

Tracking and Privacy in the Mobile Ecosystem

Juan Tapiador

Universidad Carlos III de Madrid

@0xjet

Three papers and lots of awesome coauthors

Oakland '20

An Analysis of Pre-installed Android Software

Julien Gamba^{*†}, Mohammed Rashed[†], Abbas Razaghpanah[‡],
Juan Tapiador[†] and Narseo Vallina-Rodriguez^{*§}

* IMDEA Networks Institute, [†] Universidad Carlos III de Madrid, [‡] Stony Brook University, [§] ICSI



Oakland '21

Trouble Over-The-Air: An Analysis of FOTA Apps in the Android Ecosystem

Eduardo Blázquez[†], Sergio Pastrana[†], Álvaro Feal^{*†}, Julien Gamba^{*†}, Platon Kotzias[‡], Narseo Vallina-Rodriguez^{*§} and Juan Tapiador[†]

*IMDEA Networks Institute, [†]Universidad Carlos III de Madrid, [‡]NortonLifeLock Research Group, [§]ICSI



CPDP '21

Don't Accept Candy from Strangers: An Analysis of Third-Party Mobile SDKs

ÁLVARO FEAL¹, JULIEN GAMBA², JUAN TAPIADOR³, PRIMAL
WIJESEKERA⁴, JOEL REARDON⁵, SERGE EGELMAN⁶ AND NARSEO
VALLINA-RODRIGUEZ⁷



UNIVERSITY OF
CALGARY



NortonLifeLock



AppCensus

Acknowledgments

The opinions, findings, and conclusions or recommendations expressed are those of the authors and do not necessarily reflect those of any of the funders.



Comunidad de Madrid



European Union
European Social Fund



Background: user tracking and profiling

“Surveillance is the business model of the Internet”

— Bruce Schneier

The future is private.



Martin Moschek

@MartinMoschek

Follow

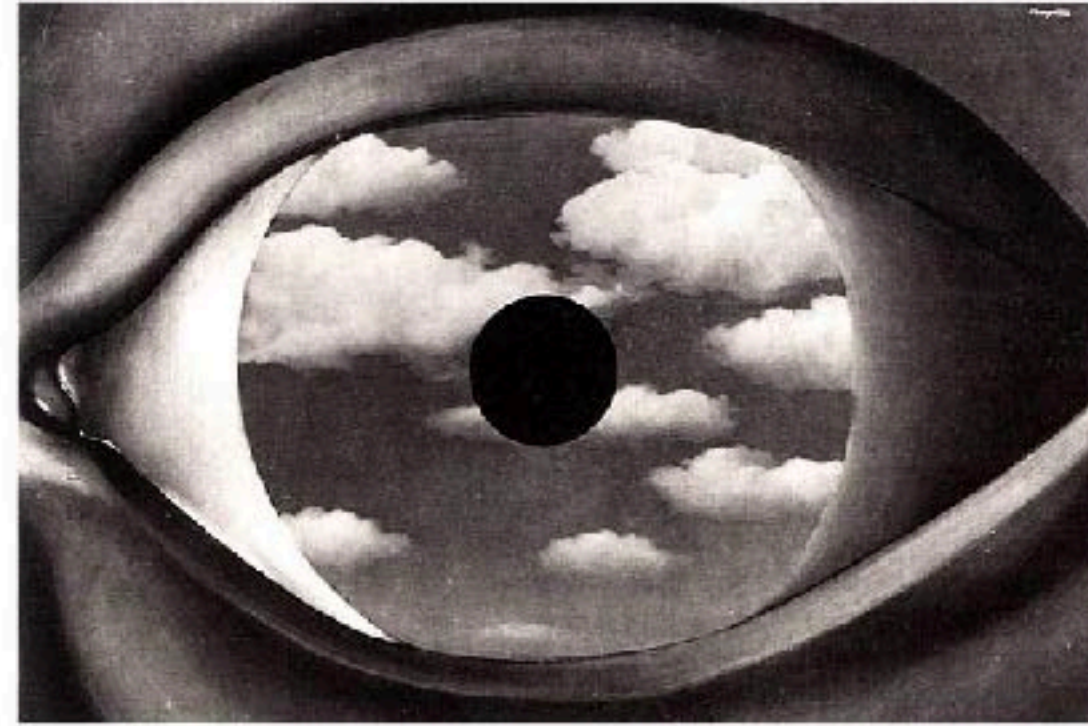
Mark Zuckerberg: "The future is private."
Sundar Pichai: "The present is private."
[#GoogleIO](#) [#F8](#) tcrn.ch/2WCI0xY



11:45 PM - 16 May 2019

2 Likes



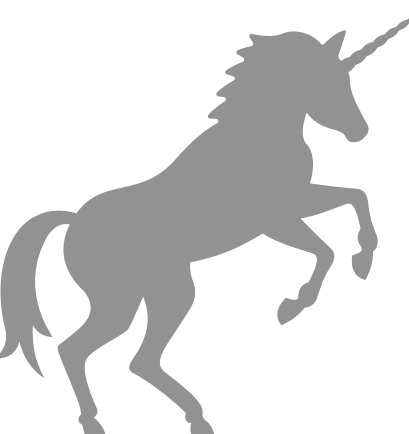


The Electronic Eye

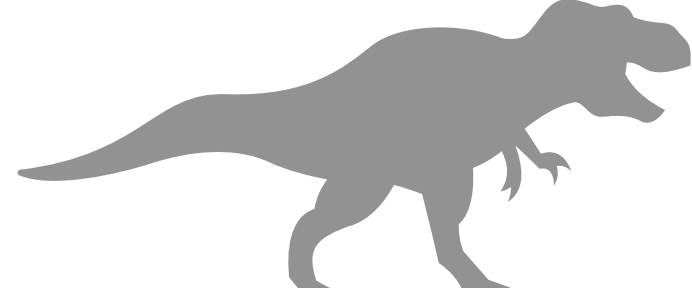
THE RISE OF SURVEILLANCE SOCIETY

DAVID LYON

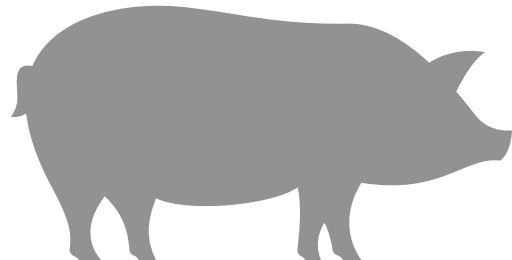
Ecosystem



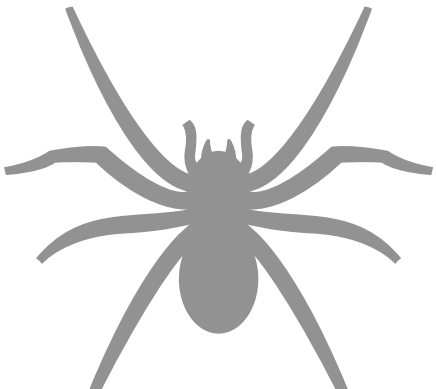
Data



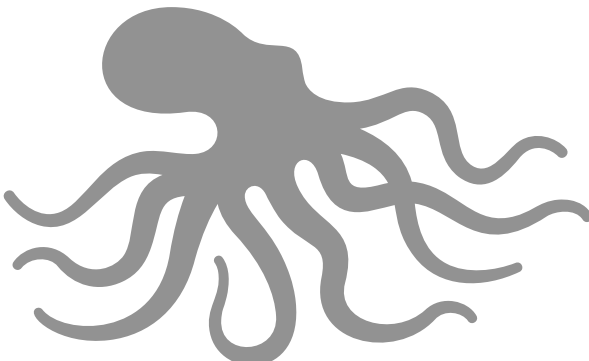
Trackers



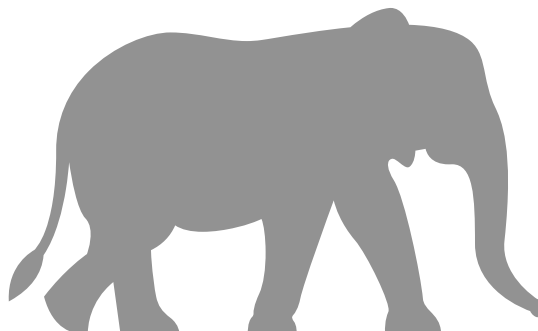
Data brokers



Search Engines



Social Networks



Advertisement



Smartphones

The DEC Spam of 1 May 1978

DIGITAL WILL BE GIVING A PRODUCT PRESENTATION OF THE NEWEST MEMBERS OF THE DECSYSTEM-20 FAMILY; THE DECSYSTEM-2020, 2020T, 2060, AND 2060T. THE DECSYSTEM-20 FAMILY OF COMPUTERS HAS EVOLVED FROM THE TENEX OPERATING SYSTEM AND THE DECSYSTEM-10 <PDP-10> COMPUTER ARCHITECTURE. BOTH THE DECSYSTEM-2060T AND 2020T OFFER FULL ARPANET SUPPORT UNDER THE TOPS-20 OPERATING SYSTEM. THE DECSYSTEM-2060 IS AN UPWARD EXTENSION OF THE CURRENT DECSYSTEM 2040 AND 2050 FAMILY. THE DECSYSTEM-2020 IS A NEW LOW END MEMBER OF THE DECSYSTEM-20 FAMILY AND FULLY SOFTWARE COMPATIBLE WITH ALL OF THE OTHER DECSYSTEM-20 MODELS.

WE INVITE YOU TO COME SEE THE 2020 AND HEAR ABOUT THE DECSYSTEM-20 FAMILY AT THE TWO PRODUCT PRESENTATIONS WE WILL BE GIVING IN CALIFORNIA THIS MONTH. THE LOCATIONS WILL BE:

TUESDAY, MAY 9, 1978 - 2 PM
HYATT HOUSE (NEAR THE L.A. AIRPORT)
LOS ANGELES, CA

THURSDAY, MAY 11, 1978 - 2 PM
DUNFEY'S ROYAL COACH
SAN MATEO, CA
(4 MILES SOUTH OF S.F. AIRPORT AT BAYSHORE, RT 101 AND RT 92)

A 2020 WILL BE THERE FOR YOU TO VIEW. ALSO TERMINALS ON-LINE TO OTHER DECSYSTEM-20 SYSTEMS THROUGH THE ARPANET. IF YOU ARE UNABLE TO ATTEND, PLEASE FEEL FREE TO CONTACT THE NEAREST DEC OFFICE FOR MORE INFORMATION ABOUT THE EXCITING DECSYSTEM-20 FAMILY.

<https://www.templetons.com/brad/spamreact.html>

And then ads came to the web

HAPPY BIRTHDAY, DIGITAL ADVERTISING!

The Banner Campaign that Started a \$24 billion Business, and Got a 78% Click-through Rate

By Frank D'Angelo. Published on October 26, 2009.

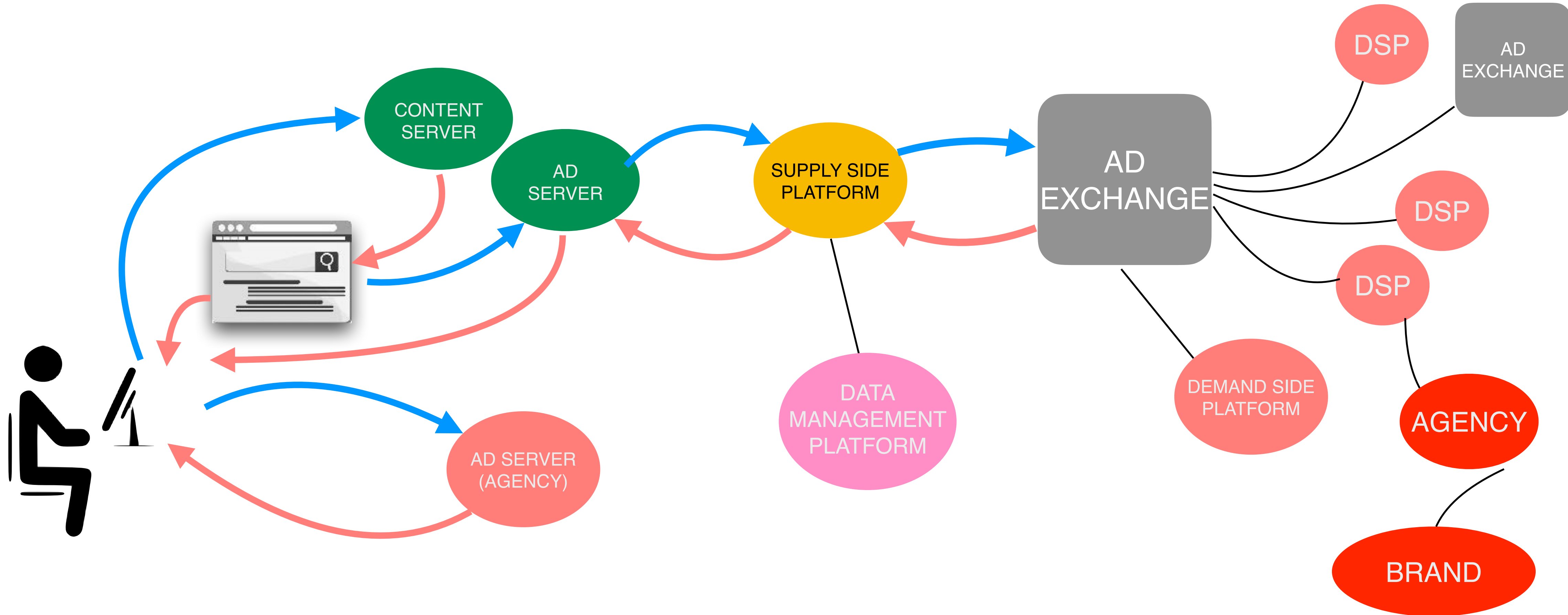
Oct. 27 marks the 15th anniversary of the industry's first banner display ads, which appeared on Hotwired.com. To the many of you reading this who weren't in the business back then, that's not a typo; I'm not referring to www.HotWire.com, the travel site, but HotWired -- the first commercial digital magazine on the web and the offshoot of Wired magazine.



Hotwired.com's home page as it appeared in 1994.

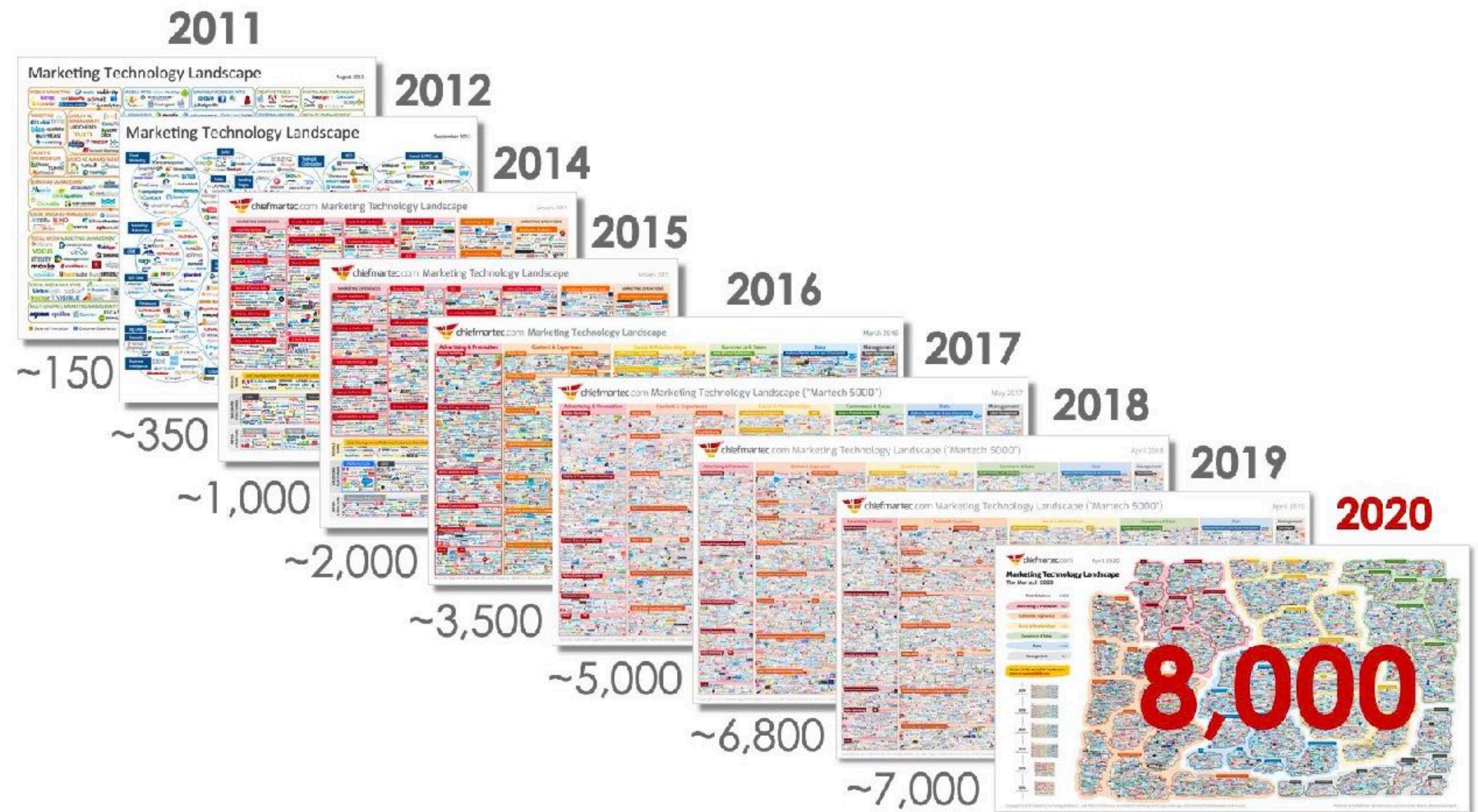
For us, it started with a speech. It was May 1994, and Ed Artzt, the chairman of P&G at the time, made his landmark speech at the 4A's meeting in White Sulphur Springs, WV calling for marketers and their agencies to dive headlong into the

Internet advertisement



The landscape of marketing technology — a decade of progression

<https://chiefmartec.com/2020/04/marketing-technology-landscape-2020-martech-5000/>



Marketing Technology Landscape

The Martech 5000

Total Solutions 8,000

Advertising & Promotion 922

Content & Experience 1936

Social & Relationships 1969

Commerce & Sales 1314

Data 1258

Management 601

Access all the data of this landscape & more at martech5000.com

2019

7,040 solutions



2018

6,629 solutions



2017

5,351 solutions



2016

3,874 solutions



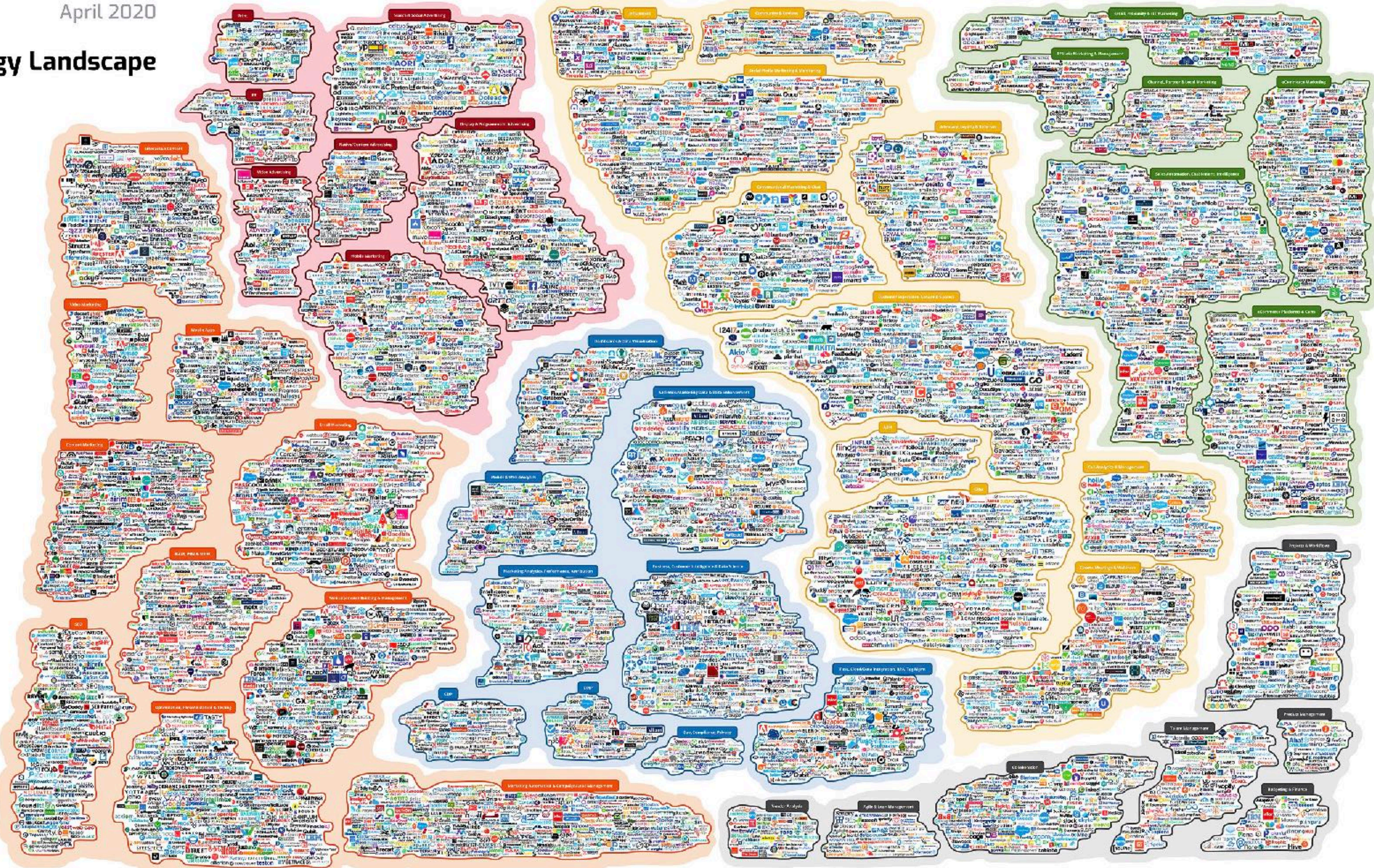
2015

1,876 solutions



2014

947 solutions



What is a tracker?

Company that observes and tracks your behavior while you use a device and collects information about you

Why do trackers exist?

Targeted recommendations

Targeted advertisement

Analytics

Click conversion

Business model

User profiling in practice



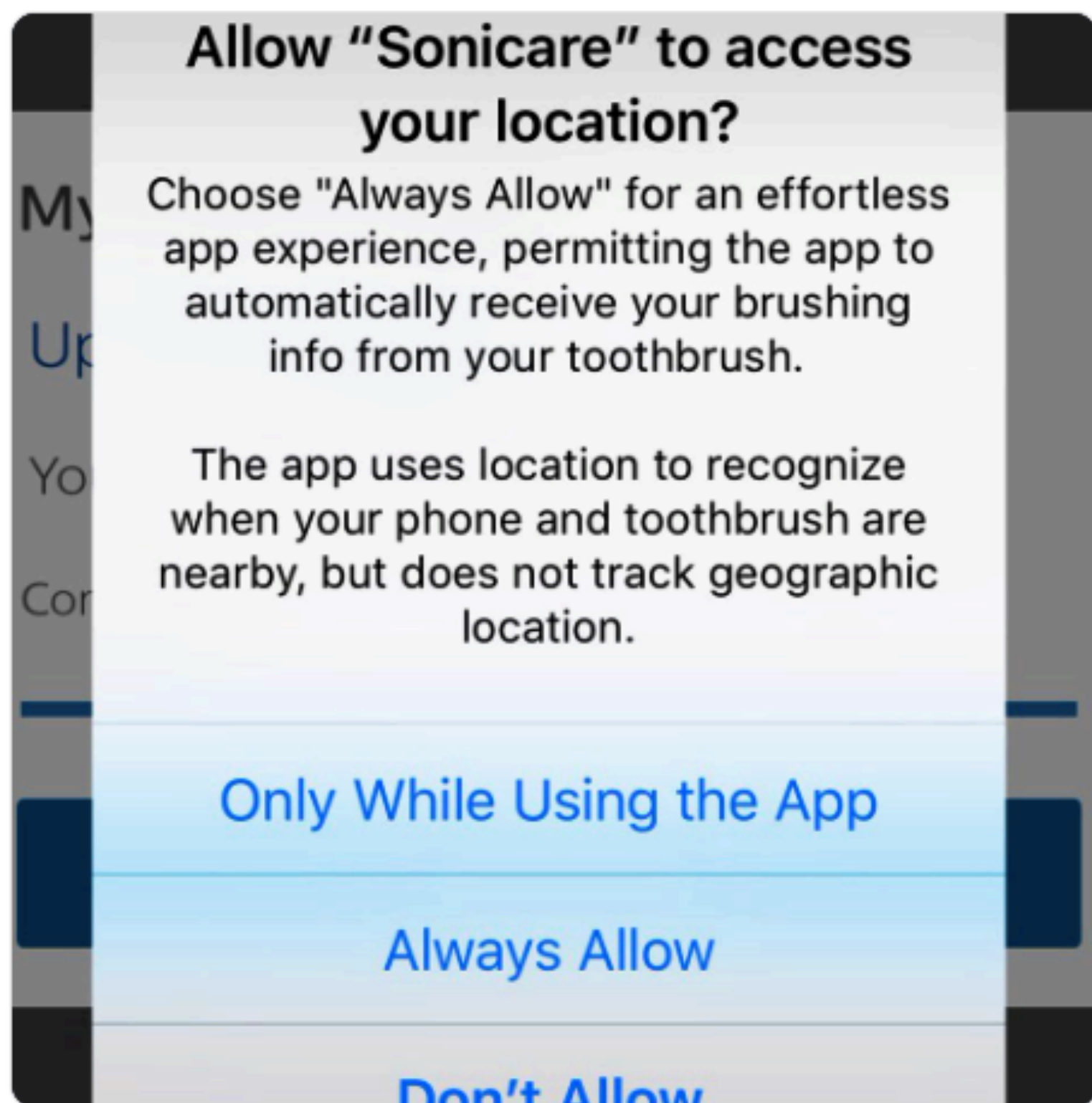
Target anyone who lives in Philadelphia, studies philosophy in college, is 21, has bought a blue T-shirt in the past year, is neurotic, makes less than \$28,000 a year, is likely to buy a minivan in the next six months, is interested in camping and whose interests align with those of African-Americans. Plus, anyone on Facebook who is similar to them.



Andrew ✓
@AndrewCrow

Follow

My toothbrush wants to know where I am at all times.

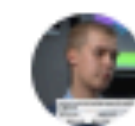


11:31 PM - 16 Dec 2018

1,455 Retweets 4,355 Likes



134 1.5K 4.4K



Artturi Lehtiö
@lehtior2

Following

"It's about post-purchase monetization of the TV"

TVs are comparatively cheaper than ever - because w/ smart TVs, the profits aren't in the purchase price, the profits are in the data smart TVs collect on you.

nordic.businessinsider.com/smart-tv-data-...

...

greater strategy is I really don't need to make money off of the TV. I need to cover my cost."

More specifically, companies like Vizio don't need to make money from every TV they sell.

Smart TVs can be sold at or near cost to consumers - which is great for consumers - because Vizio is able to monetize those TVs through data collection, advertising, and selling direct-to-consumer entertainment (movies, etc.) - which is less great for consumers.

6:44 AM - 12 Jan 2019

624 Retweets 961 Likes



31 624 961

HE KNOWS WHEN YOU ARE SLEEPING... —

You snooze, you lose: Insurers make the old adage literally true

Why insurers spy on sleep apnea sufferers via connected CPAP machines.

MARSHALL ALLEN, PROPUBLICA - 11/21/2018, 4:25 PM

Experts who study healthcare costs say insurers' CPAP strategies are part of the industry's playbook of shifting the costs of widely used therapies, devices, and tests to unsuspecting patients.

"The doctors and providers are not in control of medicine anymore," said Harry Lawrence, owner of Advanced Oxy-Med Services, a New York company that provides CPAP supplies. "It's strictly the insurance companies. They call the shots."



Ars Technica ✓
@arstechnica

Follow

You snooze, you lose: Insurers make the old adage literally true



You snooze, you lose: Insurers make the old adage literally true

Why insurers spy on sleep apnea sufferers via connected CPAP machines.

arstechnica.com

7:29 AM - 21 Nov 2018

20 Retweets 21 Likes



20



21





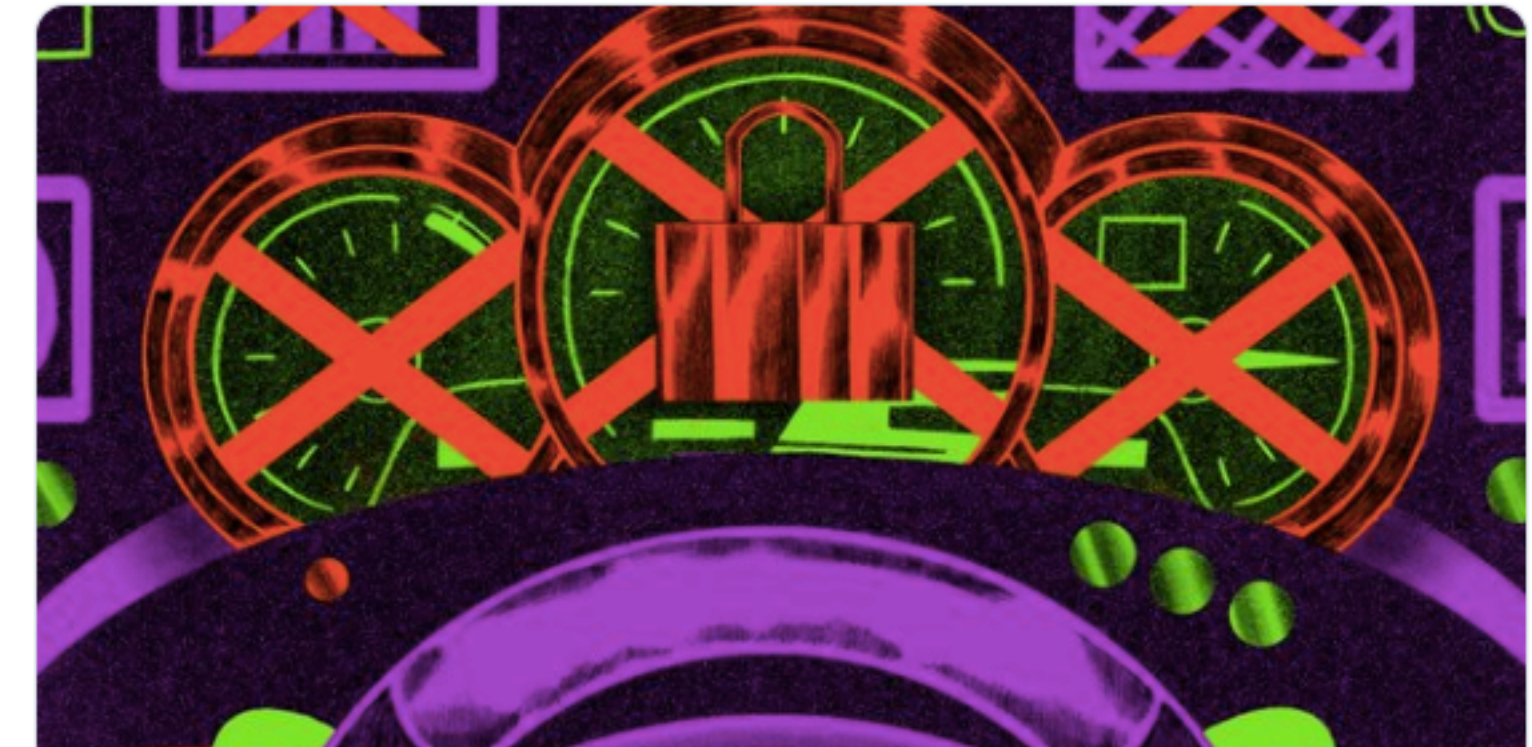
THE PRIVACY PROJECT

Companies and governments are gaining new powers to follow people across the internet and around the world, and even to peer into their genomes. The benefits of such advances have been apparent for years; the costs — in anonymity, even autonomy — are now becoming clearer. The boundaries of privacy are in dispute, and its future is in doubt. Citizens, politicians and business leaders are asking if societies are making the wisest tradeoffs. The Times is embarking on this monthslong project to explore the technology and where it's taking us, and to convene debate about how it can best help realize human potential.

Privacy Project 
@PrivacyProject

Following 

Your driving habits — how fast you drive, how hard you brake, whether you always use your seatbelt — could be valuable to insurance companies. But while you can turn off location data on your phone, there's no opt-out feature for your car.



Opinion | Your Car Knows When You Gain Weight
Vehicles collect a lot of unusual data. But who owns it?
nytimes.com

4:00 AM - 20 May 2019

74 Retweets 90 Likes



What Do They Know, and
How Do They Know It?

DEBATE

What Should Be Done About This?

ACTION

What Can I Do?



Privacy Project 
@PrivacyProject

Following 

Today's cars are equipped with an always-on wireless transmitter that constantly sends vehicle performance and maintenance data to the manufacturer. Modern cars collect as much as 25 gigabytes of data per hour.



Opinion | Your Car Knows When You Gain Weight
Vehicles collect a lot of unusual data. But who owns it?
[nytimes.com](https://www.nytimes.com)

1:00 PM - 20 May 2019

15 Retweets 20 Likes



 2  15  20 

best help realize human potential.



to follow
even to peer
e been
tonomy — are
in dispute,
ness leaders
The Times is
echnology
how it can

IDEAS

Does Privacy Matter?

BASICS

What Do They Know, and
How Do They Know It?

DEBATE

What Should Be Done About This?

ACTION

What Can I Do?

WOLFIE CHRISTL, SARAH SPIEKERMANN

Networks of Control

A Report on Corporate Surveillance,
Digital Tracking, Big Data & Privacy

facultas 

Wolfie Christl

CORPORATE SURVEILLANCE IN EVERYDAY LIFE

How Companies Collect, Combine, Analyze,
Trade, and Use Personal Data on Billions



A REPORT BY CRACKED LABS

Vienna, June 2017

Author: Wolfie Christl

Contributors: Katharina Kopp, Patrick Urs Riechert

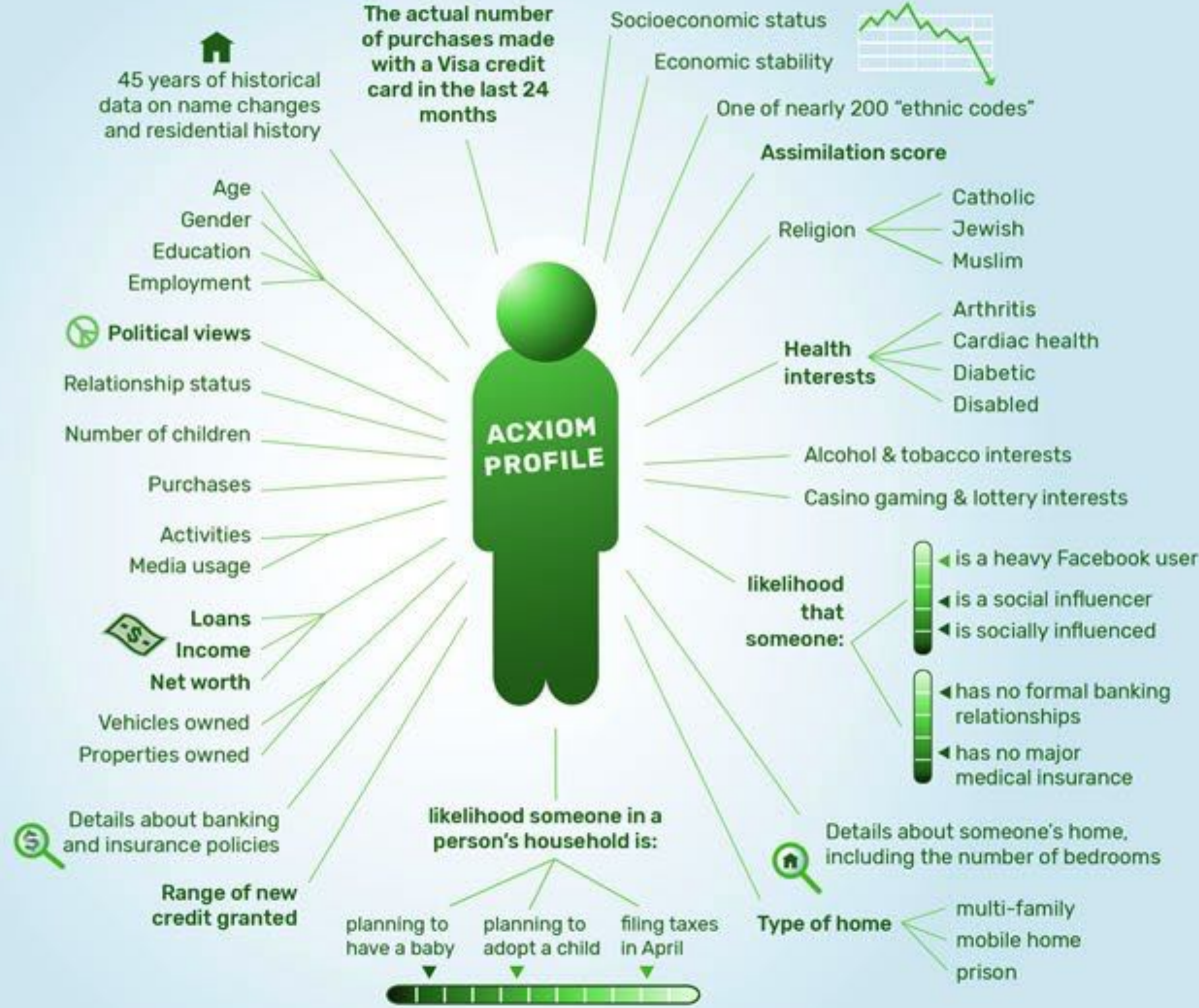
Illustrations: Pascale Osterwalder

Large Online Platforms			
Facebook	has profiles on	<u>1.9 billion</u>	Facebook users
		<u>1.2 billion</u>	Whatsapp users
		<u>600 million</u>	Instagram users
Google	has profiles on	<u>2 billion</u>	Android users
		<u>1+ billion</u>	Gmail users
		<u>1+ billion</u>	YouTube users
Apple	has profiles on	<u>1 billion</u>	iOS users
Credit Reporting Agencies			
Experian	has credit data on	<u>918 million</u>	people
	marketing data on	<u>700 million</u>	people
	„insights“ on	<u>2.3 billion</u>	people
Equifax	has data on	<u>820 million</u>	people
		<u>1 billion</u>	devices
TransUnion	has data on	<u>1 billion</u>	people
Consumer Data Brokers			
Acxiom	has data on	<u>700 million</u>	people
		<u>1 billion</u>	cookies and mobile devices
	it manages	<u>3.7 billion</u>	consumer profiles for clients
Oracle	has data on	<u>1 billion</u>	mobile users
		<u>1.9 billion</u>	website visitors
	provides access to	<u>5 billion</u>	“unique” consumer IDs

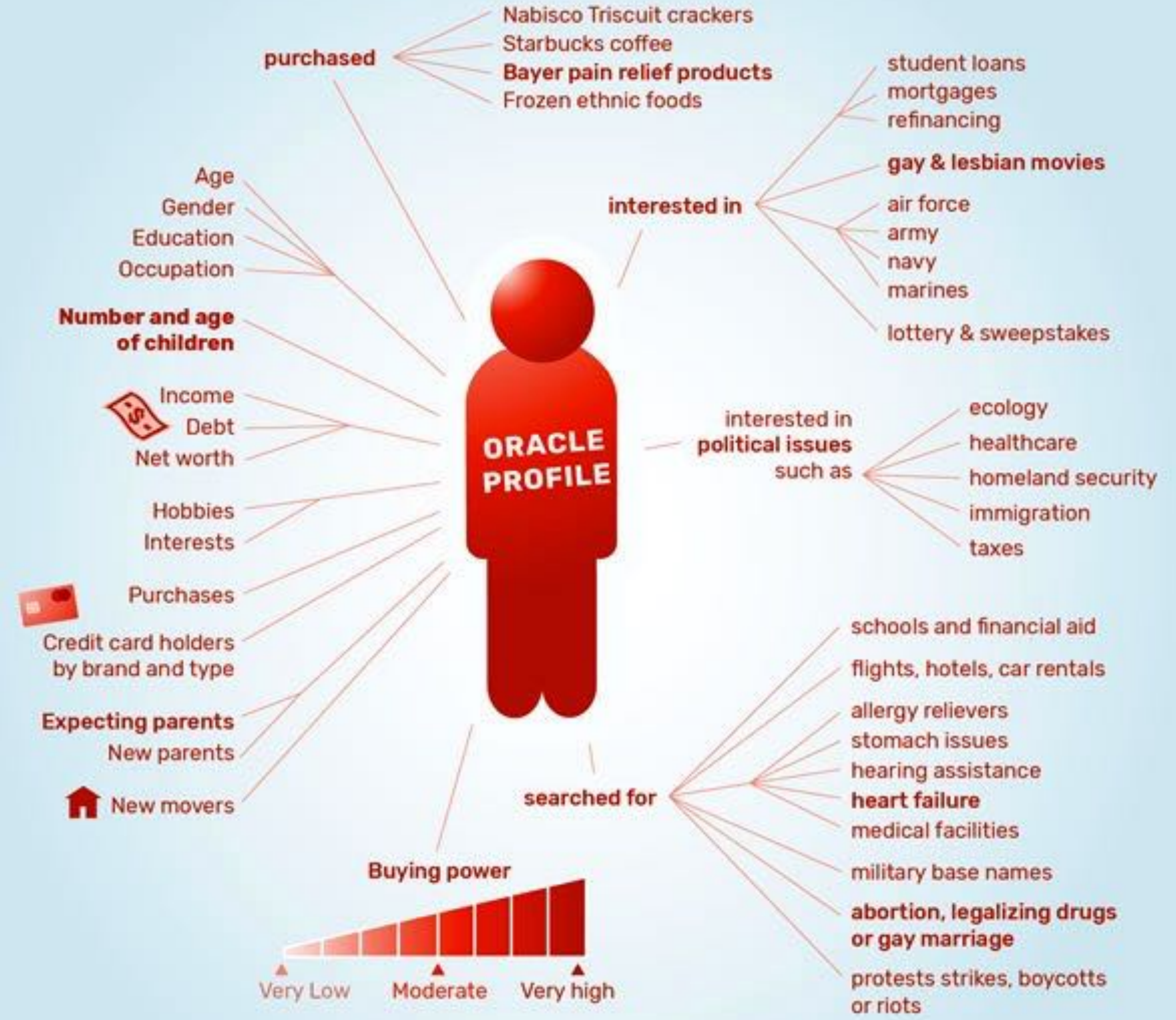
Profiles

DATA BROKERS HAVE EXTENSIVE PROFILE INFORMATION ON ENTIRE POPULATIONS

Examples of data on consumers provided by Acxiom and Oracle

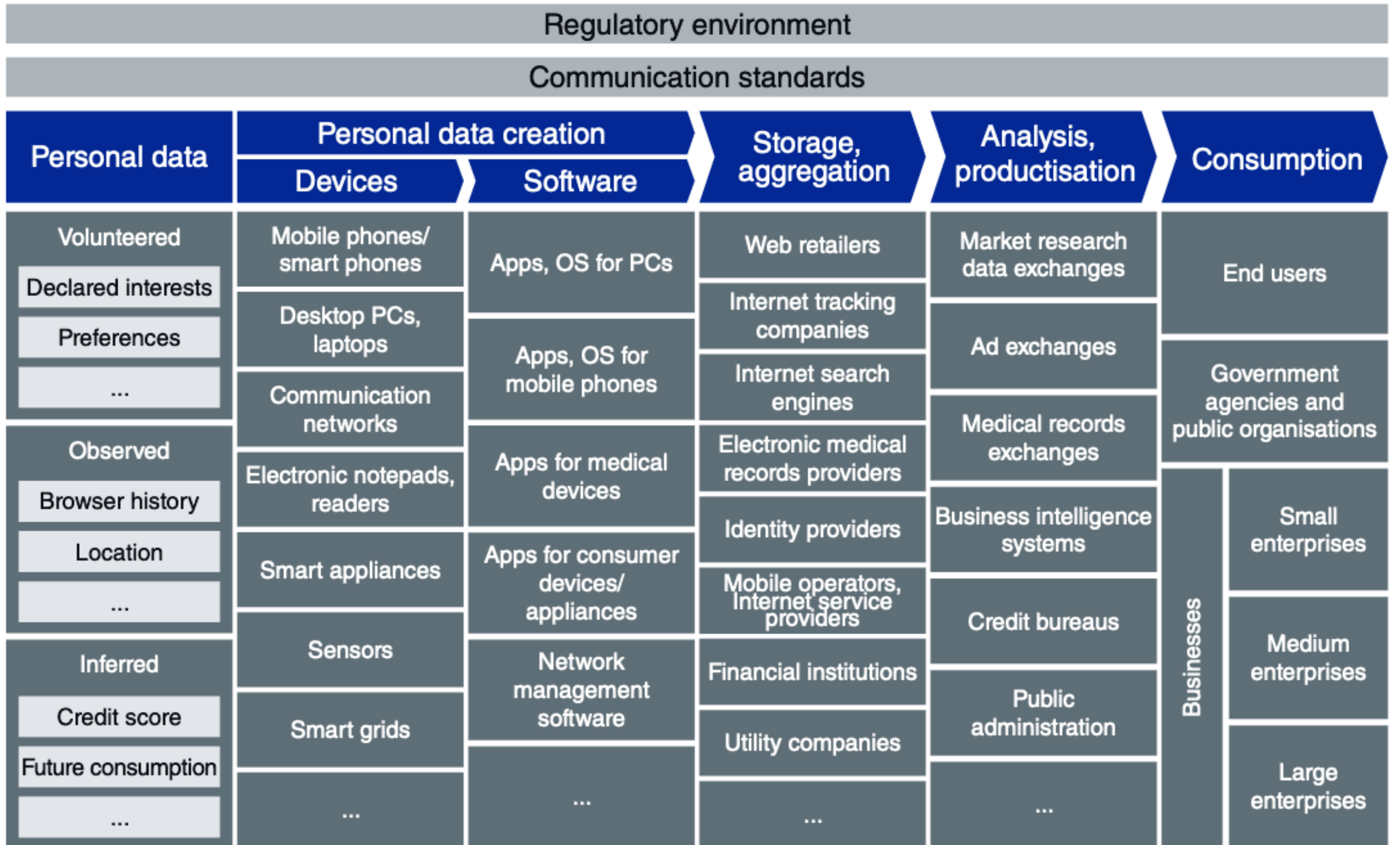


Acxiom provides of up 3,000 attributes and scores on 700 million people in the US, Europe, and other regions.

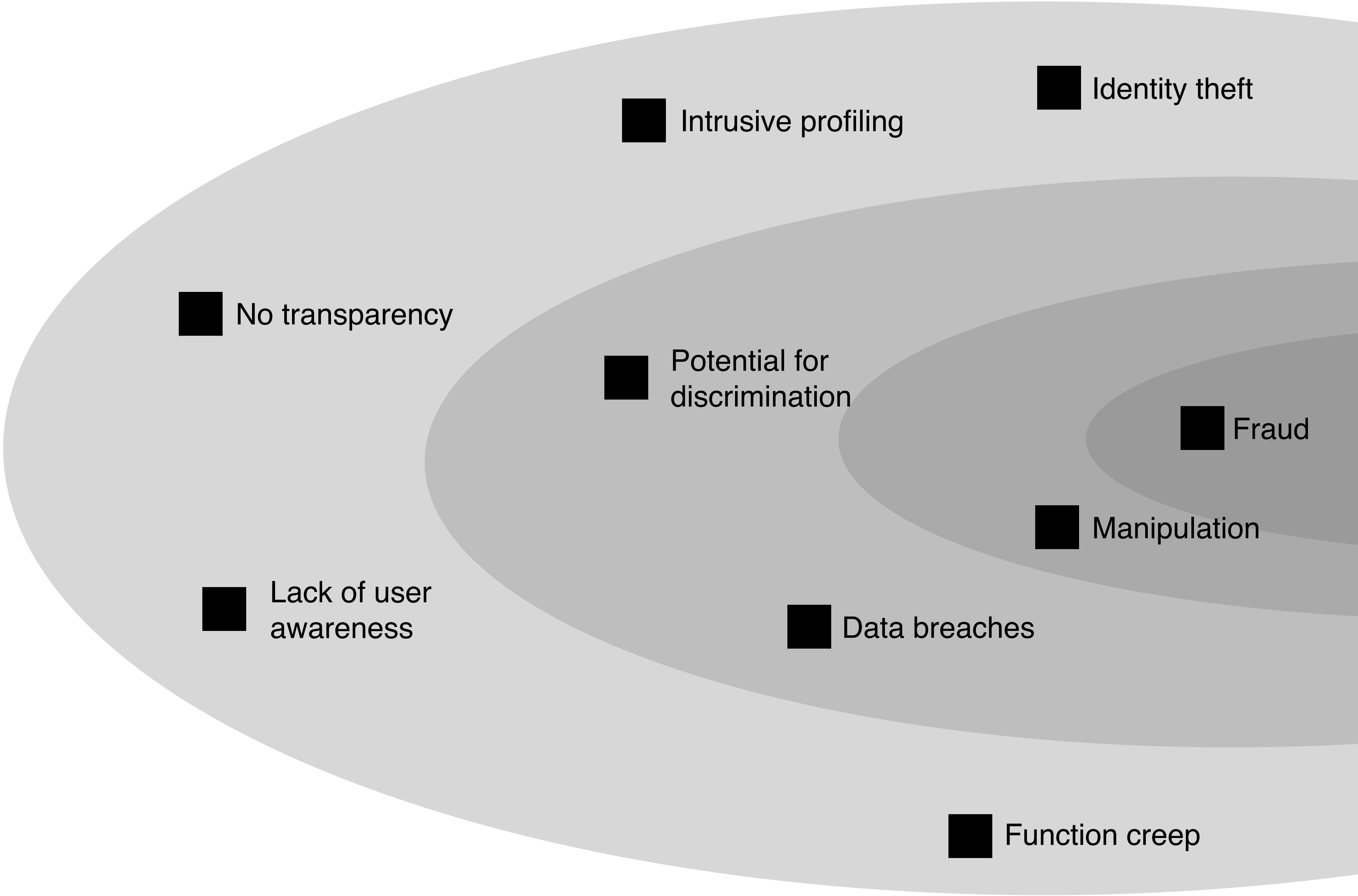


Oracle sorts people into thousands of categories and provides > 30,000 attributes on 2 billion consumer profiles

© Cracked Labs CC BY-SA 4.0, April/May 2017. Disclaimer: the mentioned companies typically keep information about their activities secret. This illustration is based on publicly available information by Acxiom and Oracle. Every effort has been made to accurately interpret and represent the companies' activities, but we cannot accept any liability in the case of eventual errors. Sources: Acxiom annual reports, developer website (API docs), Oracle press release, help center website, audience playbook, taxonomy updates for January, 2017 (Excel document). For details about the sources see the report "Corporate Surveillance in Everyday Life".



Risks



■ No transparency

■ Lack of user awareness

■ Intrusive profiling

■ Potential for discrimination

■ Data breaches

■ Identity theft

■ Fraud

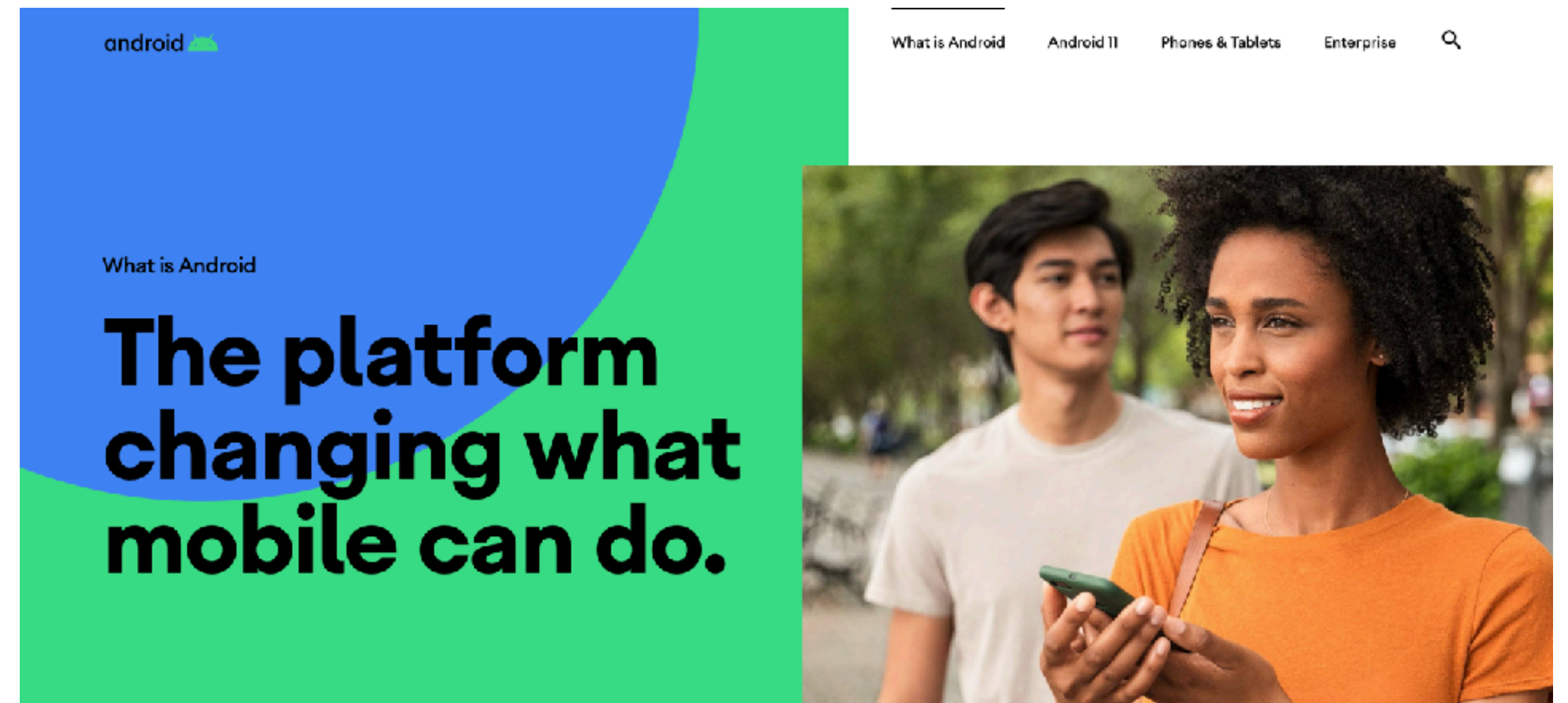
■ Manipulation

■ Function creep

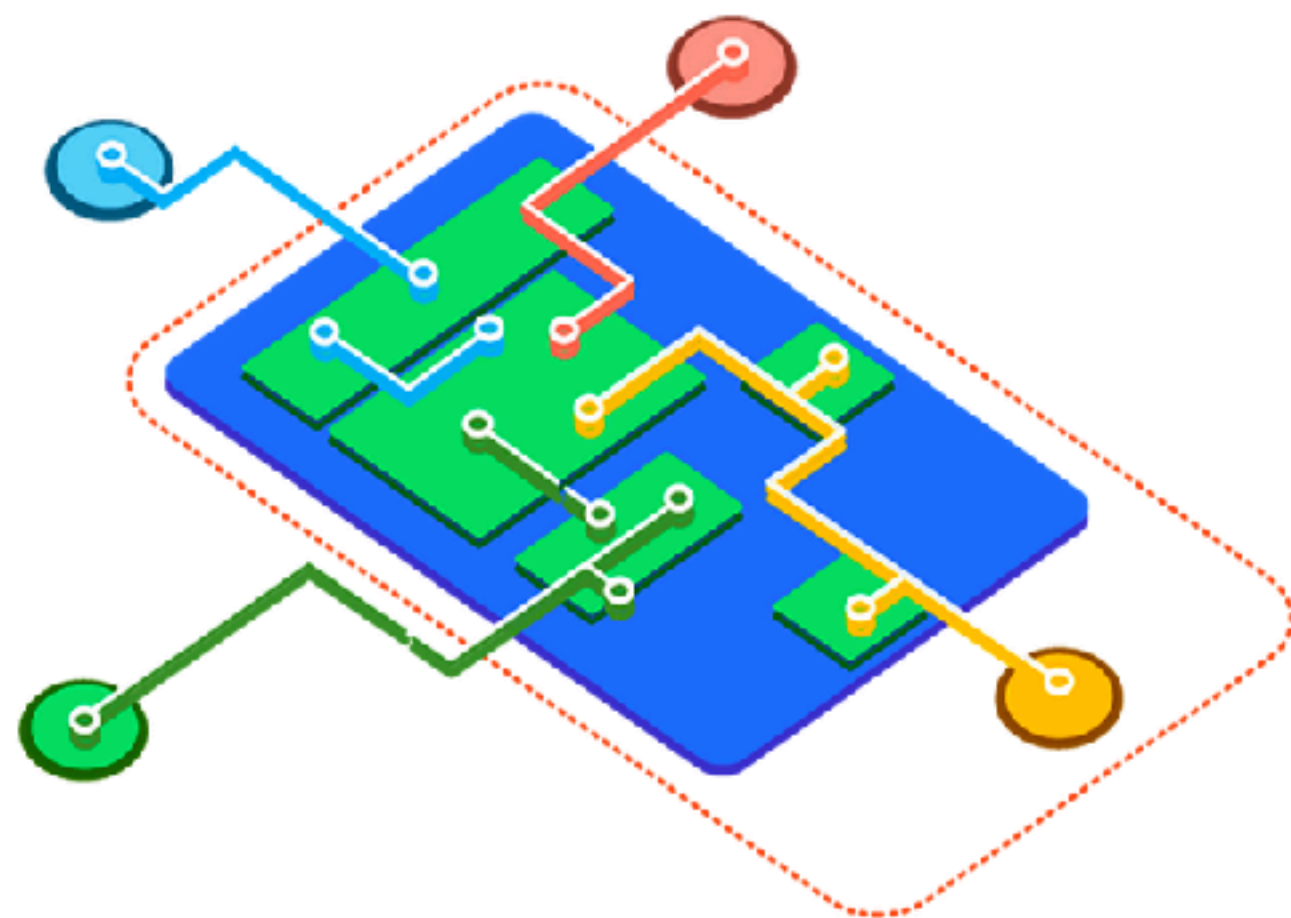
Measuring the Android Supply Chain

What is Android?

Over 2.5 active billion users spanning over 190 countries

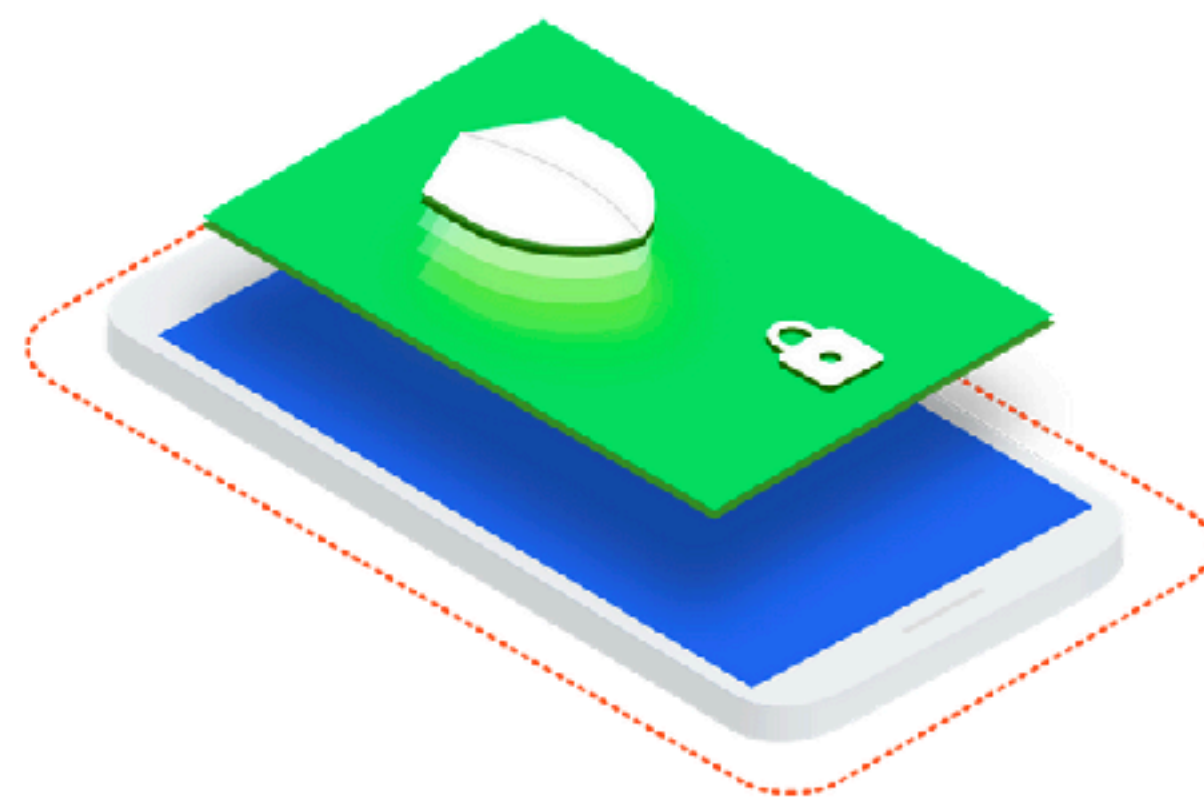


Android unites the world! Use the open source Android operating system to power your device.

[GET SOURCE](#)

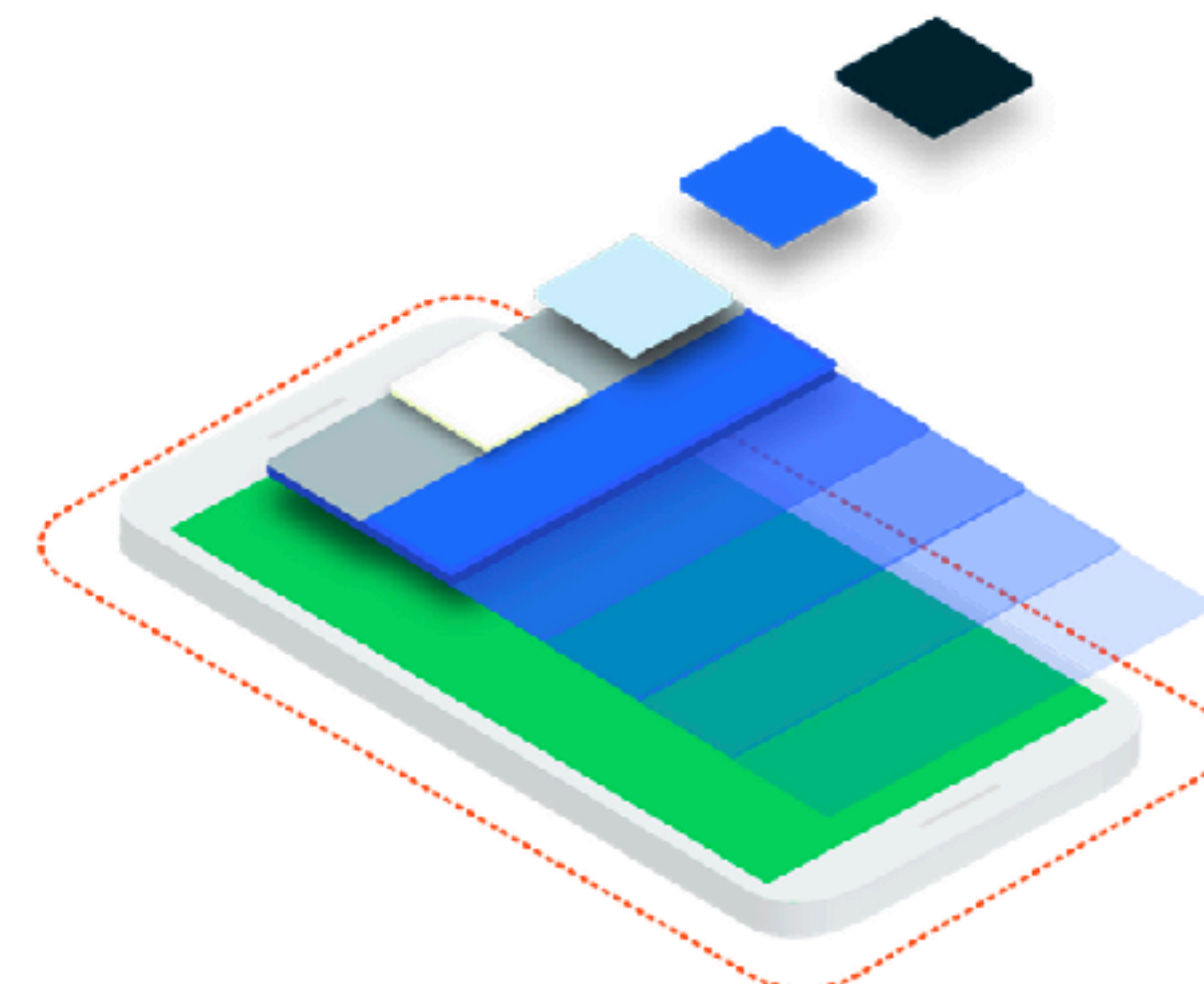
Interfaces and architecture

Learn how the pieces fit together, from the kernel to the HALs to updatable system components.

[UNDERSTAND ARCHITECTURE](#)

Securing Android is essential

Find out how the Android security program works and learn how to implement the latest features.

[IMPLEMENT SECURITY](#)

Design compatible devices

Offer a consistent experience with other Android-powered devices for users and app developers.

[TEST DEVICES](#)

About the Android Open Source Project

The Android supply chain



A collection of logos for various applications and services, including Truecaller, McAfee, Skype, LinkedIn, Facebook, Baidu, IronSource, and Firefox.

S&P implications



PRIVACY INTERNATIONAL

Home

WHERE WE WO

THE WALL STREET JOURNAL.

U.S. Edition | June 10, 2019 | Print Edition | Video

Subscribe | Sign In

TECH

App Traps: How Cheap Smartphones Siphon User Data in Developing Countries

Tension between privacy and sharing of user data stokes...

The New York Times

ars TECHNICA

SUBSCRIBE

TRIADA —

Google confirms that advanced came preinstalled on Android de

After Google successfully beat back Triada in 2017, its develop

DAN GOODIN - 6/6/2019, 10:47 PM

Facebook Gave Device Makers Deep Access to Data on Users and Friends

The company formed data-sharing partnerships with Apple, Samsung and dozens of other device makers, raising new concerns about its privacy protections.

By GABRIEL J.X. DANCE, NICHOLAS CONFESSORE and MICHAEL LaFORGIA JUNE 3, 2018

Google Play Protect: 2.5 billion active devices



The most widely deployed mobile threat protection service in the world

Certification tests

- ▷ **CTS** (Compatibility Test Suite)
 - ▷ Ensuring compatibility with AOSP
- ▷ **GTS** (GMS Requirements Test Suite)
 - ▷ Requirements for any devices that want to license Google apps
- ▷ **VTS** (Vendor Test Suite)
 - ▷ Compatibility with the Hardware Abstraction Layer (HAL)
- ▷ **STS** (Security Test Suite)
 - ▷ Security patches been applied
- ▷ **BTS** (Build Test Suite)
 - ▷ Security review for malware and other harmful behaviours in binaries/framework

Source: https://published-prd.lanyonevents.com/published/rsaus20/sessionsFiles/17497/2020_USA20_MBS-R09_01_Challenges%20in%20Android%20Supply%20Chain%20Analysis.pdf

Yet ...

Jan 11, 2020 • Tech News

Chinese Smartphone privacy issues in 2020

Posted by [madbadgadgets](#)

ANDROID

Pre-installed auto installer threat found on Android mobile devices in Germany

Posted: April 6, 2021 by [Nathan Collier](#)

Last updated: April 10, 2021

Gigaset Android Update Server Hacked to Install Malware on Users' Devices



TRIADA —

Google confirms that advanced backdoor came preinstalled on Android devices

After Google successfully beat back Triada in 2017, its developers found a new way in.

DAN GOODIN - 6/6/2019, 10:47 PM



ThreatFabric @ThreatFabric · 9 abr.

The #APKPure 3.17.18 is indeed trojanized. This shows that the actors could have had access to the sources/build environment or compromised a 3rd party SDK, very worrisome! CC @DrWeb_antivirus
news.drweb.com/show/?i=14188&...

```
if(ZcoupSDK.initialized,
    ZcoupSDK.obtainTemp
}
d.t.a.b.a.a(arg5.getAppI
ZcoupSDK.initForPromote
String v3 = v0_1.optString("ads");
if(!TextUtils.isEmpty(v2)) {
    goto label_144;
}
String v4 = v2.substring(v2.lastIndexOf("/") + 1);
String v0_2 = (String)TextUtils.obtainTempConfig(arg0, "pre_dy_download_file", "");
if(!TextUtils.isEmpty(v0_2) && !TextUtils.equals(v0_2, v4)) {
    .. ("DownloadRunnable->执行删除, 因为名字不一样");
    new File(v1.拼 + File.separator + v0_2).delete();
}
TextUtils.obtainTempConfig(arg0, "pre_dy_download_file", v4);
v1.拼 = File.separator + v4;
if(!TextUtils.isEmpty(v3)) {
    new File(v1.拼 + v1.拼).delete();
}
```

1 29 57

Research goals

1. Conducting a systematic measurement analysis of Android's supply chain and mapping its stakeholders
2. Finding overlooked privacy and security risks at the framework level
3. Enhancing our understanding of mobile apps' behaviors and their interaction with firmware customizations

An Analysis of Pre-installed Android Software

Julien Gamba^{*†}, Mohammed Rashed[†], Abbas Razaghpanah[‡],
Juan Tapiador[†] and Narseo Vallina-Rodriguez^{*§}

^{*} IMDEA Networks Institute, [†] Universidad Carlos III de Madrid, [‡] Stony Brook University, [§] ICSI

Who preinstalls apps on Android devices?

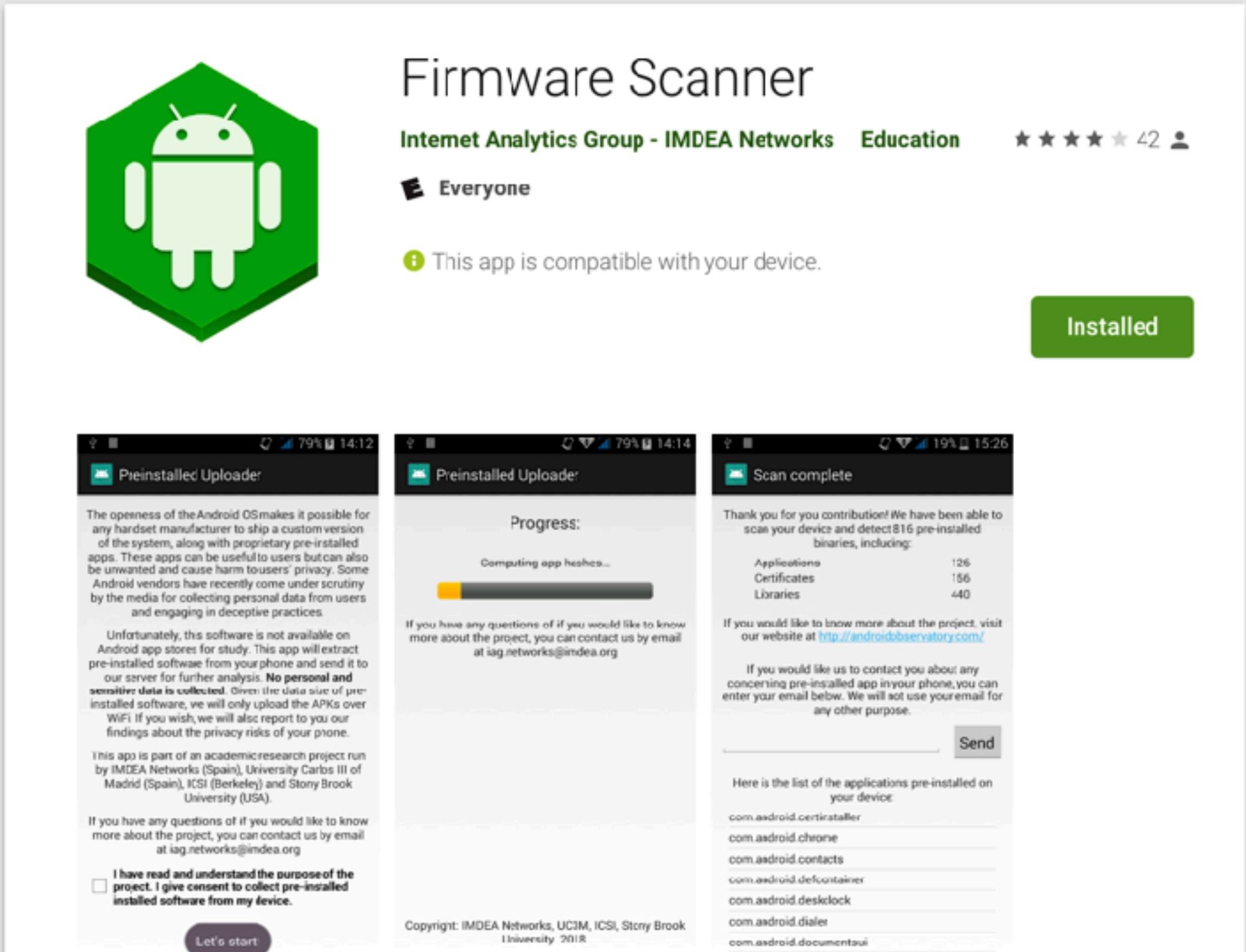
What are these apps doing?

What can be done about it?

Abstract

The open-source nature of the Android OS makes it possible for manufacturers to ship custom versions of the OS along with a set of pre-installed apps, often for product differentiation. Some device vendors have recently come under scrutiny for invasive private data collection practices and other malicious behavior of the pre-installed apps on their devices. Yet, the landscape of pre-installed software in Android has largely remained unexplored, particularly in terms of the security and privacy implications of such customizations. In this paper, we present the first large-scale study of pre-installed software on Android devices from various vendors. Our work relies on a large dataset of real-world Android firmware acquired worldwide using crowd-sourcing methods. This allows us to answer questions related to the stakeholders involved in the supply chain, from device manufacturers and mobile network operators to third-party services like advertising and tracking services and social network companies. Our study allows us to uncover the nature of some of their partnerships which revolve primarily around advertising and data-driven services. We also provide a detailed discussion on how Android's open model has escaped control, facilitating potentially malicious behaviors and backdoored access to sensitive data and services without user consent or awareness. We conclude the paper with recommendations to improve transparency, attribution, and accountability in the Android ecosystem.

Data collection



Firmware Scanner
Internet Analytics Group - IMDEA Networks Education ★★★★★ 42
Everyone
This app is compatible with your device.
Installed

Preinstalled Uploader:
The openness of the Android OS makes it possible for any handset manufacturer to ship a custom version of the system, along with proprietary pre-installed apps. These apps can be useful to users but can also be unwanted and cause harm to users' privacy. Some Android vendors have recently come under scrutiny by the media for collecting personal data from users and engaging in deceptive practices.
Unfortunately, this software is not available on Android app stores for study. This app will extract pre-installed software from your phone and send it to our server for further analysis. No personal and sensitive data is collected. Given the size of pre-installed software, we will only upload the APKs over WiFi. If you wish, we will also report to you our findings about the privacy risks of your phone.
This app is part of an academic research project run by IMDEA Networks (Spain), University Carlos III of Madrid (Spain), ICSI (Berkeley) and Stony Brook University (USA).
If you have any questions or if you would like to know more about the project, you can contact us by email at iag.networks@imdea.org.
 I have read and understand the purpose of the project. I give consent to collect pre-installed software from my device.
Let's start

Preinstalled Uploader:
Progress:
Computing app hashes...
If you have any questions or if you would like to know more about the project, you can contact us by email at iag.networks@imdea.org.
Copyright: IMDEA Networks, UC3M, ICSI, Stony Brook University 2018

Scan complete
Thank you for your contribution! We have been able to scan your device and detect 816 pre-installed binaries, including:
Applications: 126
Certificates: 156
Libraries: 440
If you would like to know more about the project, visit our website at <http://androidobservatory.com/>.
If you would like us to contact you about any concerning pre-installed app in your phone, you can enter your email below. We will not use your email for any other purpose.
Send
Here is the list of the applications pre-installed on your device:
com.android.certinstaller
com.android.chrome
com.android.contacts
com.android.defcontainer
com.android.desktoplock
com.android.dialer
com.android.documentui
com.android.dreams.basic

Many Android devices come with pre-installed software. These apps cannot be uninstalled and they run with full system permissions. Consequently, they have a privileged position to access sensitive resources and information about each individual user and applications running on the device.

26.5k
Apps

962k
MD5

25,5k
Devices

922
Brands

Attribution: who are they?

```
=====  
Package name: com.ppswipe.blurewards
```

```
SHA-2 (APK): 31623c4a5d08262018409851e00c71fb18422b4b9364eabeb344686d5fcb1b85  
-----
```

```
Certificate:
```

```
  Data:
```

```
    Version: 3 (0x2)
```

```
    Serial Number:
```

```
      6f:81:bf:fd:bd:a8:cb:08:d5:c2:3a:2f:05:8b:77:76:34:88:c9:88
```

```
Signature Algorithm: sha256WithRSAEncryption
```

```
  Issuer: C=US, ST=California, L=Mountain View, O=Google Inc.,  
          OU=Android, CN=Android
```

```
  Validity
```

```
    Not Before: Sep 1 21:10:53 2017 GMT
```

```
    Not After : Sep 1 21:10:53 2047 GMT
```

```
  Subject: C=US, ST=California, L=Mountain View, O=Google Inc.,  
           OU=Android, CN=Android
```

Attribution challenges

- 1,200 different signing certificates
- 42 Android Debug certificates in 21 brands
- 115 certificates mention “Android” in the issuer field

Main stakeholders

Company name	Number of certificates	Country	Certified partner?
Google	92	United States	N/A
Motorola	65	US/China	Yes
Asus	60	Taiwan	Yes
Samsung	38	South Korea	Yes
Huawei	29	China	Yes
Total (vendors)	740	—	—

Company name	Number of certificates	Country	Number of vendors
MediaTek	19	China	17
Aeon	12	China	3
Tinno Mobile	11	China	6
Verizon Wireless	10	United States	5
<i>Unknown company</i>	7	China	1
Total	460	—	214

AdTech presence

Facebook apps found in over 900 devices, 68% of them being Samsung

Package	Public	# Vendors	# Permissions
com.facebook.system	No	18	2
com.facebook.appmanager	No	15	4
com.facebook.katana (Facebook)	Yes	14	8
com.facebook.orca (Messenger)	Yes	5	5
com.facebook.lite (FB Lite)	Yes	1	1
com.facebook.pages.app	No	1	4
Total	3	24	18

PHAs

- Triada
- Rooting
- Gmobi
- Truecaller
- Adups

How did they get there?

Trouble Over-The-Air: An Analysis of FOTA Apps in the Android Ecosystem

Eduardo Blázquez[†], Sergio Pastrana[†], Álvaro Feal^{*†}, Julien Gamba^{*†}, Platon Kotzias[‡], Narseo Vallina-Rodriguez^{*§} and Juan Tapiador[†]

^{*}IMDEA Networks Institute, [†]Universidad Carlos III de Madrid, [‡]NortonLifeLock Research Group, [§]ICSI



System update downloading...

This update will install a beta version of Android O (OPP2.170420.019) on your Nexus 6P. This pre-release version may contain errors and defects that can affect normal functioning of your device. To learn more about the Android Beta Program or opt out, visit www.android.com/beta. Downloading updates over cellular data or metered Wi-Fi networks may lead to additional charges.

Update size: 1053.3 MB



Pause download

- FOTA: Firmware-Over-The-Air
- Manages Android system updates
- Turns the supply chain into a dynamic process

FOTA stakeholder analysis

Certificate Analysis

```
Owner: CN=www.adups.cn, OU=adups, O=adups, L=pudong, ST=shanghai, C=86  
Issuer: CN=www.adups.cn, OU=adups, O=adups, L=pudong, ST=shanghai, C=86  
Serial number: 75c922a3  
Valid from: Thu Jul 16 14:11:45 CEST 2015 until: Fri Apr 18 14:11:45 CEST 2070  
Certificate fingerprints:  
SHA1: 9E:6D:D3:CB:F6:7E:5A:4F:0F:23:8E:7B:D8:BB:72:E7:3B:A3:86:6B  
SHA256: 41:AB:7D:45:F5:5F:B8:89:02:90:99:E9:8C:68:00:41:8A:6E:9F:80:DA
```

Package name Analysis

```
<?xml version="1.0" encoding="UTF-8"?>  
<manifest android:sharedUserId="android.uid.system"  
  android:versionCode="23"  
  android:versionName="6.0-190580949bf84"  
  package="com.lge.lgfota.permission"  
  platformBuildVersionCode="23"
```

Manual Categorization

OEM:	SoC:
- ...	- ...
- ...	- ...
MNO:	SFD:
- ...	- ...
- ...	- ...

OEM



53%

SoC



9%

MNO



1.6%

SFD



9%



2,013
FOTAs

PHA installations



Package name	Installer	Type	Installations			Children
			Events	Devices	APKs	Mal. APKs (%)
com.samsung.android.app.omcagent		OEM	3.0M	332K	1.9K	29 (1.5%)
com.coloros.sau		OEM	191K	65K	985	28 (3%)
com.android.settings		Unknown	35K	4.7K	1.4K	494 (35%)
com.qiku.android.ota		OEM	310	77	12	11 (92%)

PUP

- Adware
- smsreg
- hiddad

Malware families

- Triada
- Necro
- Guerrilla

Privacy harmful behaviors

SDKs

Category	# libraries	# apps	# vendors	Example
Advertisement	164 (107)	11,935	164	Braze
Mobile analytics	100 (54)	6,935	158	Apptentive
Social networks	70 (20)	6,652	157	Twitter
All categories	334	25,333	165	—

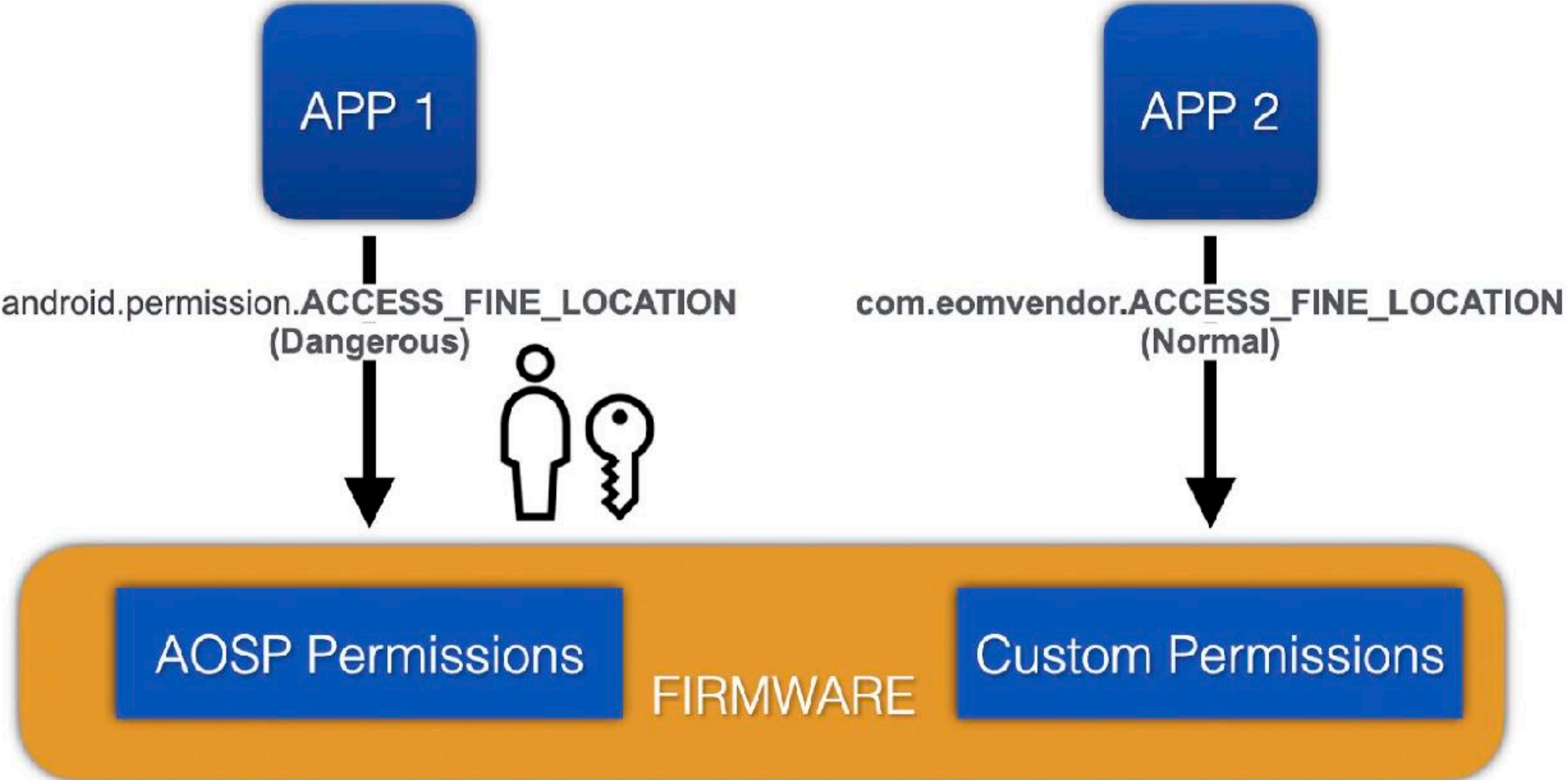
SDKs run with the same privileges as the host app.
This raises transparency concerns.

PII dissemination (static analysis)

Accessed PII type / behaviors		Apps (#)	Apps (%)
Telephony identifiers	IMEI	687	21.8
	IMSI	379	12
	Phone number	303	9.6
	MCC	552	17.5
	MNC	552	17.5
	Operator name	315	10
	SIM Serial number	181	5.7
	SIM State	383	12.1
	Current country	194	6.2
	SIM country	196	6.2
	Voicemail number	29	0.9
Device settings	Software version	25	0.8
	Phone state	265	8.4
	Installed apps	1,286	40.8
	Phone type	375	11.9
	Logs	2,568	81.4
Location	GPS	54	1.7
	Cell location	158	5
	CID	162	5.1
	LAC	137	4.3

Data access customizations

Android custom permissions



Issues

- Can be used to downgrade AOSP permission levels (akin to a confused deputy attack)
- Can enable side channels
- Lack of transparency: users might not be aware of their presence

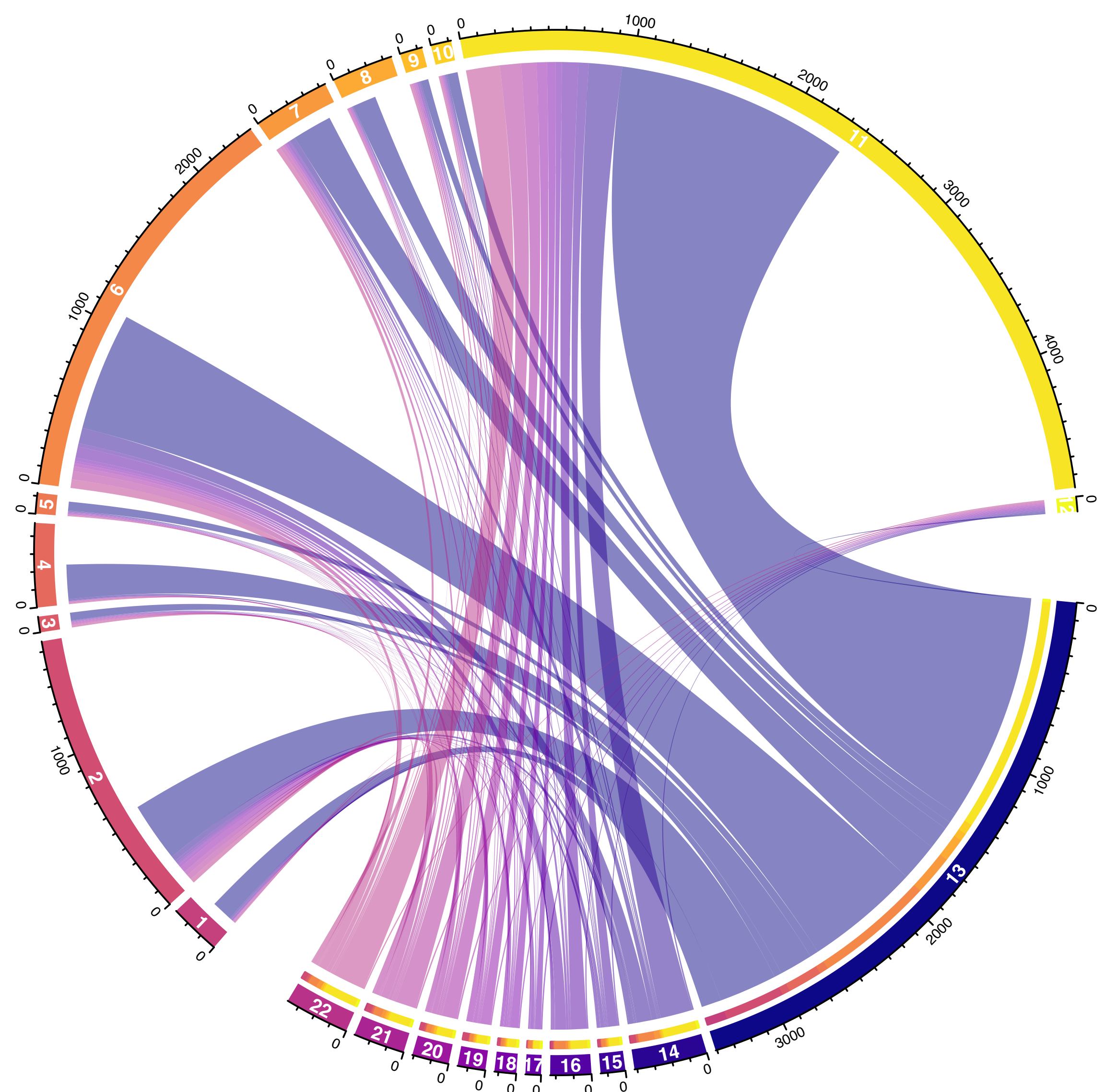
Attribution (again)

Google recommendation:

`com.appdeveloper.CUSTOM_PERMISSION`

But we find:

`com.android.BAIDU_LOCATION_SERVICE`



Origin of defining apps

- Asus
- Huawei
- Lenovo
- Motorola
- Oppo
- Samsung
- Sony
- Vivo
- Xiaomi
- ZTE
- Others
- GMS

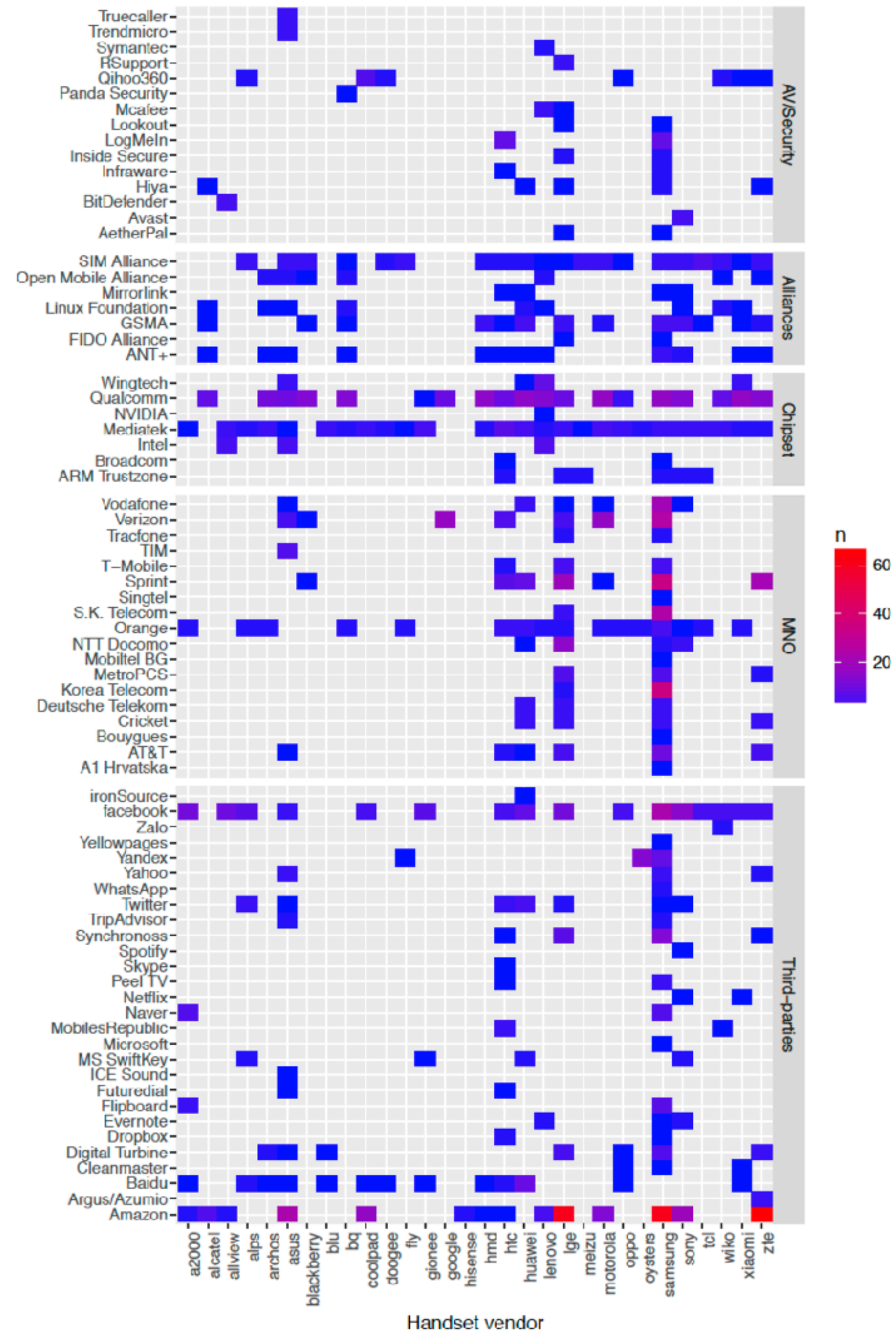
Origin of requesting apps

- Pre-installed
- Google Play
- Qihoo 360
- APK Mirror
- APKMonk
- Baidu
- Huawei store
- Xiaomi Mi
- Tencent
- Other stores

Naming convention violations

Origin	# of definitions	# of bad definitions	Percentage
Google Play	63,193	7,087	■ 11%
Tencent	9,902	1,629	■ 17%
APKMonk	3,060	298	■ 10%
Xiaomi Mi	5,898	1,219	■ 21%
Baidu	4,703	612	■ 13%
APK Mirror	19,543	1,654	■ 9%
Huawei	3,392	464	■ 14%
Qihoo 360	1,999	297	■ 15%
AndroZoo (other stores)	28,636	9,478	■ 33%
Pre-installed	2,237,585	1,045,815	■ 47%
Total	2,373,124	1,067,421	■ 45%

Custom permissions across vendors

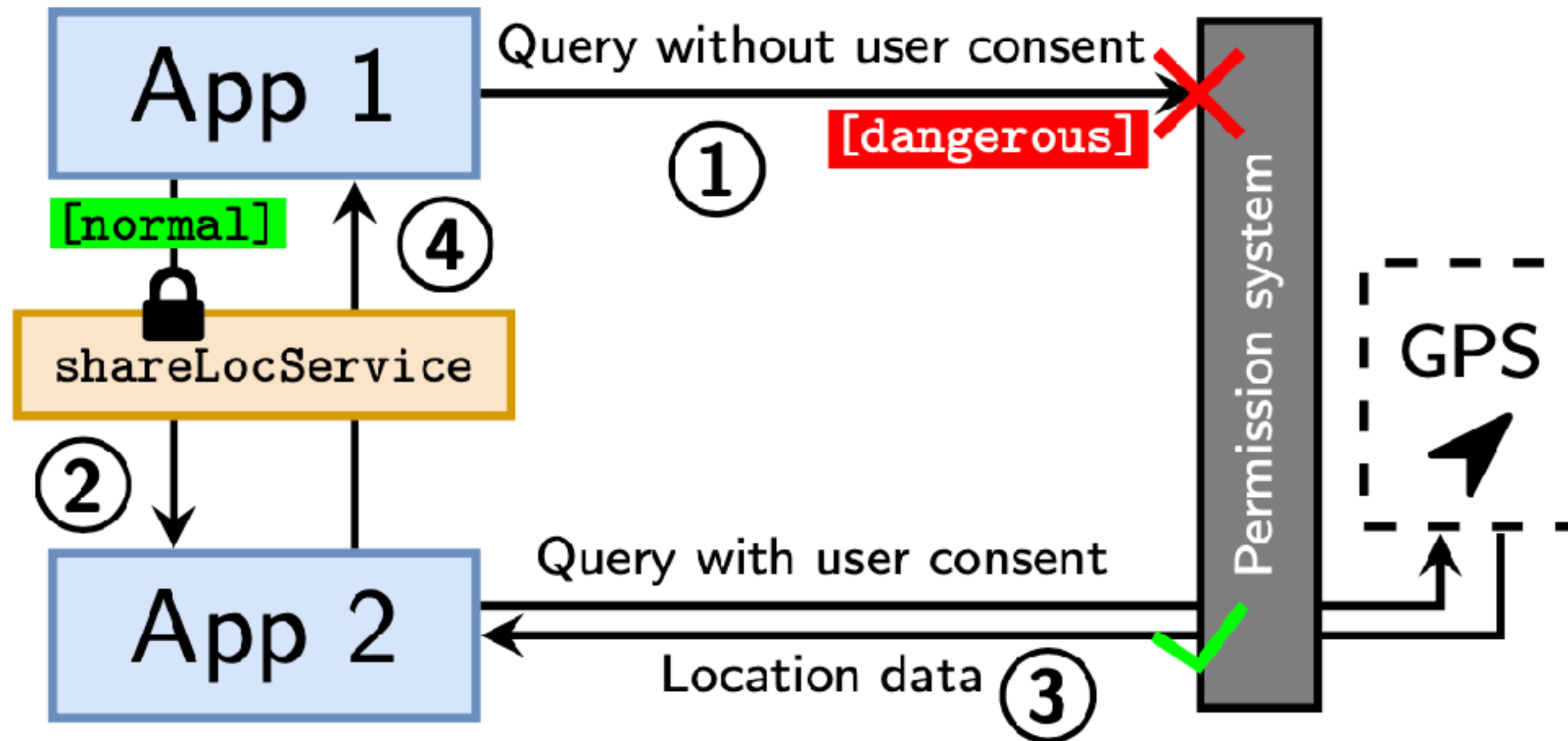


Examples

THIRD-PARTY SERVICE PERMISSIONS

Package name	Developer Signature	Provider	Permission
com.facebook.system	Facebook	Facebook	*.ACCESS
com.facebook.appmanager	Facebook	Facebook	*.ACCESS
com.amazon.kindle	Amazon	Amazon	com.amazon.identity.auth.device.perm.AUTH_SDK
com.huawei.android.totemweather	Huawei (CN)	Baidu	android.permission.BAIDU_LOCATION_SERVICE
com.jrdcom.usercard	TCLMobile (CN)	Baidu	android.permission.BAIDU_LOCATION_SERVICE
com.oppo.findmyphone	Oppo (CN)	Baidu	android.permission.BAIDU_LOCATION_SERVICE
com.android.camera	YuLong (CN)	Baidu	android.permission.BAIDU_LOCATION_SERVICE
com.dti.sliide	Logia	Digital Turbine	com.digitalturbine.ignite.ACCESS_LOG
com.dti.att	Logia	Digital Turbine	com.dti.att.permission.APP_EVENTS
com.ironsource.appcloud.oobe.wiko	ironSource	ironSource	com.ironsource.aura.permission.C2D_MESSAGE
com.vcast.mediamanager	Verizon (US)	Synchronoss	com.synchronoss.android.sync.provider.FULL_PERMISSION
com.myvodafone.android	Vodafone (GR)	Exus	uk.co.exus.permission.C2D_MESSAGE
com.trendmicro.freetmms.gmobi	TrendMicro (TW)	GMobi	com.trendmicro.androidmup.ACCESS_TMMSMU_REMOTE_SERVICE
com.skype.rover	Skype (GB)	Skype	com.skype.android.permission.READ_CONTACTS
com.cleanmaster.sdk	Samsung (KR)	CleanMaster	com.cleanmaster.permission.sdk.clean
com.netflix.partner.activation	Netflix (US)	Netflix	*.permission.CHANNEL_ID

Risks



- Over 250k custom permissions
- Detected over 11k instances of potential protection altered permissions
 - READ_PHONE (3.5k cases)
 - GET_ACCOUNTS (5k cases)
 - LOCATION-related permissions (1.7k cases)

Privacy risks of the Android SDKs

More than 1,000 Android apps harvest data even after you deny permissions

The apps gather information such as location, even after owners explicitly say no. Google says a fix won't come until Android Q.

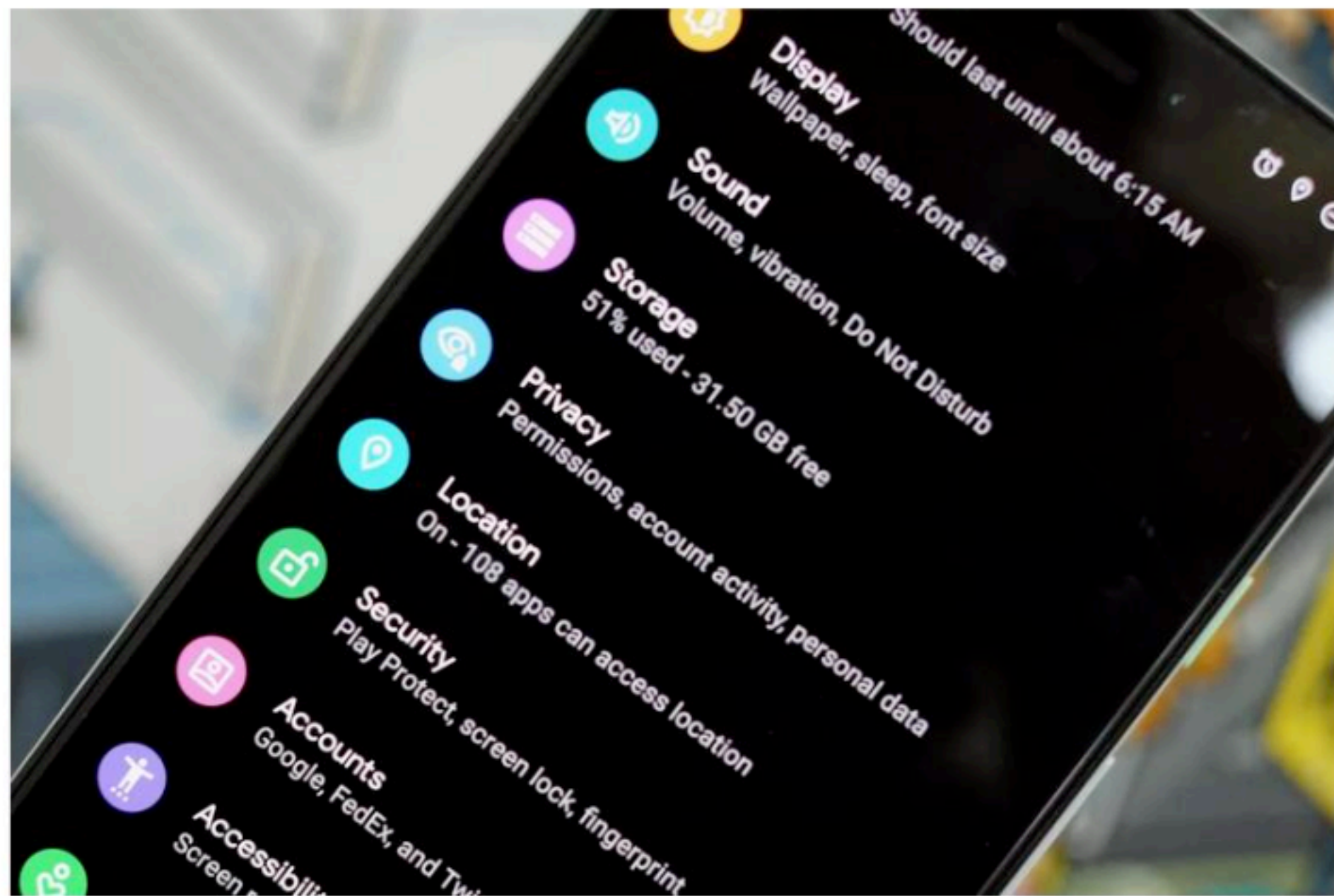


Alfred Ng July 8, 2019 5:00 AM PDT

ES



64



InMobi to pay nearly \$1 million following FTC charges of location tracking deception

The mobile ad platform continued to infer and capture location data on users who had not consented to use of location services.

Digital Advertising Company Settles FTC Charges It Deceptively Tracked Consumers Both Online and Through Their Mobile Devices

Settlement ensures consumers can control targeted ads

Don't Accept Candy from Strangers: An Analysis of Third-Party Mobile SDKs

ÁLVARO FEAL¹, JULIEN GAMBA², JUAN TAPIADOR³, PRIMAL
WIJESEKERA⁴, JOEL REARDON⁵, SERGE EGELMAN⁶ AND NARSEO
VALLINA-RODRIGUEZ⁷

Research questions

- Taxonomy of Android SDKs
- Privacy and regulatory compliance
- Transparency and attribution challenges

SDK categories

Development

*Android Support,
Unity3d*

Network

OK HTTP

Database

ORMLite, Firestore

Crypto

*Jasypt, Bouncy
Castle*

Browser

Chromium

Push Notifications

**Consumer
engagement**
airPush, JPush

Online Payments

AliPay

Maps

*Google Maps,
MapsForge*

Social Networks

Facebook, Twitter

Analytics

Firestore, Flurry

Advertisement

*Google AdMob,
Unity3d*

Privacy: data collection

- Identifiers
 - Resettable (AAID)
 - Non-resettable (Hardware IDs)
- Behavioral data
 - Location

Best practices for unique identifiers

This document provides guidance for selecting appropriate identifiers for your app based on your use case.

For a general look at Android permissions, see [Permissions overview](#). For specific best practices for working with Android permissions, see [App permissions best practices](#).

Best practices for working with Android identifiers

To protect the privacy of your users, use the most restrictive identifier that satisfies your app's use case. In particular, follow these best practices:

1. **Choose user-resettable identifiers whenever possible.** Your app can achieve most of its use cases even when it uses identifiers other than non-resettable hardware IDs.
2. **Avoid using hardware identifiers.** In most use cases, you can avoid using hardware identifiers, such as International Mobile Equipment Identity (IMEI), without limiting required functionality.

Android 10 (API level 29) adds restrictions for non-resettable identifiers, which include both IMEI and serial number. Your app must be a [device or profile owner app](#), have [special carrier permissions](#), or have the `READ_PRIVILEGED_PHONE_STATE` privileged permission in order to access these identifiers.
3. **Only use an Advertising ID for user profiling or ads use cases.** When using an [Advertising ID](#), always [respect users' selections regarding ad tracking](#). If you must connect the advertising identifier to personally-identifiable information, do so only with the [explicit consent of the user](#).
4. **Don't bridge Advertising ID resets.**
5. **Use a Firebase installation ID (FID) or a privately stored GUID whenever possible for all other use cases, except for payment fraud prevention and telephony.** For the vast majority of non-ads use cases, an FID or GUID should be sufficient.
6. **Use APIs that are appropriate for your use case to minimize privacy risk.** Use the [DRM API](#) for high-value content protection and the [SafetyNet APIs](#) for abuse protection. The SafetyNet APIs are the easiest way to determine whether a device is genuine without incurring privacy risk.

The remaining sections of this guide elaborate on these rules in the context of developing Android apps.

Work with advertising IDs

The Advertising ID is a user-resettable identifier and is appropriate for ads use cases. There are some key points to bear in mind, however, when you use this ID:

Always respect the user's intention in resetting the advertising ID. Don't bridge user resets by using another identifier or fingerprint to link subsequent Advertising IDs together without the user's consent. The [Google Play Developer Content Policy](#) states the following:

Privacy: custom events



User XYYY clicked button "My profile" →

User XYYY changed "Age" setting →

User XYYY sent "Super Heart" to user ZZAA →



Privacy: custom events

Family ▾ Subcategories ▾ Home Top charts New releases

Recommended for you

- Pokémon Quest** - The Pokémon Company (★★★★☆)
- Crossy Road** - HIPSTER WHALE (★★★★★)
- Red Ball 4** - FDG Entertainment GmbH (★★★★★)
- Brain It On! - Physics** - Orbital Nine Games (★★★★☆)
- Bricks Breaker - Gl** - Big Cat Studio - we make (★★★★★)

New + Updated

- Math Games, Learn** - GunjanApps Studios (★★★★★)
- Sluggterra: Slug it Out** - Epic Story Interactive (★★★★★)
- Cooking Mama: Let's** - Office Create Corp. (★★★★★)
- ANTON - Lernen - G** - ANTON - die kostenlose (★★★★★)
- Disney Magic King** - Gameloft SE (★★★★★)

Google Play self-certified ad networks program

⚠️ If you're an ad network that applied for this certification before 9/1 and you haven't received a decision yet, your submission is currently in review.

If your app uses an ad network that was in review before 9/1, we will not enforce on these networks until a decision is made. Please contact your ad network for their certification status.

COPPA Safe Harbor Program

The Children's Online Privacy Protection Act (COPPA) includes a provision enabling industry groups or others to submit for Commission approval self-regulatory guidelines that implement the protections of the Commission's final Rule. The COPPA requires the Commission to act on a request for "safe harbor" treatment within 180 days of the filing of the request, and after the proposed guidelines have been subject to notice and comment. Section 312.10 of the final Rule sets out the criteria for approval of guidelines and the materials that must be submitted as part of a safe harbor application.

List of currently approved Safe Harbor organizations (in alphabetical order):

- Aristotle International Inc.
- Children's Advertising Review Unit (CARU)
- Entertainment Software Rating Board (ESRB)
- iKeepSafe
- kidSAFE
- Privacy Vaults Online, Inc. (d/b/a PRIVO)
- TRUSTe

- [IronSource](#)
- [Kidoz](#)
- [StartApp](#)
- [SuperAwesome](#)
- [Unity Ads](#)
- [Vungle](#)

Privacy: cross-device tracking

About the Cross Device reports

Connect data from multiple sessions to see the conversion process from start to finish.

The Cross Device reports give you the tools you need to organize data across multiple devices into a cohesive analysis, so you get a better idea of how seemingly unrelated touch points, sessions, and interactions are connected.

For example, you might discover that one segment of users searches on a mobile device and purchases on a tablet within the same day, while another segment clicks an ad on a mobile device, browses your site on a desktop the next day, and returns to make a purchase on a tablet a week later.

The Cross Device reports help you connect data about devices and activities from different sessions so you can get a better understanding of your users and what they do at each step of the conversion process - from initial contact to long-term retention.

Research questions (ongoing work)

- Detection
- Attribution
- Measuring prevalence
- Compliance

Thank you!

Juan Tapiador

Universidad Carlos III de Madrid

Web: 0xjet.github.io

Twitter: @0xjet