CSE508 Network Security

Stony Brook University

2021-04-29

Privacy

Michalis Polychronakis

Stony Brook University

Privacy

"The right of an entity (normally a person), acting in its own behalf, to determine the degree to which it will interact with its environment, including the degree to which the entity is willing to share information about itself with others." [RFC2828]

Beyond private data (messages/files):

- Activities (browsing history, daily routine, voice commands, …)
- Location (3/4G, GPS, WiFi, cameras, …)
- Preferences ("likes," Amazon, Netflix, …)
- Health (Fitbit, iWatch, …)
- …

Real-world Privacy

Large-scale data collection examples

- Credit cards, Metrocards, loyalty cards
- Street/public space cameras, tolls, badge readers
- Named tickets (travel, events, services)
- …

Part of our everyday activities and personal information is (voluntarily or compulsorily) recorded

- Information from different sources can be **correlated**
- *Did you buy your Metrocard with your credit card?*

The same happens in the online world…

Third parties have access to…

Our email (Gmail, Yahoo, …)

Our files (Dropbox, Google Drive, …)

Our finances (e-banking, credit reporting, Mint, …)

Our communication (Instant messengers, Zoom, …)

Our traffic (WiFi hotspots, ISPs, …)

Our location (3/4/5G, GPS, WiFi, BLE, …)

Our activities (browsing history, daily routine, …)

Our preferences ("Likes," Amazon, Netflix, …)

Our health (Fitbit, iWatch, 23andMe, …)

…

Hacking of Government C

www.nytimes.com/2015/07/10/us/office-of-personnel-management-hackers-got-data-of-millions.html?emc=edit_na_2015

U.S. | Hacking of Government Computers Exposed 21.5 Million People

MORE

Hacking of Government Computers Exposed 21.5 Million People

By JULIE HIRSCHFELD DAVIS JULY 9, 2015

Katherine Archuleta, director of the Office of Personnel Management, right, at hearing before the House Oversight and Government Reform Committee last month. Mark Wilson/Getty Images

Email

WASHINGTON — The Obama administration on Thursday revealed that 21.5 million people were swept up in a colossal breach of government computer systems that was far more damaging than

US news

Credit firm Equifax says 143m Americans' social security numbers exposed in hack

- **Atlanta-based company says 'criminals' accessed personal data**
- **Before notifying public, Equifax executives sold $1.8m in shares**

▲ Equifax says 143 million Americans' data was breached. Photograph: Mike Stewart/AP

Olivia Solon *in San Francisco*
@oliviasolon

Thu 7 Sep 2017 21.05 EDT

768

Credit monitoring company Equifax says a breach exposed the social security numbers and other data of about 143 million Americans.

After discovering the breach, but before notifying the public, three Equifax senior executives sold shares in the company worth almost $1.8m. Since the public announcement, the company's share price has tumbled.

The Atlanta-based company said Thursday that "criminals" exploited a US website application to access files between mid-May and July of this year.

It said consumers' names, social security numbers, birth dates, addresses and, in some cases, driver's license numbers were exposed. Credit card numbers for about 209,000 US consumers were also accessed.

"This is clearly a disappointing event for our company, and one that strikes at the heart of who we are and what we do," said the company's chairman and

World's Biggest Data Breaches & Hacks

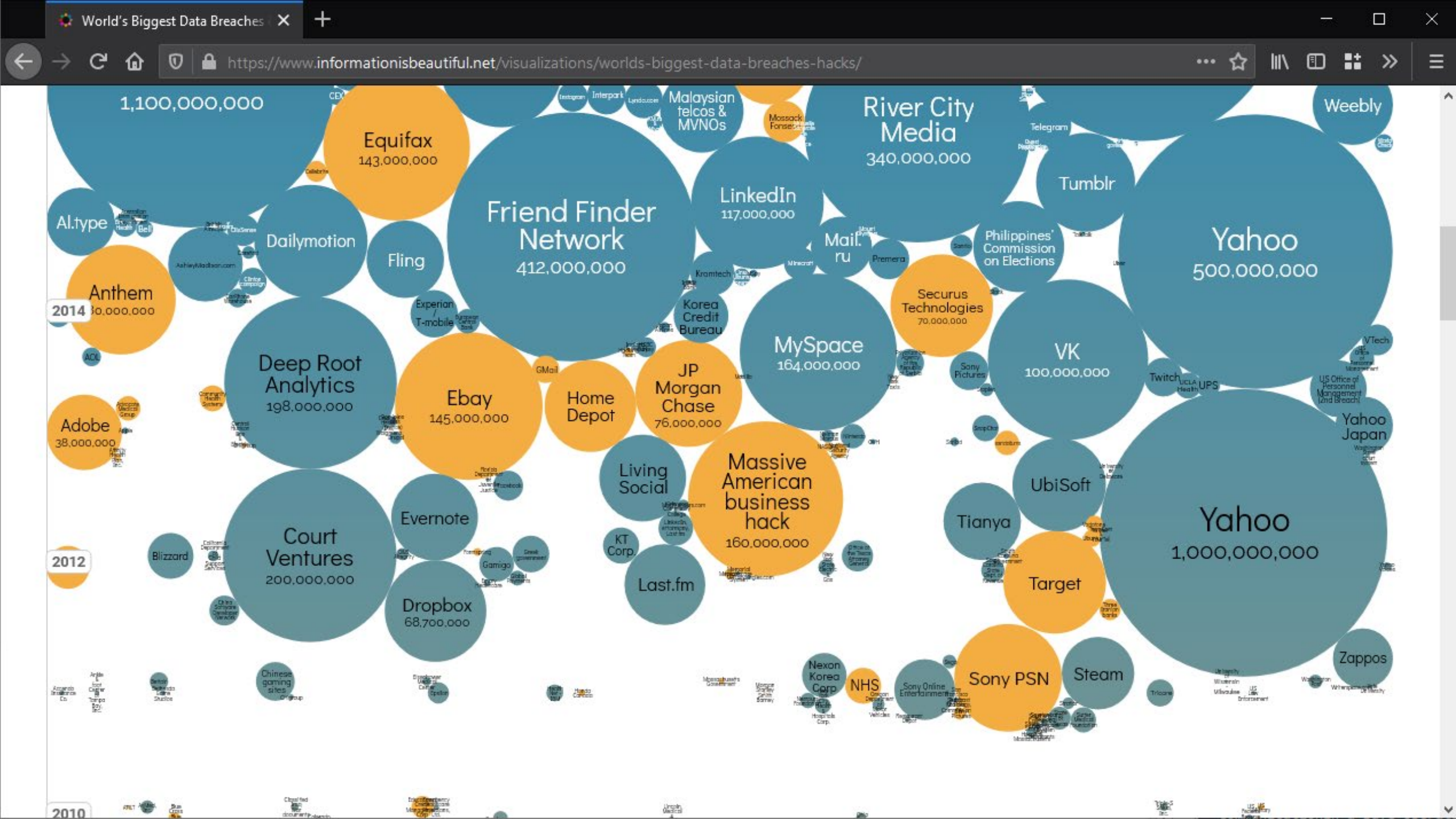
interesting story

Selected events over 30,000 records

UPDATED: Jan 2021

size: records lost **filter**

search...


World's Biggest Data Breaches
https://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/
1,100,000,000
Equifax
143,000,000
Malaysian telcos & MVNOs
River City Media
340,000,000
Weebly
Telegram
Tumblr
Friend Finder Network
412,000,000
LinkedIn
117,000,000
Mail.ru
Philippines' Commission on Elections
Yahoo
500,000,000
Al.type
Dailymotion
Fling
Premera
Securus Technologies
70,000,000
Anthem
80,000,000
2014
Experian / T-mobile
Korea Credit Bureau
MySpace
164,000,000
VK
100,000,000
Sony Pictures
Twitch
UPS
VTech
US Office of Personnel Management (2nd Breach)
Deep Root Analytics
198,000,000
Ebay
145,000,000
Home Depot
JP Morgan Chase
76,000,000
Adobe
38,000,000
Yahoo Japan
Living Social
Massive American business hack
160,000,000
UbiSoft
Tianya
Yahoo
1,000,000,000
Evernote
Court Ventures
200,000,000
Blizzard
2012
KT Corp.
Last.fm
Target
Dropbox
68,700,000
Zappos
Chinese gaming sites
Nexon Korea Corp
NHS
Sony Online Entertainment
Sony PSN
Steam
2010

SAVE BIG SUBSCRIBE TODAY

The Netanyahu Disaster
By Jeffrey Goldberg

The Effects of Forgiveness
By Olga Khazan

Rural America's Silent Housing Crisis
By Gillian B. White

Introducing the Supertweet
By Ian Bogost

Armed With Facebook 'Likes' Alone, Researchers Can Tell Your Race, Gender, and Sexual Orientation

REBECCA J. ROSEN | MAR 12 2013, 2:59 PM ET

But the deeper aspects of your personality remain hard to detect.

VIDEO

How to Build a Tornado

A Canadian inventor believes his tornado machine could solve the world's energy crisis.

MORE IN TECHNOLOGY

Introducing the Supertweet
IAN BOGOST

My Parents' Facebook Will
JAKE SWEARINGEN

Facebook knows you're g

americablog.com/2013/03/facebook-might-know-youre-gay-before-you-do.html

CONTRIBUTE TAKE ACTION CONTACT/TIPS ADVERTISING ABOUT US

Google™ Custom Search

AMERICAblog
GAY - A GREAT NATION DESERVES EQUALITY

LGBT Obamacare Videos Climate Pets Fun Stuff Author Archives

Like 6.6k Follow @americabloggay 48.1K followers

HOME › GAY › FACEBOOK KNOWS YOU'RE GAY BEFORE YOU DO

Facebook knows you're gay before you do

3/20/13 4:29pm by Jon Green 39 Comments

Like 2k Tweet 761 3 points g+1 39

Am I the only one creeped out that Facebook is now guessing, sometimes correctly, if its users are gay?

In the world of Big Data, our private lives are increasingly becoming intermingled with the shadowy, yet public, world of cyberspace.

Whenever we go online we are providing data that can be used to market to us; from Google searches to Facebook likes to eBay purchases, we are inputting data into a series of mathematical models which make *incredibly* educated guesses about the kinds of people we are.

Facebook creepily offers help to a gay guy thinking of "coming out"

Enter Matt. As BuzzFeed notes, Matt was your typical Facebook user who suddenly found an ad in his news feed for help in coming out. The weird thing was that Matt "did" need help coming out, and understandably he was more than a bit curious as to how Facebook knew.

At first, Matt wondered if Facebook had accessed his text messages, as he had confided in a close friend the previous

LATEST COMMENTS TAGS

Let's slow down this race, together: Starbuc and a bad hashtag
3/20/15 12:00pm 7 Comments

It's time to make college free
3/20/15 10:00am 19 Comments

Rick Perry's new adviser has suggested tha God isn't #ReadyForHillary. Technically, he right.
3/20/15 8:00am 14 Comments

Fatwas, gay sex tourism and the Indonesian LGBT underground
3/19/15 10:00am 6 Comments

Support AMERICAblog

Click here to donate securely via PayPal

We Recommend

Parallels between India's sexism and America's racism

Facebook users unwitting

www.theguardian.com/technology/2013/mar/11/facebook-users-reveal-intimate-secrets

sign in subscribe search jobs US edition

theguardian
Winner of the Pulitzer prize

US world opinion sports soccer tech arts lifestyle fashion business travel environment science all

home › tech

Facebook

Facebook users unwittingly revealing intimate secrets, study finds

Personal information including sexuality and drug use can be correctly inferred from public 'like' updates, according to study

Most popular in US

Barcelona v Real Madrid: El Clásico - live! Jacob Steinberg

The eight best young adult books - and why grownups should read them, too

Singapore's Lee Kuan Yew dies aged 91

How Smart TVs in Millions of U.S. Homes Track More Than What's On Tonight

By Sapna Maheshwari

July 5, 2018

The growing concern over online data and user privacy has been focused on tech giants like Facebook and devices like smartphones. But people's data is also increasingly being vacuumed right out of their living rooms via their televisions, sometimes without their knowledge.

In recent years, data companies have harnessed new technology to immediately identify what people are watching on internet-connected TVs, then using that information to send targeted advertisements to other devices in their homes. Marketers, forever hungry to get their products in front of the people most likely to

China Is Using Facial Recognition Technology to Send Jaywalkers Fines Through Text Messages

It's the latest update to a widely deployed facial recognition surveillance system in China.

By Daniel Oberhaus

March 28, 2018, 8:00am Share Tweet Snap

In China, law enforcement agencies have been using advanced biometric technology to track citizens for years. These technologies are part of a coordinated national effort to create the "omnipresent, completely

MORE LIKE THIS

Tech

How Target Figured Out A

www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/

Forbes | New Posts +1 | Most Popular | Lists | Video | Subscribe to Forbes | Search

TECH 2/16/2012 @ 11:02AM | 2,698,356 views

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

+ Comment Now + Follow Comments

Share

Next Post

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, 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

Charles Duhigg outlines in the New York Times how Target tries to hook parents-to-be at that crucial moment before they turn into rampant — and

CONFERENCES AND MORE

Web Browsing Tracking

Webpages are often mashups of content loaded from different sources

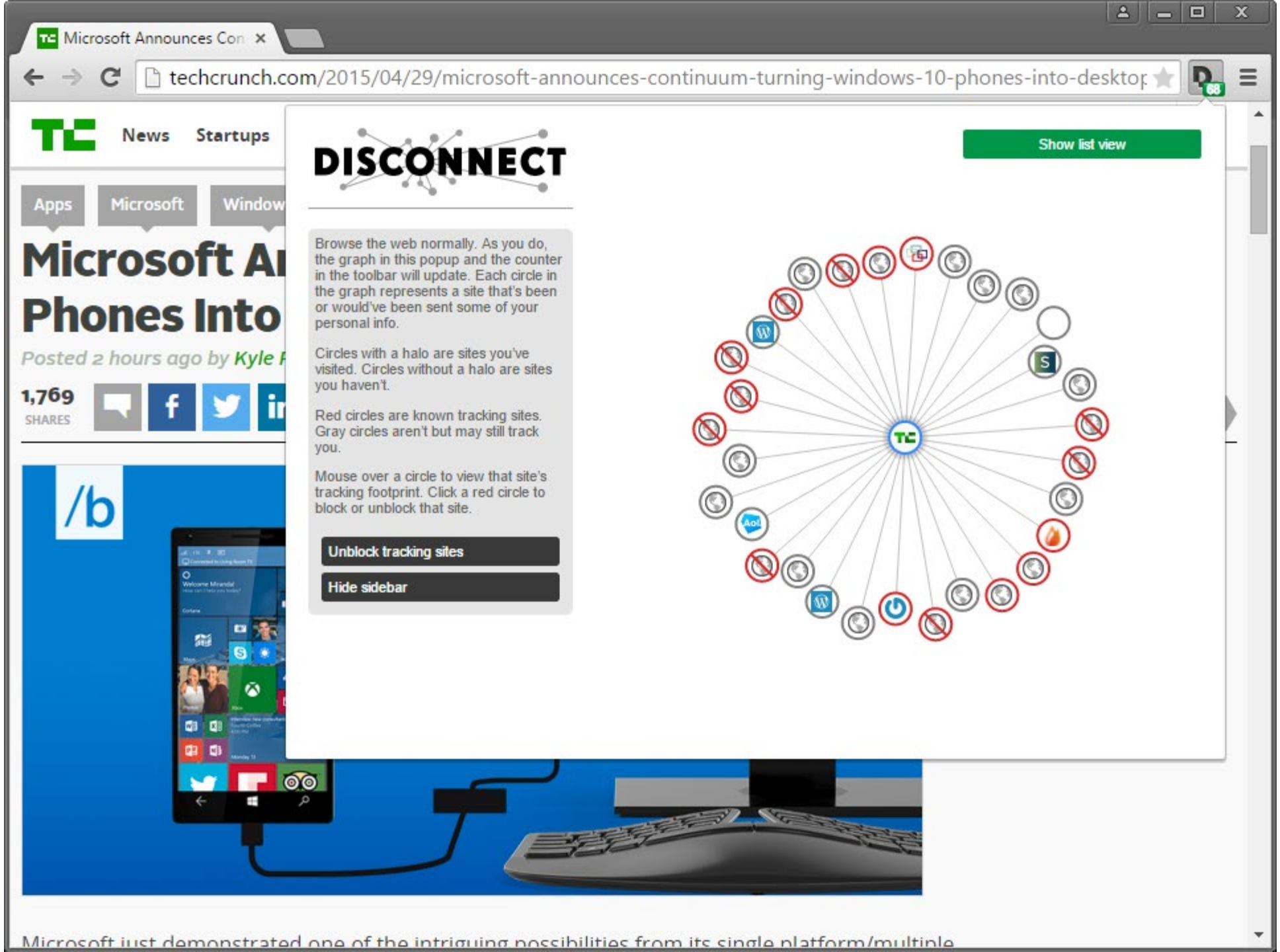
- Ads, images, videos, widgets, …
- IMG URLs, IFRAMEs, JavaScript, web fonts, social widgets, …
- Hosted on third-party servers: CDNs, cloud providers, ad networks, …

A third party involved in many different websites can track user visits across all those websites

- Multiple third parties may collude to expand their collective "view"

Trackers want to learn two key pieces of information

- **What webpage was visited**
- **Who visited it**


Microsoft Announces Con
techcrunch.com/2015/04/29/microsoft-announces-continuum-turning-windows-10-phones-into-desktop
News
Startups
Apps
Microsoft
Window
Microsoft A
Phones Into
Posted 2 hours ago by Kyle
1,769
SHARES
/b
DISCONNECT
Show list view
Browse the web normally. As you do, the graph in this popup and the counter in the toolbar will update. Each circle in the graph represents a site that's been or would've been sent some of your personal info.
Circles with a halo are sites you've visited. Circles without a halo are sites you haven't.
Red circles are known tracking sites. Gray circles aren't but may still track you.
Mouse over a circle to view that site's tracking footprint. Click a red circle to block or unblock that site.
Unblock tracking sites
Hide sidebar
Microsoft just demonstrated one of the intriguing possibilities from its single platform/multiple

What webpage was visited?

HTTP Referer [sic] header

- The full URL of the webpage from which a link was followed
- Useful for statistics/analytics, bad for privacy
- Can be turned off trough browser options/extensions
- HTML5 `rel="noreferrer"` anchor attribute to indicate to the user agent not to send a referrer when following the link
- Most browsers have started sending only the origin part in cross-origin requests

Page-specific, session-specific, user-specific URLs

- Unique URL per page (even for the same resource) ➔ track what page was visited
- Unique URL per session/user ➔ distinguish between visits from different users

Firefox 87 trims HTTP Referrers by default to protect user privacy

Dimi Lee and Christoph Kerschbaumer | March 22, 2021

We are pleased to announce that Firefox 87 will introduce a stricter, more privacy-preserving default Referrer Policy. From now on, by default, Firefox will trim path and query string information from referrer headers to prevent sites from accidentally leaking sensitive user data.

Referrer headers and Referrer Policy

Browsers send the HTTP Referrer header (note: original specification name is 'HTTP Referer') to signal to a website which location "referred" the user to that website's server. More precisely, browsers have traditionally sent the full URL of the referring document (typically the URL in the address bar) in the HTTP Referrer header with virtually every navigation or subresource (image, style, script) request. Websites can use referrer information for many fairly innocent uses, including analytics, logging, or for optimizing caching.

Unfortunately, the HTTP Referrer header often contains private user data: it can reveal which articles a user is reading on the referring website, or even include information on a user's account on a website.

Tracking URLs are also commonly used in promotional emails

Embedded image loading

- This is an active email address! Detect the time a user viewed a message
- The request reveals much more: user agent, device, location, …

Embedded links

- Learn which email addresses resulted in visits (click-through rate)

Default behavior of email clients varies

- Gmail used to block images by default, now uses image proxy servers
- Tracking through unique images still possible: senders can track the first time a message is opened (user's IP is not exposed though)

Who visited the page?

Browsing to a web page reveals a wealth of information

Source IP address

Not very accurate (e.g., NAT, DHCP, on-the-go users) but still useful

Third-party cookies: precise user tracking

Easy to block (configurable in most browsers, defaults vary)

"Evercookies:" exploit alternative browser state mechanisms

ETags, HTML5 session/local/global storage, plugin-specific storage, …

Browser/device fingerprinting: recognize unique system characteristics

Browser user agent, capabilities, plugins/extensions, system fonts, screen resolution, time zone, and numerous other properties

Cookie Status

Search...

Current status
Introduction
Brave
Chrome
Edge
Firefox
Safari
Cliqz

MORE

Glossary

	Brave	Chrome	Edge	Firefox	Safari
Mechanism	Shields	n/a	Tracking prevention	Enhanced Tracking Protection (ETP)	Intelligent Tracking Prevention (ITP)
Deployed in	0.55.18	n/a	78.0.276.8	69.0	Safari 11
Default protection mode	Default Shield settings	n/a	Balanced	Standard	ITP enabled
Classification of "known trackers"	Multiple filter lists	n/a	Trust Protection Lists (with engagement and organization mitigation)	Disconnect.me	Algorithmic
Cookies in 3rd party context	Restrict access in subresource requests. Partitioned access in frame. Partitioned	No restrictions.	Access restricted for known trackers.	Access restricted for known trackers.	All access restricted, except with Storage Access API.

HOW TO READ YOUR REPORT

You will see a summary of your overall tracking protection. The first section gives you a general idea of what your browser configuration is blocking (or not blocking). Below that is a list of specific browser characteristics in the format that a tracker would view them. We also provide descriptions of how they are incorporated into your fingerprint.

HOW CAN TRACKERS TRACK YOU?

Trackers use a variety of methods to identify and track users. Most often, this includes tracking cookies, but it can also include browser fingerprinting. Fingerprinting is a sneakier way to track users and makes it harder for users to regain control of their browsers. This report measures how easily trackers might be able to fingerprint your browser.

HOW CAN I USE MY RESULTS TO BE MORE ANONYMOUS?

Knowing how easily identifiable you are, or whether you are currently blocking trackers, can help you know what to do next to protect your privacy. While most

Here are your Cover Your Tracks results. They include an overview of how visible you are to trackers, with an index (and glossary) of all the metrics we measure below.

IS YOUR BROWSER:

Blocking tracking ads?	**Yes**
Blocking invisible trackers?	**Yes**
Protecting you from fingerprinting?	**Your browser has a unique fingerprint**

Note: because tracking techniques are complex, subtle, and constantly evolving, Cover Your Tracks does not measure all forms of tracking and protection.

Your Results

Your browser fingerprint **appears to be unique** among the 273,004 tested in the past 45 days.

Currently, we estimate that your browser has a fingerprint that conveys **at least 18.06 bits of identifying information.**

The measurements we used to obtain this result are listed below. You can **read more about our methodology, statistical results, and some defenses against fingerprinting here**.

What do web tracking techniques really track?

Distinguish between different visitors

Track anonymous individuals

Actually: track the pages visited by a particular browser running on a particular device

Better: distinguish between different *persons*

Track named individuals

The transition is easy…

Personally identifiable information (PII) is often voluntarily provided to websites:

Social networks, cloud services, web sites requiring user registration, …

Cookies/sessions are associated with PII

Contamination: trackers may collude with services

Previously "anonymous" cookies/fingerprints can be associated with named individuals

Verizon's 'Perma-Cookie'

www.wired.com/2014/10/verizons-perma-cookie/

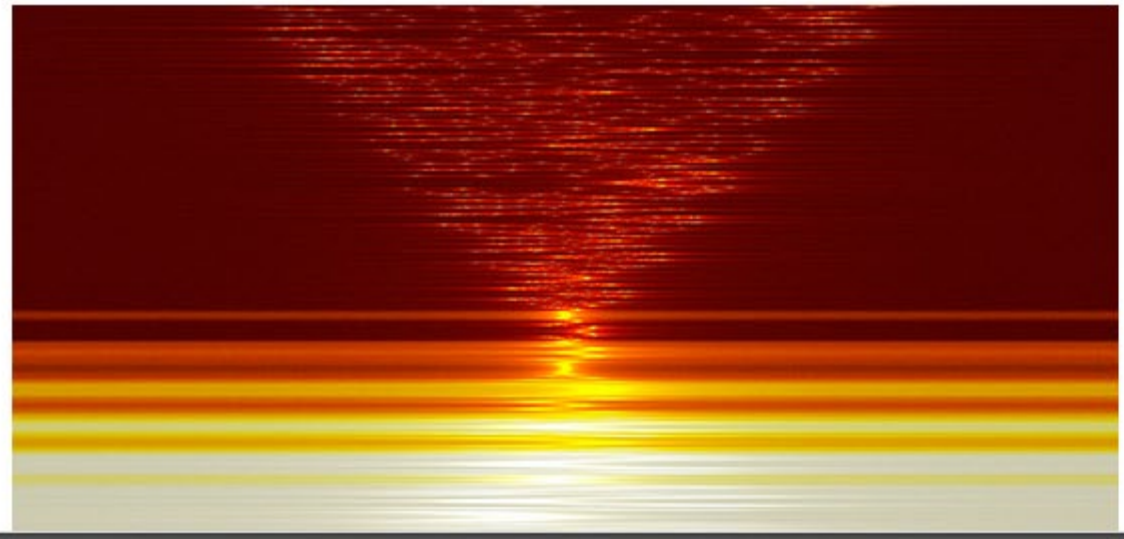
WIRED

SUBSCRIBE

BUSINESS | DESIGN | ENTERTAINMENT | GEAR | SCIENCE | SECURITY

ROBERT MCMILLAN 10.27.14 6:30 AM

VERIZON'S 'PERMA-COOKIE' IS A PRIVACY-KILLING MACHINE



LATEST NEWS

JAKOB SCHILLER

Stunning Snowy Landscapes from the Edge of the Earth

3 MINS

SPACE

Jeff Bezos' Blue Origin Just Launched Its Flagship Rocket

14 MINS

SCIENCE

An Atlas of the Bacteria and Fungi We Breathe Every Day

1 HOUR

DESIGN

The Age of Drone

AT&T charges $29 more f

arstechnica.com/business/2015/02/att-charges-29-more-for-gigabit-fiber-that-doesnt-watch-your-web-browsing/

Register Log in

ars technica

MAIN MENU MY STORIES: 25 FORUMS SUBSCRIBE JOBS ARS CONSORTIUM

MINISTRY OF INNOVATION / BUSINESS OF TECHNOLOGY

AT&T charges $29 more for gigabit fiber that doesn't watch your Web browsing

AT&T goes head to head against Google in KC on fiber and targeted ads.

by Jon Brodkin - Feb 16, 2015 12:38pm EST

Share Tweet 205

AT&T

AT&T's gigabit fiber-to-the-home service has just arrived in Kansas City, and the price is the same as Google Fiber—if you let AT&T track your Web browsing history.

LATEST FEATURE STORY

FEATURE STORY (2 PAGES)

Battlefield Hardline review: an odd, cops-and-robbers facade

New twists on old formula help in multiplayer, baffle in single player.

WATCH ARS VIDEO

T-Mobile will sell your web-usage data to advertisers unless you opt out

Data sales begin April 26 unless you opt out; T-Mobile claims it'll be anonymous.

JON BRODKIN - 3/9/2021, 5:35 PM

113

T-Mobile next month will start a new program that gives customers' web-browsing and device-usage data to advertisers unless customers opt out of the data sharing.

"[S]tarting April 26, 2021, T-Mobile will begin a new program that uses some data we have about you, including information we learn from your web and device usage data (like the apps installed on your device) and interactions with our products and services for our own and 3rd party advertising, unless you tell us not to," T-Mobile said in a privacy notice. "When we share this information with third parties, it is not tied to your name or information that directly identifies you."

For directions on how to opt out of the expanded data sharing, see the first section of the T-Mobile privacy notice. We've heard from customers who say they've had problems opting out so you may have to try multiple links or make multiple attempts. There's another list of opt-out links here and a link here to change the "Do Not Sell" setting. "T-Mobile will not sell personal data to third parties when you tell us not to," the company's privacy notice said.

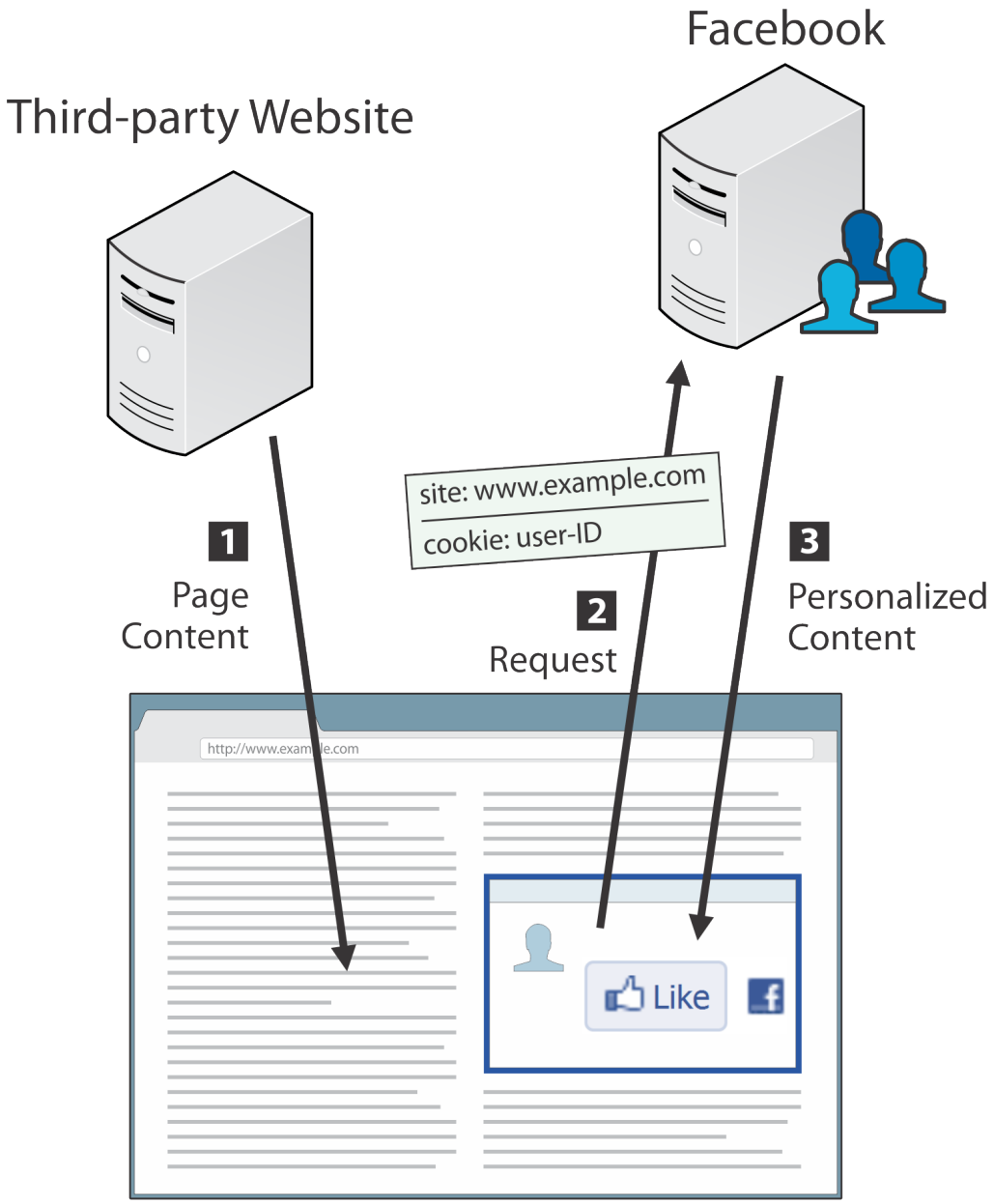
Users register on trackers!

Social widgets are prevalent

- 2.8+ billion Facebook (monthly active) users
- Twitter, LinkedIn, Pinterest, AddThis, …
- OS/app integration

A growing part of our browsing history can be tracked by social networking services

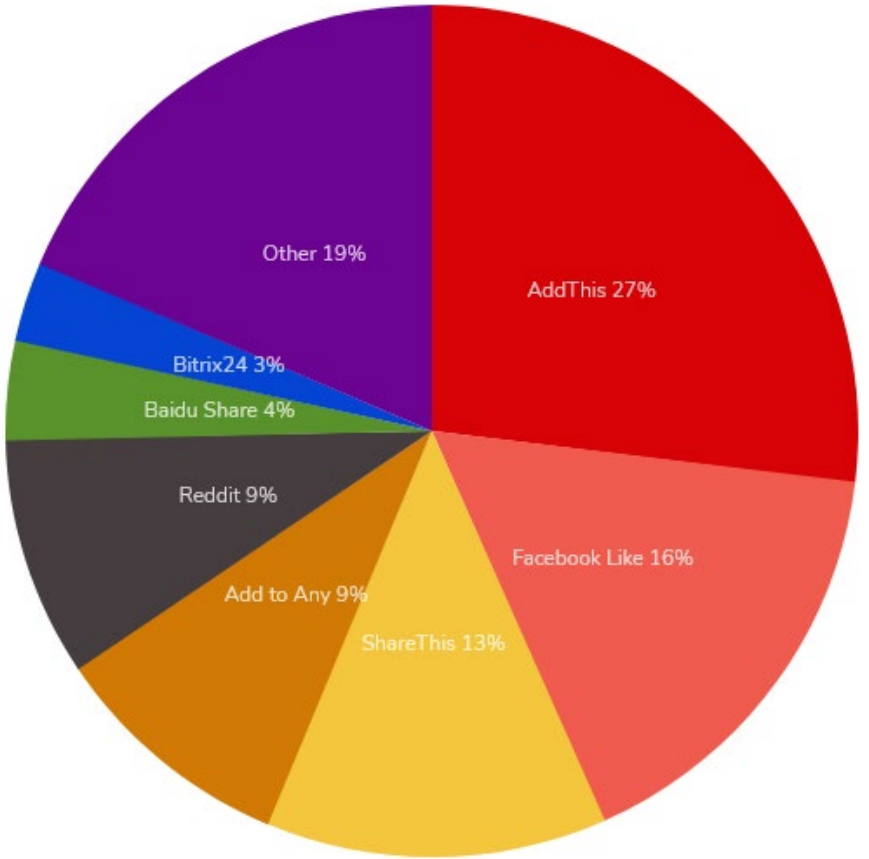
- Not as merely anonymous visitors, but as ***named persons***
- Just visiting the page is enough (no interaction needed)
- Cross-device tracking


Facebook
Third-party Website
site: www.example.com
cookie: user-ID
1
Page Content
2
Request
3
Personalized Content
http://www.example.com
Like

Social Sharing Usage Distribution in the Top 1 Million Sites

Top In Social Sharing Usage Distribution in the Top 1 Million Sites

Technology	Websites	%
AddThis	61,528	6.15
Facebook Like	37,506	3.75
ShareThis	29,531	2.95
Add to Any	21,180	2.12
Reddit	20,724	2.07
Baidu Share	8,567	0.86
Bitrix24	6,861	0.69
Yotpo	4,232	0.42
Sassy Social Share	4,225	0.42
POWr	2,882	0.29
Instagram API	2,791	0.28
Sina Weibo	2,531	0.25
Facebook Embedded Posts	1,834	0.18
Juicer	1,818	0.18
bShare	1,608	0.16



Existing Solutions

Log out

- Some cookies persist

Block third-party cookies

- Not always effective

Block social widgets completely

Incognito mode

All existing solutions disable content personalization

- Privacy vs. functionality dilemma

First Party Isolation (Firefox)

AKA Cross-Origin Identifier Unlinkability (Tor Browser)

All identifier sources and browser state are scoped (isolated) using the URL bar domain

- Cookies, cache, HTTP Authentication, DOM Storage, Flash cookies, SSL and TLS session resumption, HSTS and HPKP supercookies, OCSP, …

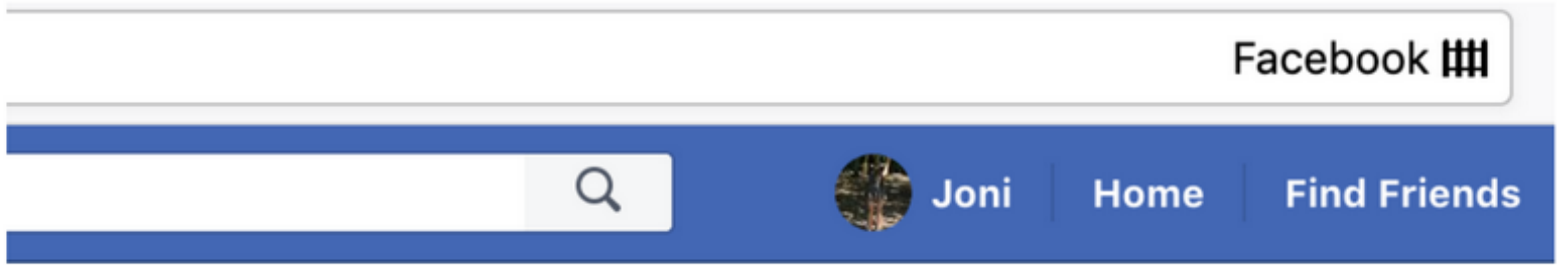
Example: `tracker.com` sets/reads cookies in `bbc.com` and `cnn.com`

- Before: `tracker.com` can track the same person on both sites
- After: `tracker.com` will see two different cookies
- Third party cookies are stored with a tag of the first party (e.g., `bbc.com.tracker.com` and `cnn.com.tracker.com`)

How does Facebook Container work?

The Facebook "Like" and "Share" buttons that appear on shopping, news and other sites contain Facebook trackers. Even if you don't use them, Facebook uses these buttons to track you. Facebook Container blocks these trackers and will display a fence icon to show you where these trackers were removed.

When you visit Facebook, the add-on loads it in another tab and the fence icon is displayed in your address bar. This puts Facebook in its own boundary with other Facebook-owned sites, including Instagram and Messenger. You can allow other sites into the Facebook Container boundary, but this will allow Facebook to track more of your web activity.



When you visit a non-Facebook site that has Facebook trackers, Facebook Container will alert you and block these trackers.

You can add a website to Facebook Container if you prefer to allow Facebook to see your activity on that site.

Was this article helpful?

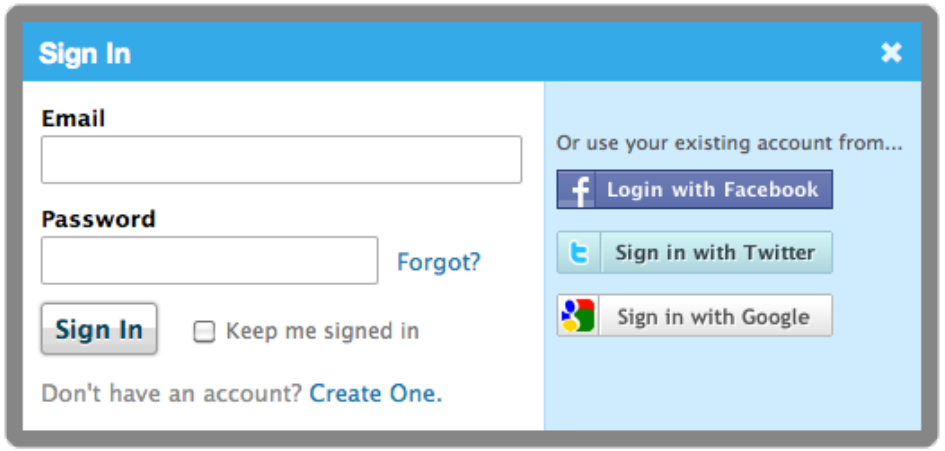
Single Sign-on/Social Login

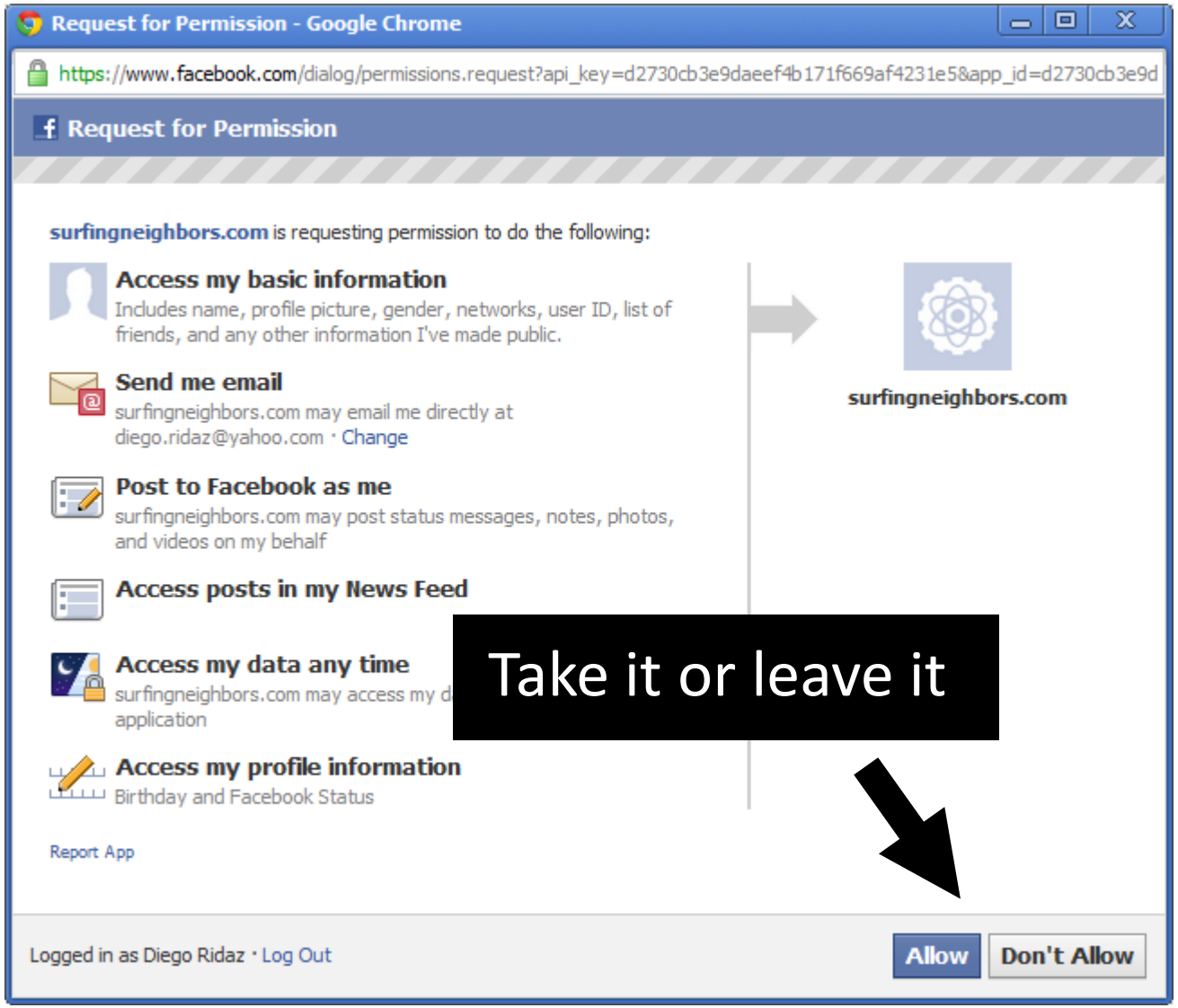
Pros

- Convenience: fewer passwords to remember
- Rich experience through social features
- Outsource user registration and management

Cons

- Same credentials for multiple sites
- User tracking
- Access to user's profile




Request for Permission - Google Chrome
https://www.facebook.com/dialog/permissions.request?api_key=d2730cb3e9daeef4b171f669af4231e5&app_id=d2730cb3e9d
Request for Permission
surfingneighbors.com is requesting permission to do the following:
Access my basic information
Includes name, profile picture, gender, networks, user ID, list of friends, and any other information I've made public.
Send me email
surfingneighbors.com may email me directly at diego.ridaz@yahoo.com · Change
Post to Facebook as me
surfingneighbors.com may post status messages, notes, photos, and videos on my behalf
Access posts in my News Feed
Access my data any time
surfingneighbors.com may access my d
application
Access my profile information
Birthday and Facebook Status
Report App
surfingneighbors.com
Take it or leave it
Logged in as Diego Ridaz · Log Out
Allow
Don't Allow

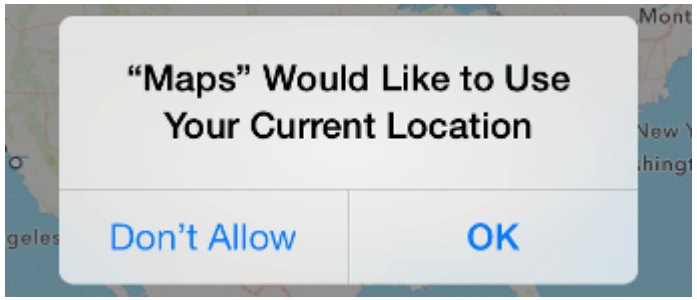
Location Tracking

IP addresses reveal approximate location information

- MaxMind statistics: 99.8% accurate on a country level, 90% accurate on a state level in the US, and 81% accurate for cities in the US within a 50 kilometer radius

Mobile devices allow for precise location tracking

- Cell tower triangulation/trilateration
- GPS, GLONASS, …
- WiFi access points in known locations



Per-app permissions

- Android vs. iOS:
  installation vs. usage time

Attention, Shoppers: Store

www.nytimes.com/2013/07/15/business/attention-shopper-stores-are-tracking-your-cell.html?_r=0

SECTIONS HOME SEARCH

The New York Times

LOG IN

BUSINESS DAY

410 COMMENTS

Attention, Shoppers: Store Is Tracking Your Cell

By STEPHANIE CLIFFORD and QUENTIN HARDY JULY 14, 2013

Email

Share

Tweet

Save

More

Like dozens of other brick-and-mortar retailers, Nordstrom wanted to learn more about its customers — how many came through the doors, how many were repeat visitors — the kind of information that e-commerce sites like Amazon have in spades. So last fall the company started testing new technology that allowed it to track customers' movements by following the Wi-Fi signals from their smartphones.

Brick-and-mortar stores are looking for a chance to catch up with their online competitors by using software that allows them to watch customers as they shop, and gather data about their behavior. Video by Erica Berenstein on July 14, 2013.

But when Nordstrom posted a sign telling customers it was tracking them, shoppers were unnerved.

"We did hear some complaints," said Tara Darrow, a spokeswoman for the store. Nordstrom ended the experiment in May, she said, in part because of the comments.

Nordstrom's experiment is part of a movement by retailers to gather data about in-store shoppers' behavior and moods, using video surveillance and signals from their cellphones and apps to learn

GPS

Fitness tracking app Strava gives away location of secret US army bases

Data about exercise routes shared online by soldiers can be used to pinpoint overseas facilities

Alex Hern

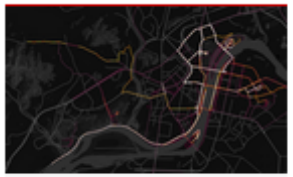
@alexhern

Sun 28 Jan 2018
16.51 EST

6948

Sensitive information about the location and staffing of military bases and spy outposts around the world has been revealed by a fitness tracking company.

The details were released by Strava in a data visualisation map that shows all the activity tracked by users of its app, which allows people to record their exercise and share it with others.



Strava suggests military users 'opt out' of heatmap as row deepens

Read more

The map, released in November 2017, shows every single activity ever uploaded to Strava - more than 3 trillion individual GPS data points, according to the company. The app can be used on various devices including smartphones and fitness trackers like Fitbit to see popular running routes in major cities, or spot individuals in more remote areas who have unusual exercise patterns.

However, over the weekend military analysts noticed that the map is also

Privacy and Security Built In

AirTag is designed from the ground up to keep location data private and secure. No location data or location history is physically stored inside AirTag. Communication with the Find My network is end-to-end encrypted so that only the owner of a device has access to its location data, and no one, including Apple, knows the identity or location of any device that helped find it.

AirTag is also designed with a set of proactive features that discourage unwanted tracking, an industry first. Bluetooth signal identifiers transmitted by AirTag rotate frequently to prevent unwanted location tracking. iOS devices can also detect an AirTag that isn't with its owner, and notify the user if an unknown AirTag is seen to be traveling with them from place to place over time. And even if users don't have an iOS device, an AirTag separated from its owner for an extended period of time will play a sound when moved to draw attention to it. If a user detects an unknown AirTag, they can tap it with their iPhone or NFC-capable device and instructions will guide them to disable the unknown AirTag.

Online Behavioral Tracking

Many of our daily activities are being recorded

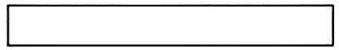
- What we are interested in (Searches, Likes, …)
- What we read (News, magazines, blogs, …)
- What we buy (Amazon, Freshdirect, …)
- What we watch (Netflix, Hulu, …)
- What we eat (Seamless, GrubHub, …)
- Where we eat (Opentable, Foursquare, …)
- Where we go (online travel/hotel/event booking)
- What we own/owe (e-banking, credit services, Mint, …)

Mobile apps make behavioral tracking easier and more accurate

Behavioral profiles have desirable and not so desirable uses

- Recommendations, content personalization, insights, …
- Targeted advertising, price discrimination (e.g., insurance premiums based on past behavior, higher prices for high-end device users), …

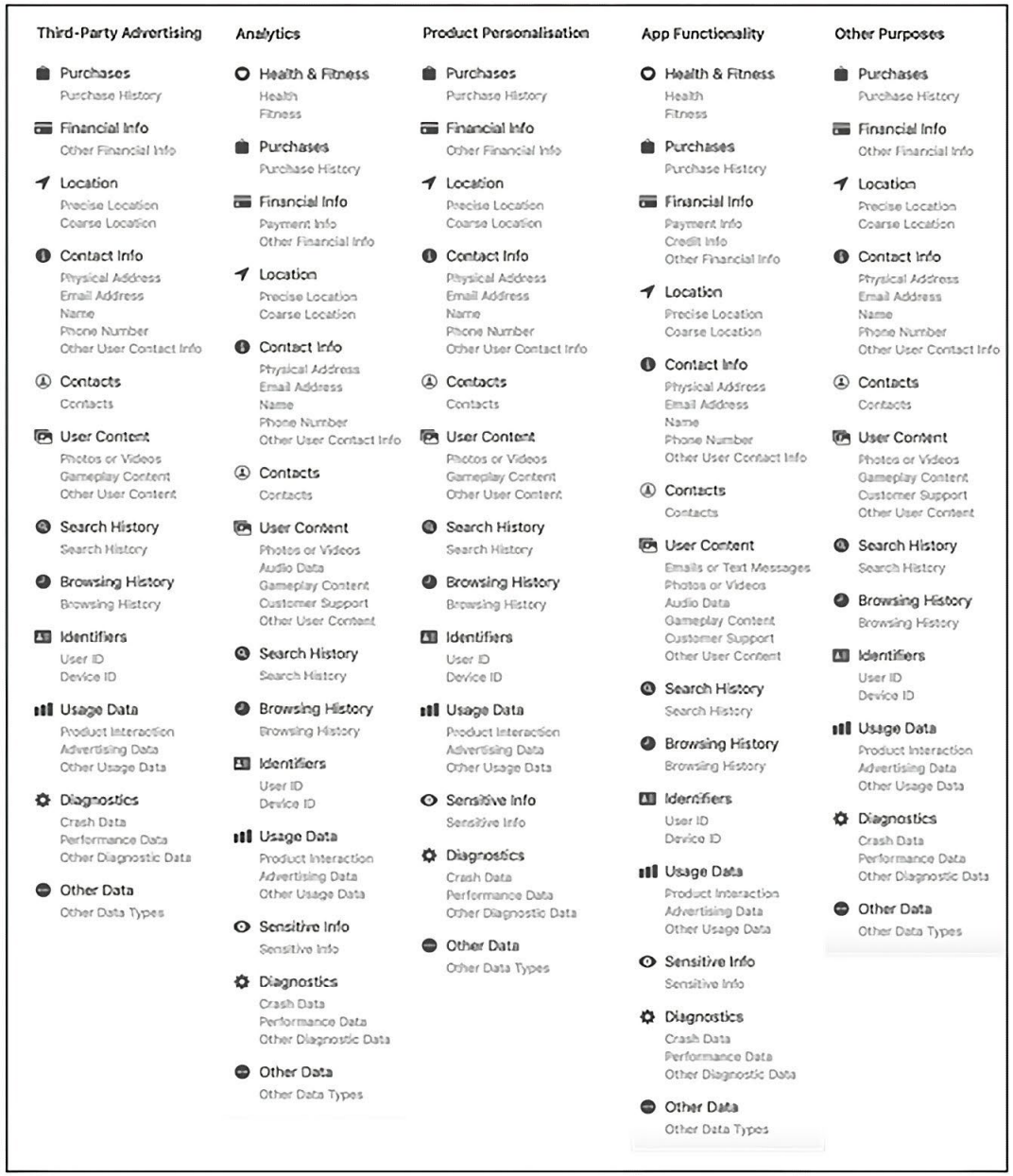
Signal
'Data Linked To You'



iMessage
'Data Linked To You'

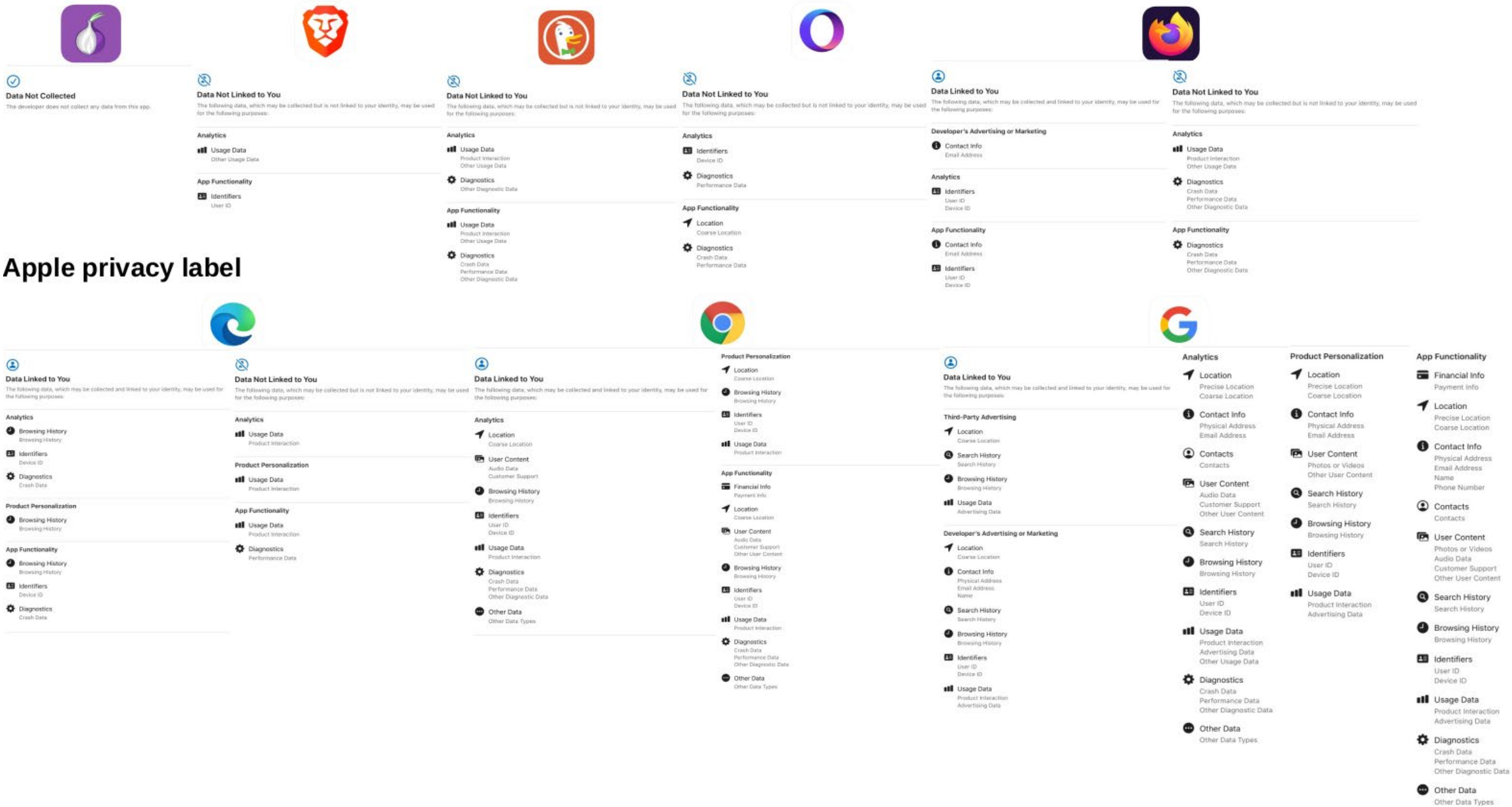
WhatsApp
'Data Linked To You'

Facebook Messenger
'Data Linked To You'



https://twitter.com/morqon/status/1346464501319622657

Apple privacy label



https://www.reddit.com/r/privacytoolsIO/comments/m6v0e3/apple_privacy_label_browsers_comparison/

Health and Activity

Health records

- How securely are they handled and stored?

Devices track our activities and health

- Activity tracking devices
- Health monitoring devices
- Mobile phones

Many upload all data to the “cloud”…

- Who can access them?

Doctor/hospital health portals managed by third parties

Protecting Privacy

Preferably through technical means, not promises

Avoid collecting personal data in the first place

iOS vs. Android, DuckDuckGo vs. Google, …

Block tracking, fingerprinting, profiling, …

Brave, Firefox, Safari, ad blockers, …

Privacy-preserving protocols/mechanisms

Differential privacy, on-device processing, content prefetching, …

Self-hosted services

Only for geeks

Data privacy laws

EU General Data Protection Regulation (GDPR), California Consumer Privacy Act (CCPA)