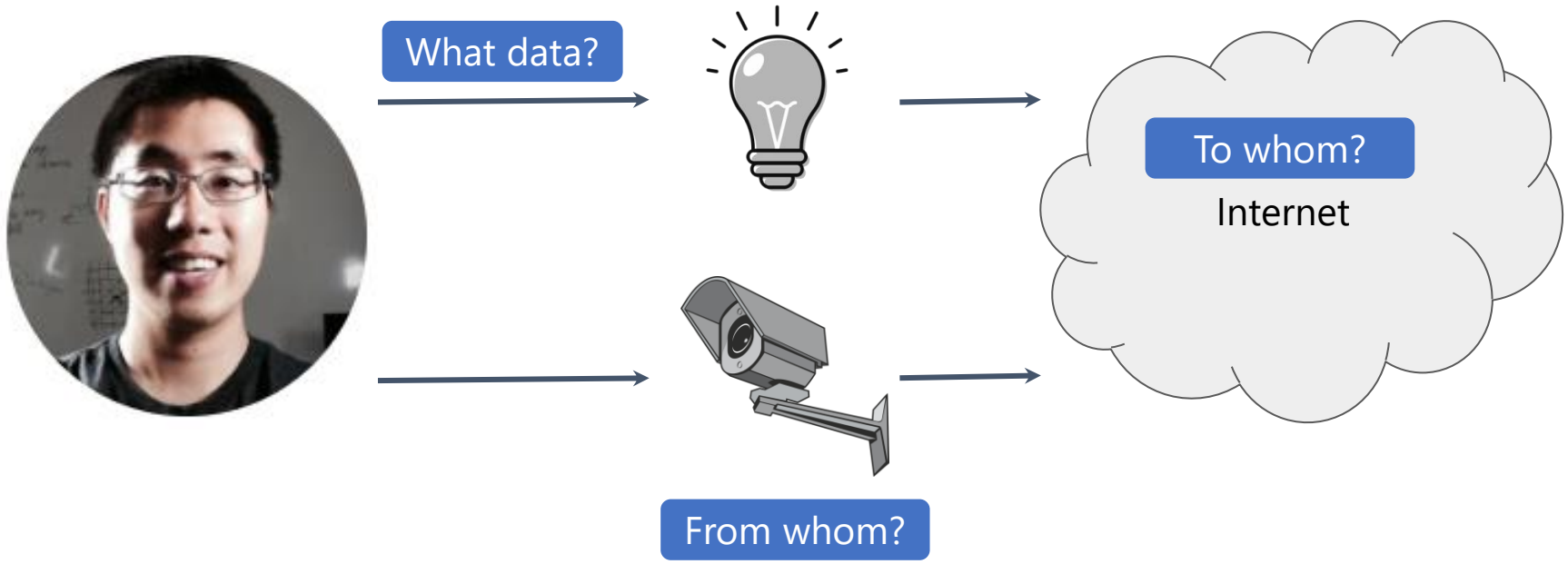
ROKU

Video: I’m watching my TV while it is watching me

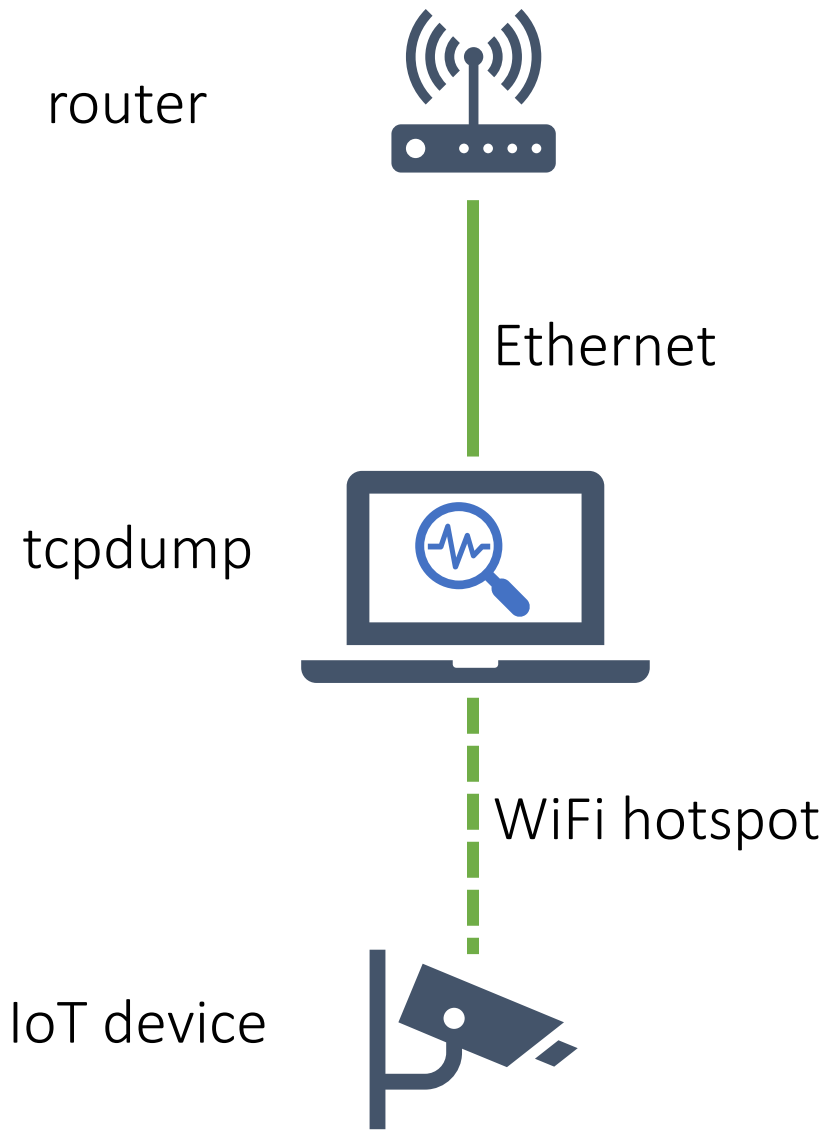


Adobe Marketing Cloud

Many consumers are concerned about IoT security and privacy



Analyzing devices' operational network traffic in lab



Are connections correctly encrypted?

Which Internet service is device talking to?

What data is being sent by device?

Google

小米 xiaomi.com

amazon

alhua TECHNOLOGY

SAMSUNG

HIKVISION

Incentivizing volunteers to collect IoT network traffic at scale

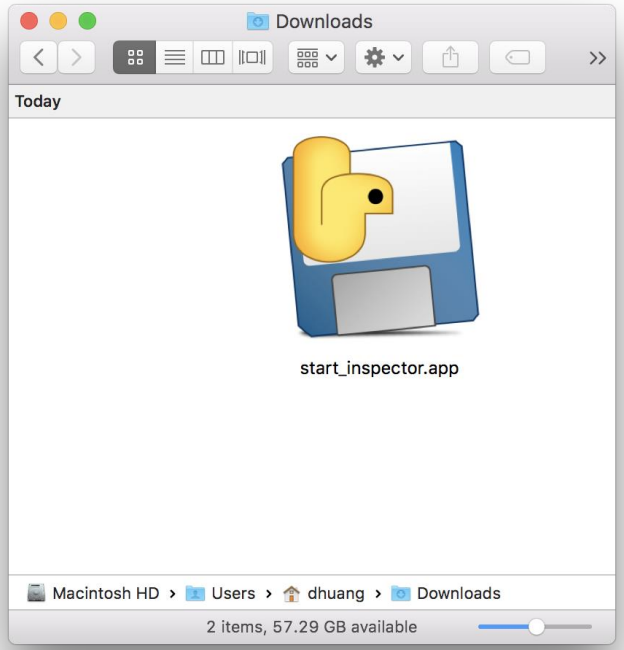
Build software tool that provides volunteers with usable insight on IoT security & privacy with one-click

IoT Inspector: usable system to crowdsource IoT network traffic at scale

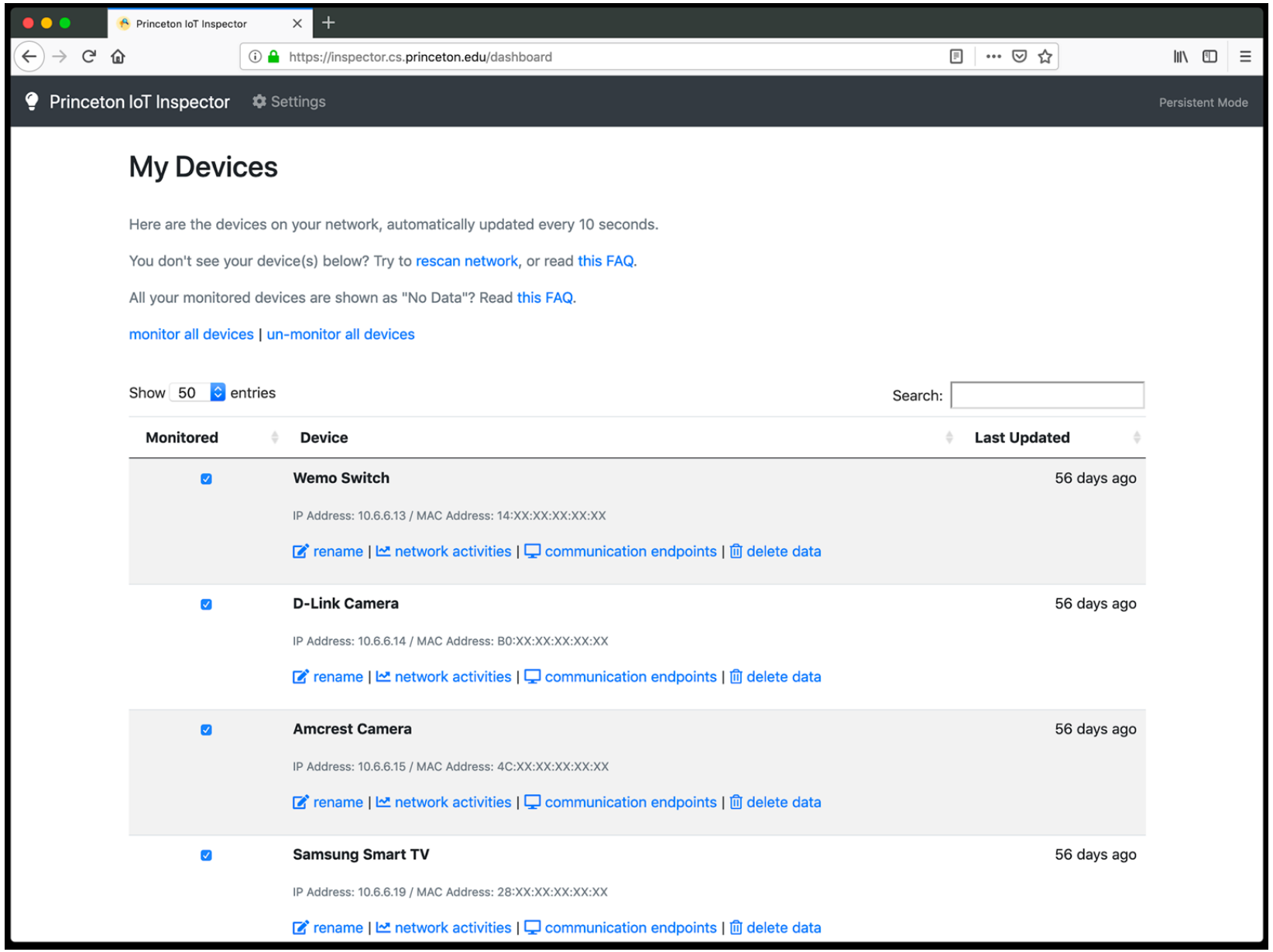
IoT Inspector Client (Windows)
Users view network activities and label devices

IoT Inspector Server
Researchers analyze traffic & device labels

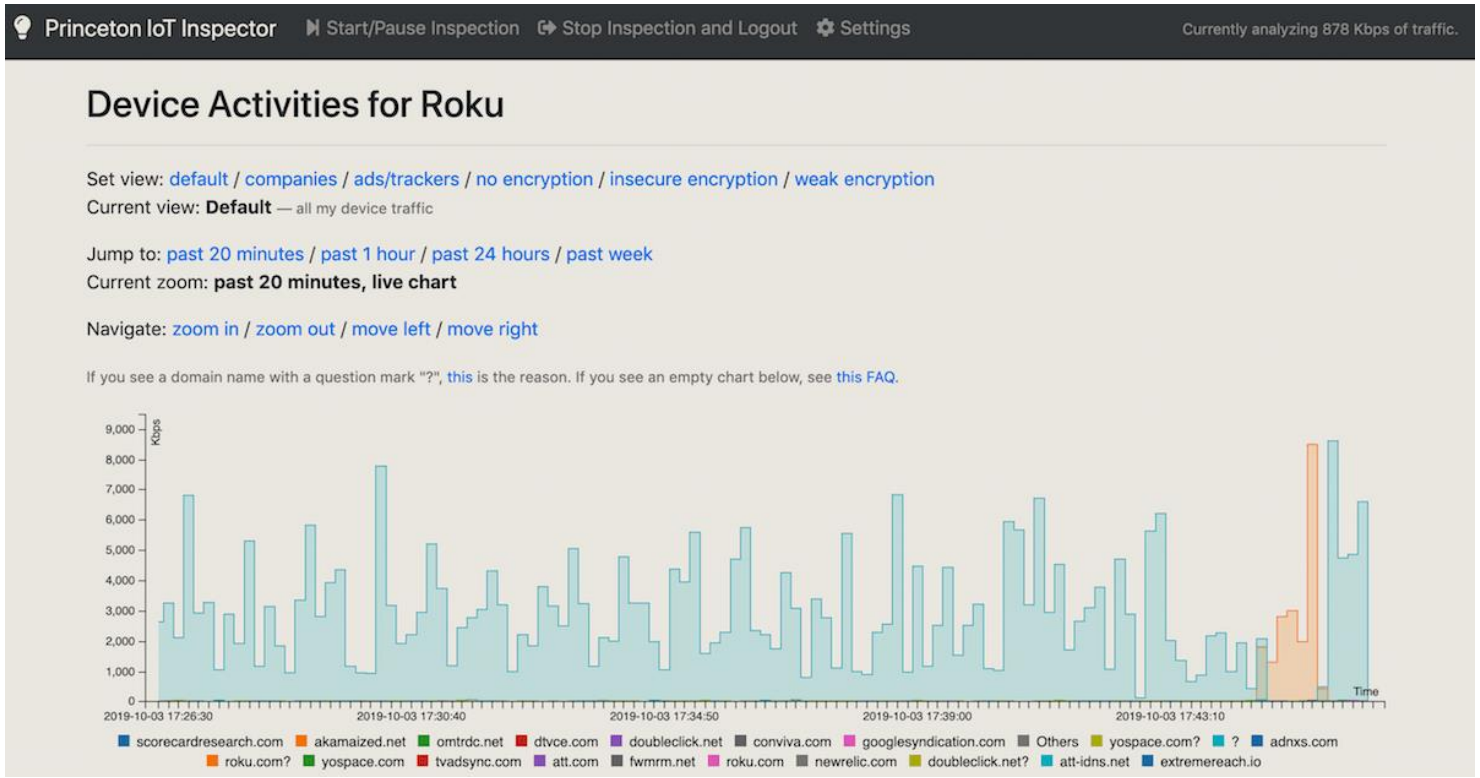
Downloading and running IoT Inspector



Downloading and running IoT Inspector



Insights from an independent user



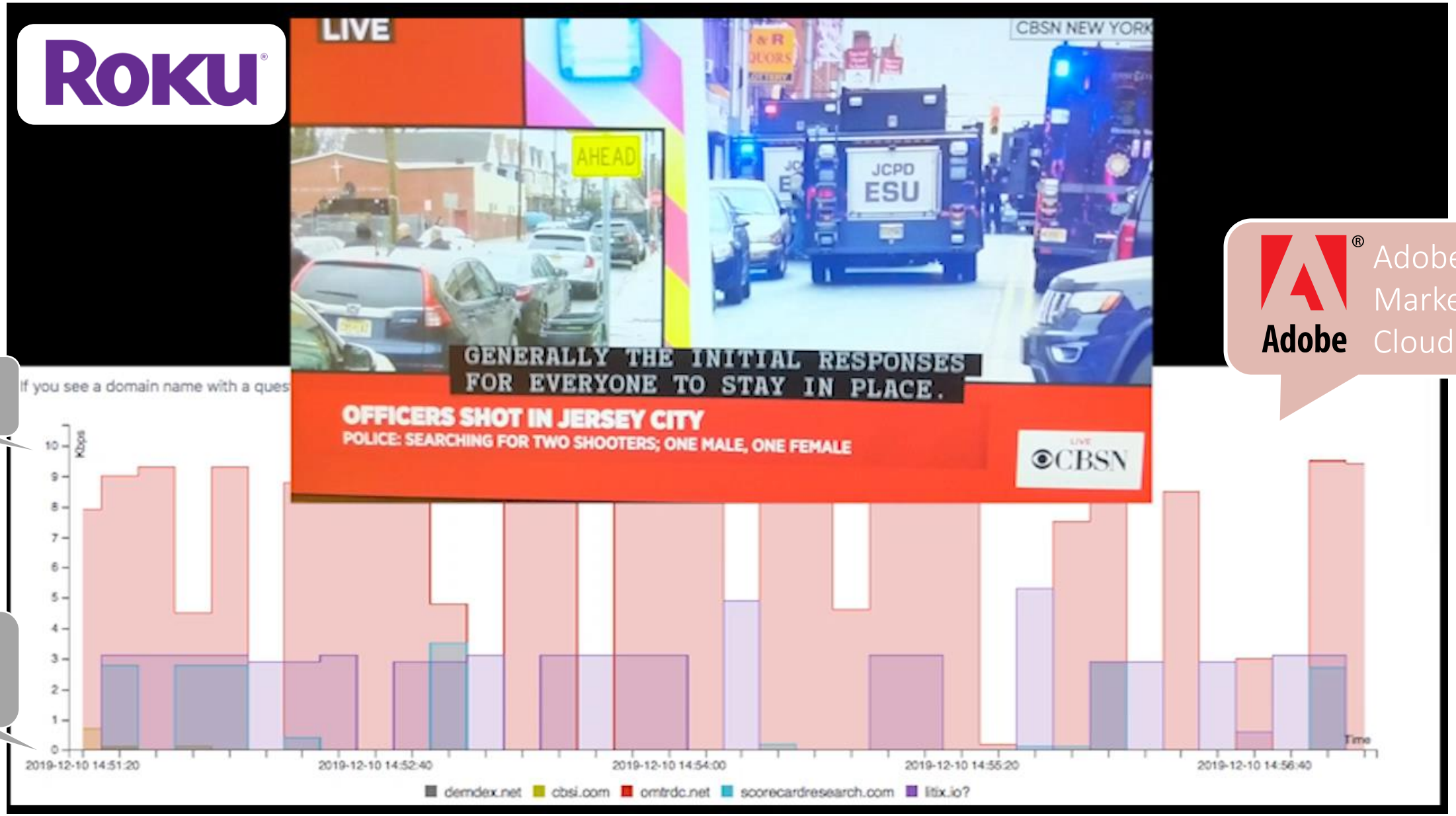
Ira Flatow
Host of Science Friday

"Here is what the **Princeton IoT Inspector** tracked in a 20 minute time span on Ira's Roku."

(October 4, 2019)

Insight – Ira's Roku TV constantly communicated with advertising and tracking services

Video: IoT Inspector showing network activities of Roku TV



Adobe Marketing Cloud

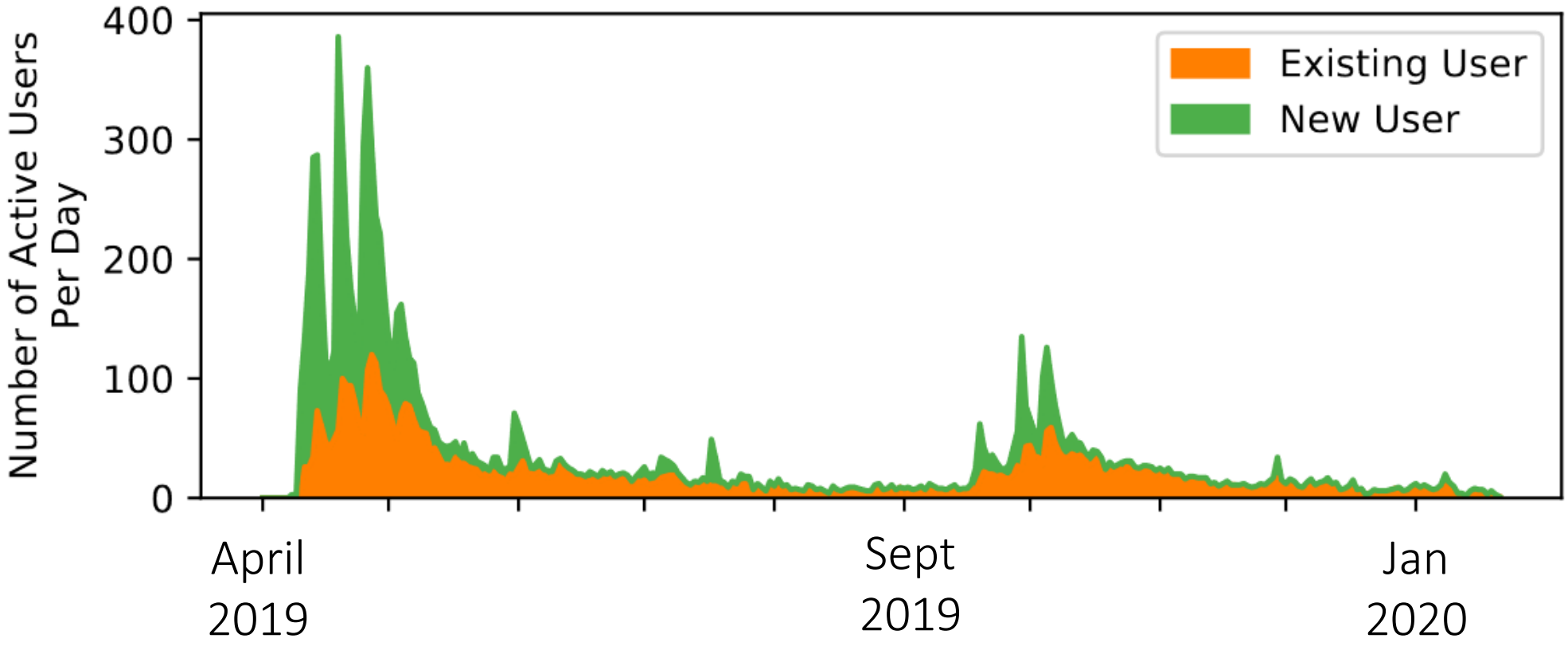
Number of users and devices keep growing

Deployed since April 2019

125 daily active users in the first two months

5,404 users, 54,094 devices

63% users in US time zones, 28% in EU time zones



Snapshot:
April 10, 2019 – Jan 31, 2020

Contributions of IoT Inspector

Tool

5,400+ anonymous users since April ’19

Still gaining users and collecting data

Users

npr

The Washington Post

The New York Times

CR Consumer Reports

NYC Cyber Command

Dataset

54,000+ Internet-connected devices

12,000+ device labels

10+ organizations requesting data access

Collaborators

NC STATE UNIVERSITY

Carnegie Mellon University

ILLINOIS — UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

THE UNIVERSITY OF CHICAGO

Insight

Security: Non-encryption, security vulnerabilities → Device certification? Min security standards?

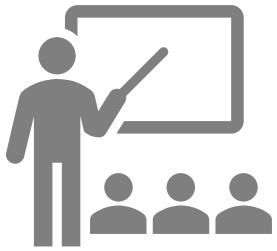
Privacy: Tracking on smart TVs → Violation of COPPA?

Implications

Insight: tracking on smart TVs

417 smart TVs in the dataset

22% of registered domains contacted by these smart TVs are advertising/tracking services, based on Disconnect List



Most TVs talk to what advertising/tracking companies?

A: Google
B: Amazon
C: Facebook
D: Others

Insight: tracking on smart TVs

417 smart TVs in the dataset

22% of registered domains contacted by these smart TVs are advertising/tracking services, based on Disconnect List

doubleclick.net

34%

of smart TVs

scorecardresearch.com

14%

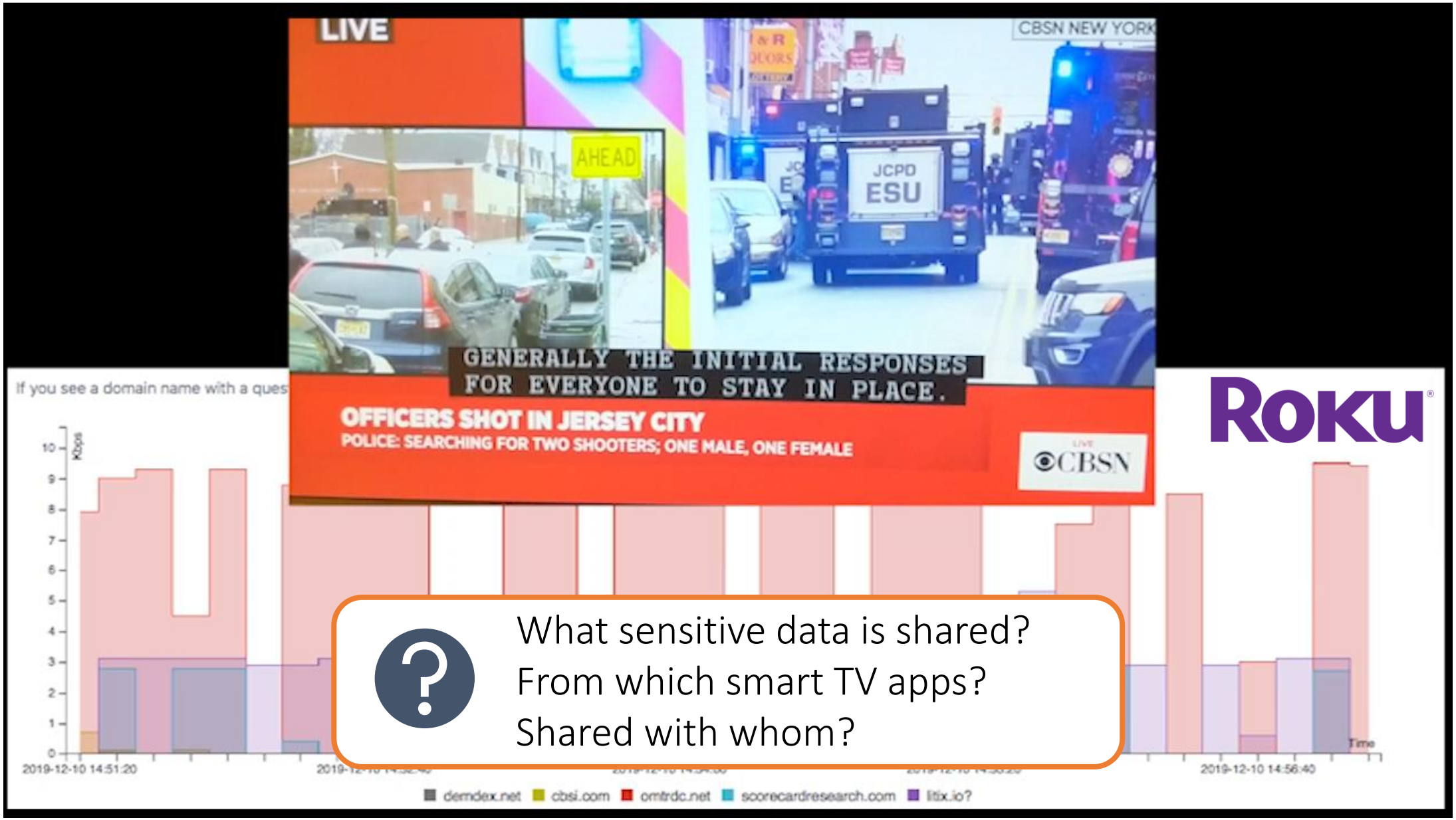
of smart TVs

fwmrm.net

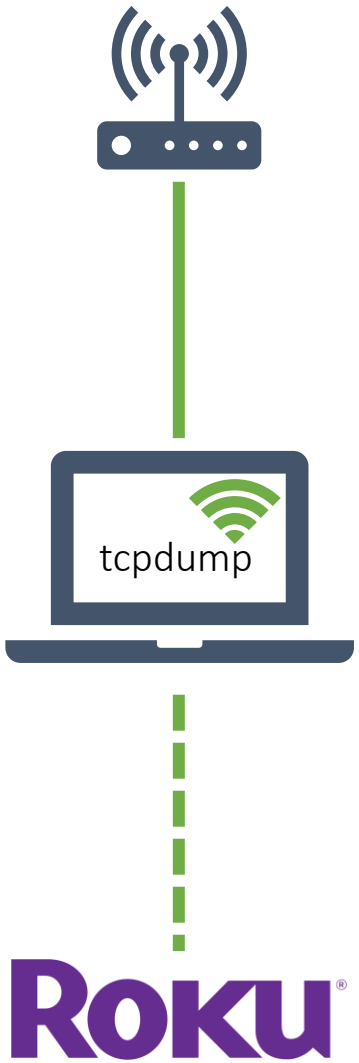
5%

of smart TVs

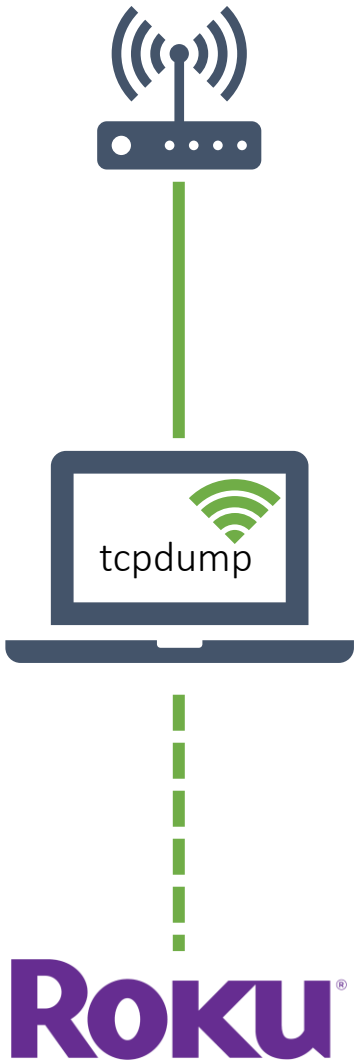
Video: using IoT Inspector while watching live videos on CBS app



Challenges of analyzing smart TV traffic in lab

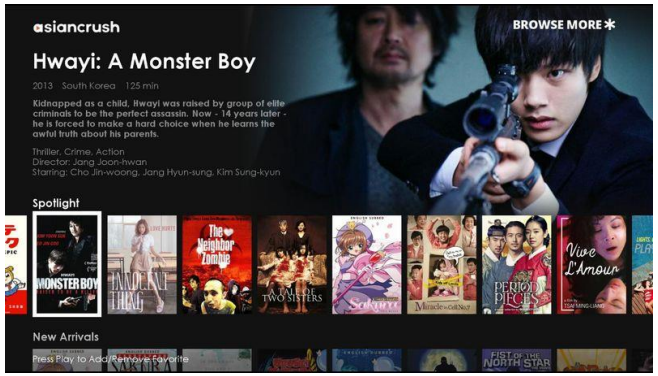


Challenges of analyzing smart TV traffic in lab



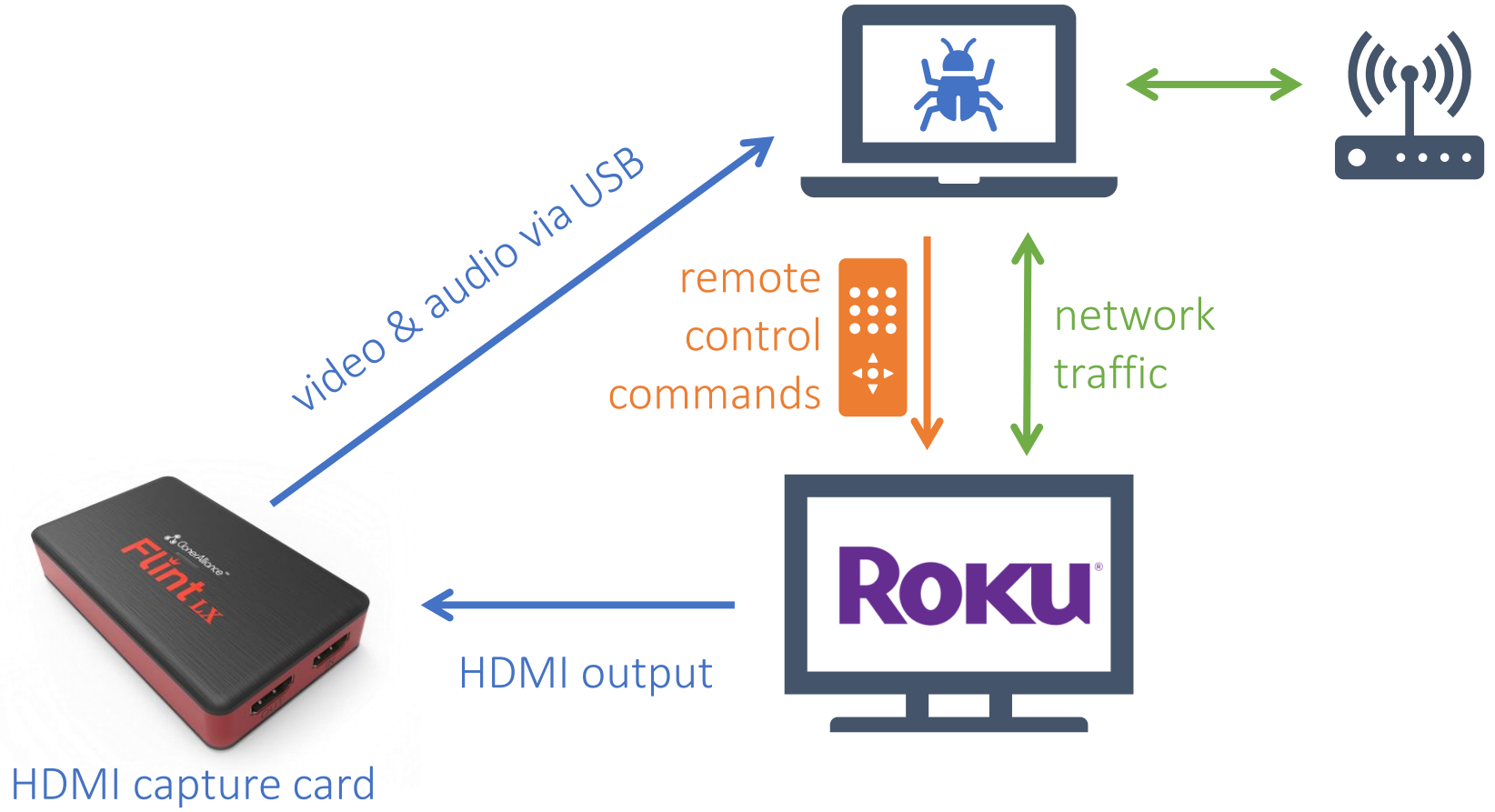
SPOTX

```
So%20Young%202%3A%20Never%20Gone

HTTP outbound to 192.35.249.124:80(DNS: search.spotxchange.com)(channel name: asiancrush)

GET./vast/3.0/146141?VPI[]=MP4&VPI[]=ROKU&app[name]=asiancrush&app[domain]=asiancrush.com&
app[bundle]=com.dmr.asiancrush&player_width=1280&player_height=720&device[devicetype]=7&de
vice[make]=Roku&device[model]=Roku&device[ifa]=39fc6352-aede-53f6-b3e3-58bf562bd074&ip_add
r=128.112.139.195&cb=1557313464653&custom[movie_title]=So%20Young%202%3A%20Never%20Gone&cu
stom[content_id]=3417&token[device_id]=39fc6352-aede-53f6-b3e3-58bf562bd074&token[connecti
on]=wifi&token[category_ID]=241&token[category_Title]=Romance&device[dnt]=0&max_bitrate=70
00 HTTP/1.1
Host: search.spotxchange.com
User-Agent: Roku/DVP-9.0 (519.00E04142A)
Accept: */*
```



How to analyze the traffic of TV apps at scale?

Automating interactions with smart TVs



Findings: sensitive data shared with ad/tracking services

Roku	% apps	amazon	% apps
Ad ID			
App name			
Serial number			
Zip code			
City or state			

Findings: sensitive data shared with ad/tracking services

Roku	% apps	amazon	% apps
Ad ID	32%		
App name	20%		
Serial number	11%		
Zip code	1%		
City or state	1%		

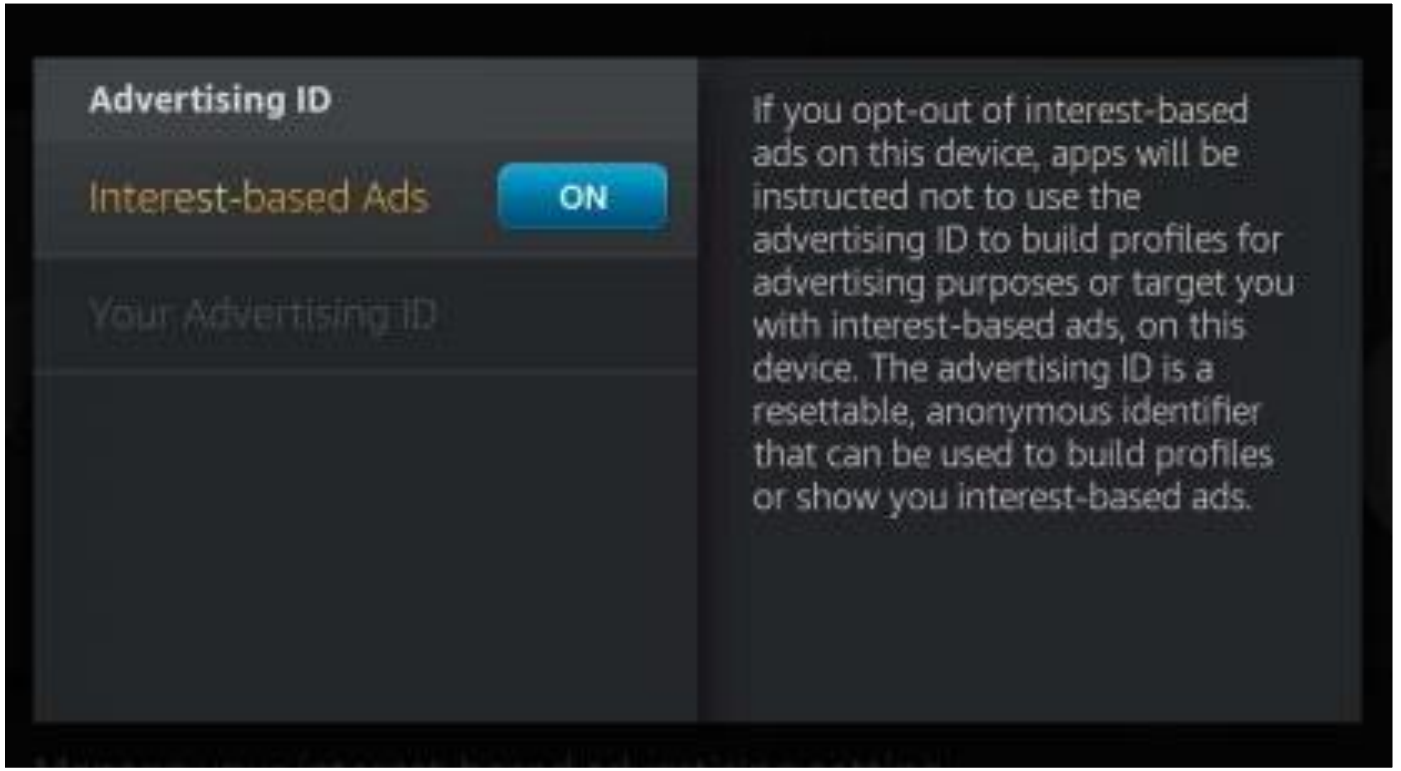
Findings: sensitive data shared with ad/tracking services

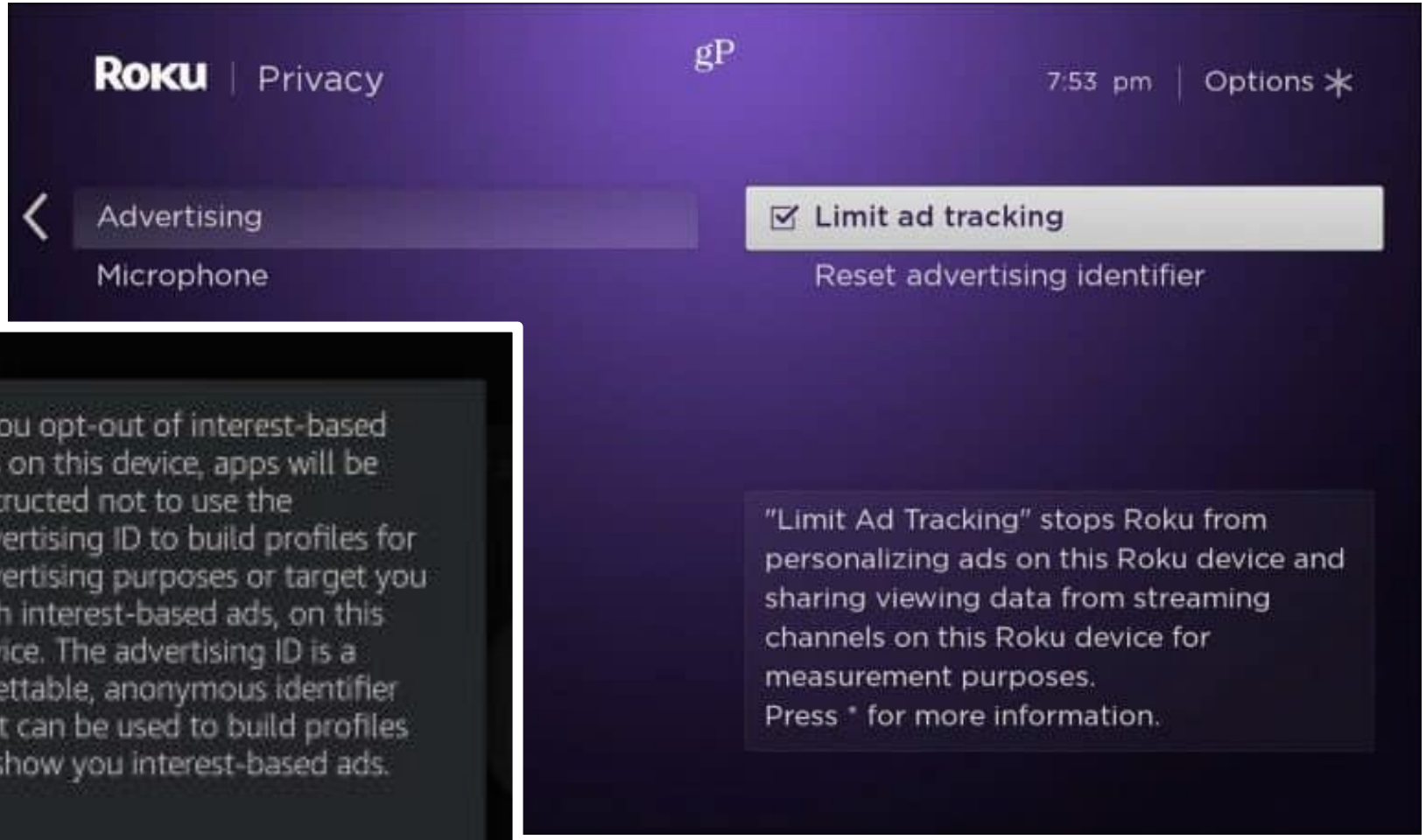
Roku	% apps	amazon	% apps
Ad ID	32%	Android ID	39%
App name	20%	Ad ID	22%
Serial number	11%	Serial number	10%
Zip code	1%	MAC address	5%
City or state	1%	WiFi SSID	2%

CNN animal planet Discovery CHANNEL

Limited ad tracking (Roku) / No interest-based ads (Amazon)

amazon





Poll: What happens when you disable ad tracking?

	Roku	% apps	amazon	% apps
A	Ad ID	32%	Android ID	39%
B	App name	20%	Ad ID	22%
C	Serial number	11%	Serial number	10%
D	Zip code	1%	MAC address	5%
E	City or state	1%	WiFi SSID	2%

Finding: 0 apps sent Ad ID under “limited tracking”

Roku	% apps	amazon	% apps
Ad ID	32%	Android ID	39%
App name	20%	Ad ID	22%
Serial number	11%	Serial number	10%
Zip code	1%	MAC address	5%
City or state	1%	WiFi SSID	2%

0%

Privacy for children?

FEDERAL TRADE COMMISSION

September 4, 2019

Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law

FTC, New York Attorney General allege YouTube channels collected kids' personal information without parental consent

The "FTC and New York Attorney General allege that YouTube violated the COPPA Rule by collecting personal information—in the form of **persistent identifiers** that are used to track users across the Internet—from viewers of **child-directed apps**, **without** first notifying parents and getting their **consent**."

Privacy for children?

FEDERAL TRADE COMMISSION

September 4, 2019

Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law

FTC, New York Attorney General allege YouTube channels collected kids' personal information without parental consent

The "FTC and New York Attorney General allege that YouTube violated the COPPA Rule by collecting personal information—in the form of persistent identifiers that are used to track users across the Internet—from viewers of child-directed apps, without first notifying parents and getting their consent."

Findings from smart TV study: privacy leaks in child-directed apps

	Roku	amazon
Number of apps	1,882	1,183
Number of child-directed apps	470	220

Findings from smart TV study: privacy leaks in child-directed apps

	Roku	amazon
Number of apps	1,882	1,183
Number of child-directed apps	470	220
Number of child-directed apps that leaked persistent IDs	34	23

Examples of persistent IDs in child-directed apps

amazon

PBS KIDS Video
Oct 16, 2012 | by PBS KIDS
4,547
App
FREE
Available instantly on compatible devices.

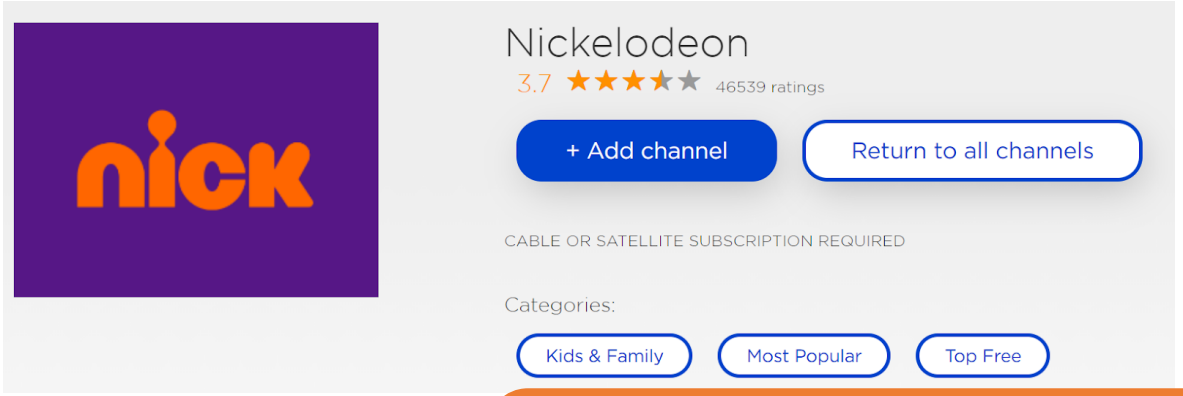
Leaked
Android ID

Fun with Roblox by HappyKids.tv
Jan 4, 2019
88
App
FREE
Available instantly on compatible devices.

Leaked
Android ID
Serial Number

Examples of persistent IDs in child-directed apps

Leaked
Ad ID
Serial Number



Leaked
Ad ID
Serial Number

How to identify child-directed contents?

What features? Manual labeling?

My ongoing work with collaborators

IoT firewall

THE UNIVERSITY OF CHICAGO Stanford University

IoT privacy perception

Carnegie Mellon University

Healthcare

Northwestern University

Voice assistant privacy

University of Virginia

NYU

Privacy law?

Cybersecurity insurance?