No More Apologies: Inside Facebook's Push to Defend Its Image

Mark Zuckerberg, the chief executi
to show users pro-Facebook stories
scandals.

'Spy pixels in emails have become endemic'

By Leo Kelion
Technology desk editor

PLAYING FAST AND LOOSE —

How your sensitive data can be sold after a data broker goes bankrupt

Sensitive location data could be sold off to the highest bidder.

JON KEEGAN, THE MARKUP - 2/25/2024, 6:57 AM

Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret

Dozens of companies use smartphone locations to help advertisers and even hedge funds. They say it's anonymous, but the data shows how personal it is.

META'S COURT LOSS

Meta illegally collected data from Flo period and pregnancy app, jury finds

Lawyers hail jury's "clear message" to Big Tech; Meta will fight

Credit: Getty Images | Kenneth Cheung

Thousands of Android and iOS Apps Leak Data From the Cloud

It's the digital equivalent of leaving your windows or doors open when you leave the house —and in some cases, leaving them open all the time.

Meta and Yandex Are De-Anonymizing Android Users' Web Browsing Identifiers (github.io) 77

Posted by **BeauHD** on Tuesday June 03, 2025 @05:00PM from the PSA dept.

"It appears as though Meta (aka: Facebook's parent company) and Yandex have found a way to sidestep the Android Sandbox," writes Slashdot reader TheWho79. Researchers disclose the novel tracking method in a report:

> We found that native Android apps -- including Facebook, Instagram, and several Yandex apps including Maps and Browser -- silently listen on fixed local ports for tracking purposes.
>
> These native Android apps receive browsers' metadata, cookies and commands from the Meta Pixel and Yandex Metrica scripts embedded on thousands of web sites. These JavaScripts load on users' mobile browsers and silently connect with native apps running on the same device through localhost sockets. As native apps access programmatically device identifiers like the Android Advertising ID (AAID) or handle user identities as in the case of Meta apps, this method effectively allows these organizations to link mobile browsing sessions and web cookies to user identities, hence de-anonymizing users' visiting sites embedding their scripts.

DEBUGGER

Your Smartphone Apps Are Filled With Trackers You Know Nothing About

The privacy crisis Apple and Google need to fix—now

Facebook pays teens to install VPN that spies on them

Cyber Smart

Protecting yourself online in an age of digital threats

Michael Prather | Dr. Brian Krupp

People use apps and services

Platforms refer to people as users

"our ability to retain or increase users and engagement levels" - from Meta Investors Page;

What other "industry" uses the term "users"?

Privacy is not about secrets—it's about control.

Agenda

1. Understand common online threats and how they affect everyday people

2. Learn practical ways to protect your accounts, devices, and data

3. Recognize signs of scams and phishing attempts

4. Strengthen your online privacy and digital habits

Foundational concepts

A Safer Mindset Online

- **Zero Trust**: Verify before you trust.
- **Assume Breach**: No system is perfectly safe — prepare for “what if.”
- **Evolving Threats**: Attackers change tactics constantly; stay curious and cautious.
- **Limit Your Digital Footprint**: Share less, risk less.
- **Obfuscate**: Make it difficult to easily link data to you.

Passwords

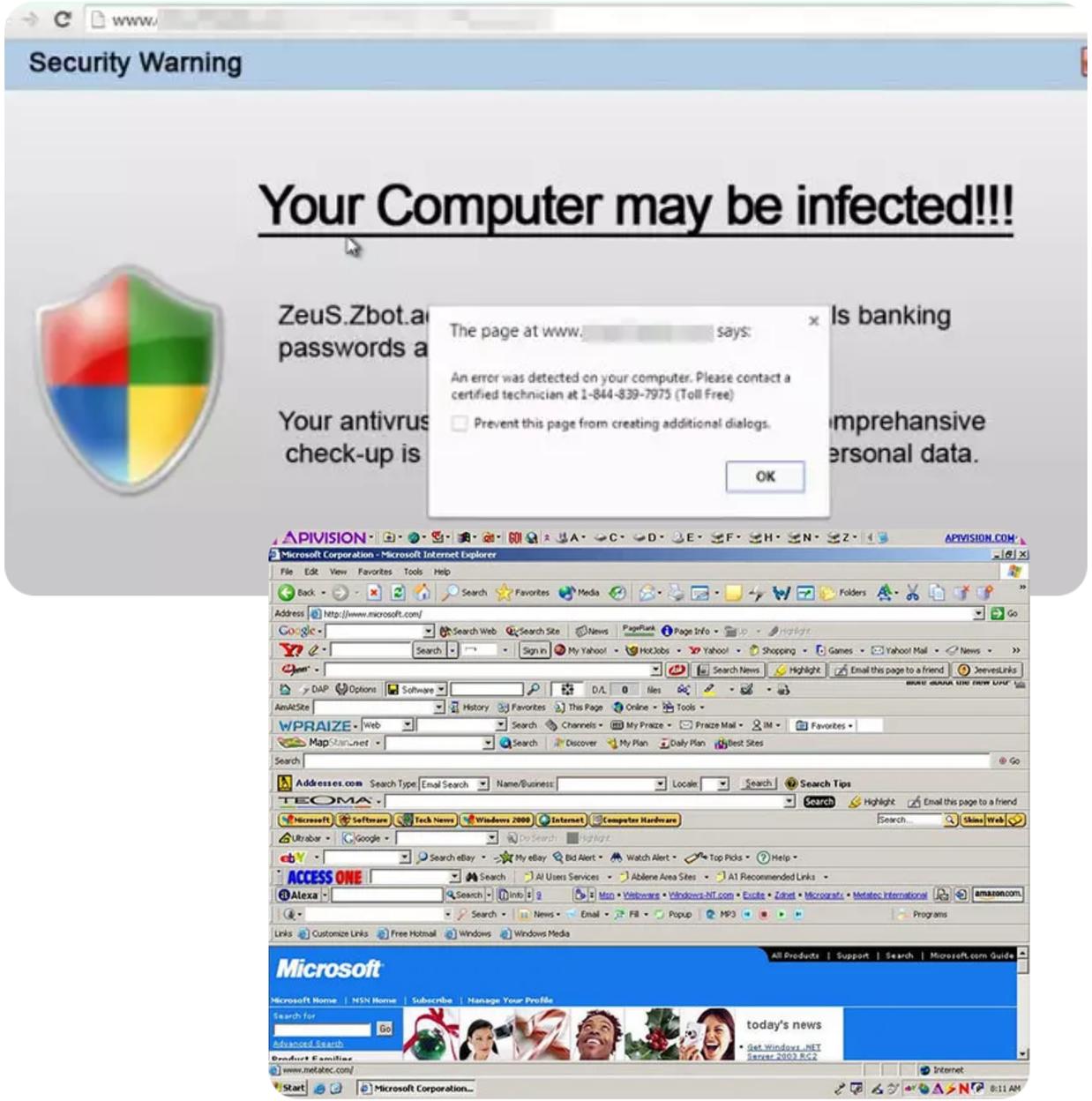
- Longer is stronger
- Never reuse a password
- No personal info or generics
- Change only if compromised
- Use memorable passphrase if needed (ex. “blue-banana-window-piano”)
- Use multi-factor authentication (MFA)

Devices & Network

- Obfuscate your network name
- Use a strong Wi-Fi password — not the default
- Update your router and devices regularly
- Use WPA3 or WPA2 encryption
- Limit access: separate guest and smart-device networks
- Turn off devices or Wi-Fi when not in use

Browsing

- Check for “https://” and padlock 🔒
- Don’t click suspicious links or pop-ups
- Verify URLs before entering credentials
- Keep browsers & plugins updated
- Download apps from official sources and app stores



Private Browsing

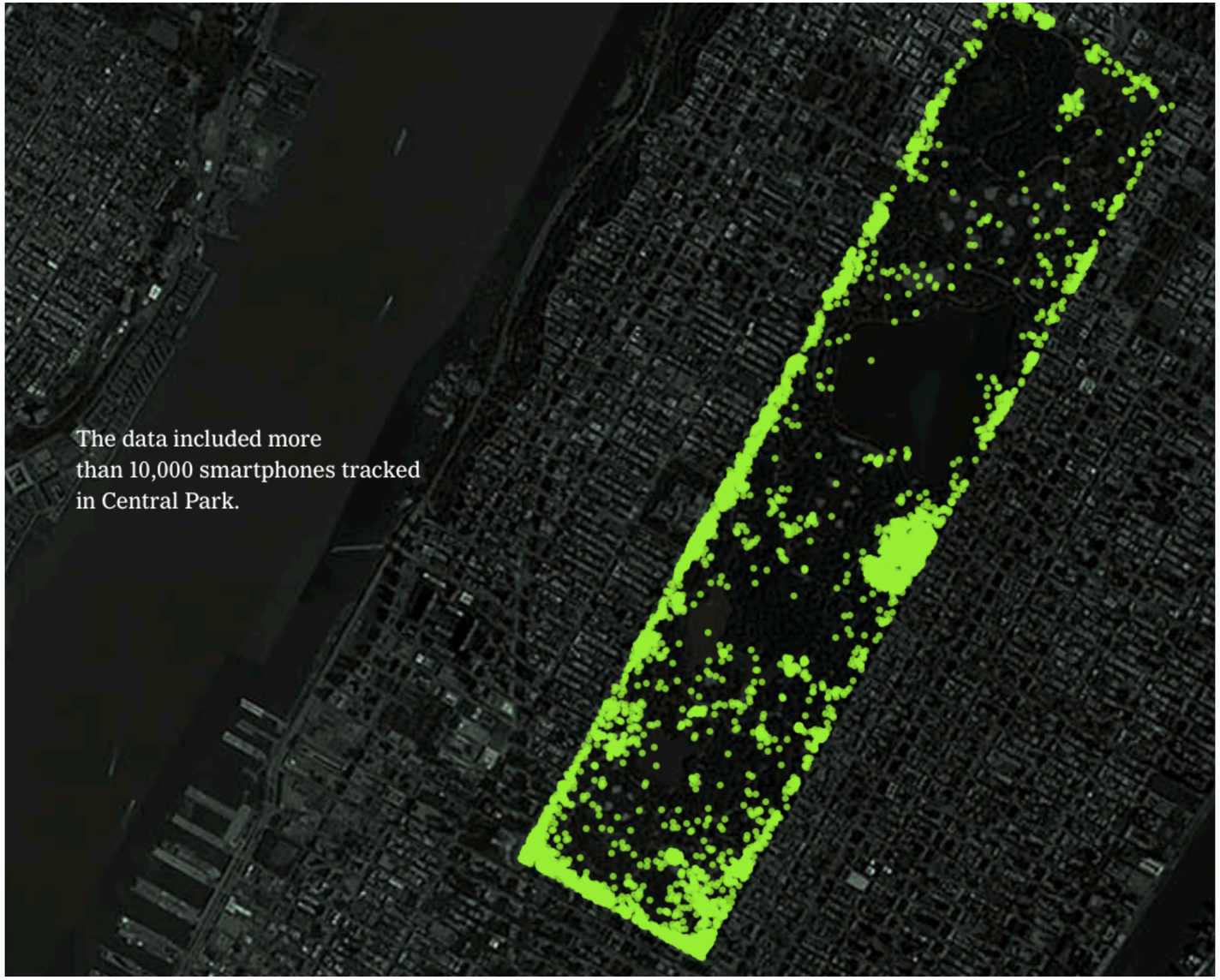
- Is your private browser truly private?
- Each browser contains a "fingerprint"
  - IP, Browser, Cookies, Extensions, Screen Size
  - Operating System, CPU/GPUs, etc
- Some browsers offer protection
  - Firefox, Safari, DuckDuckGo
- Private browsing does not protect you
- You can test here: https://coveryourtracks.eff.org

VPNs

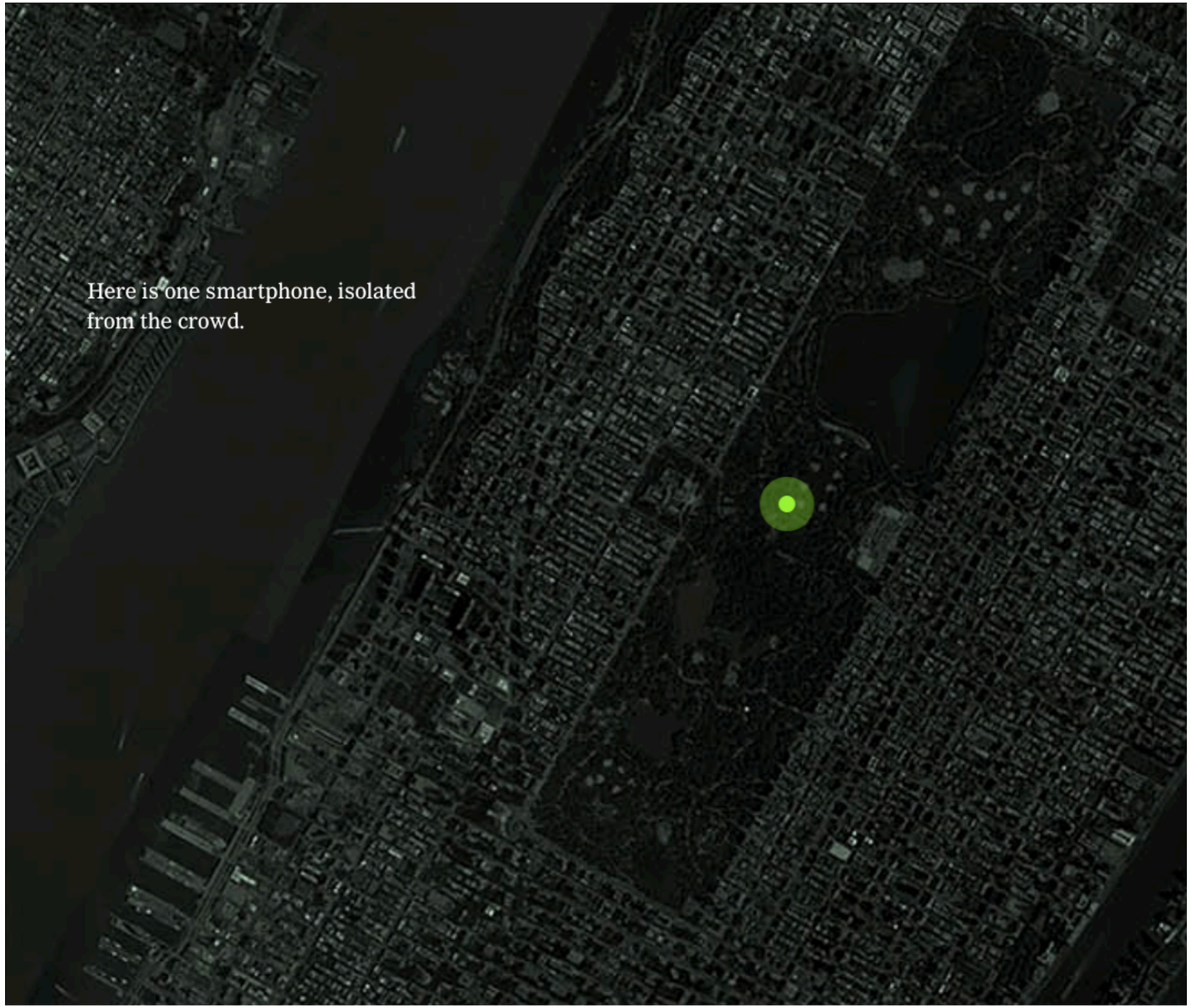
- If I use a VPN, doesn't that protect my privacy?
- It *does help* but it is not a silver bullet
- You are transferring your trust to the VPN provider
- Good video on "Do you need a VPN": https://neat.tube/w/6HDQH1wnTACKFHh2u1CRQ5
  - How does Tor differ from a VPN: https://neat.tube/w/f7QkKGe5TJaPi6Y4S61Uoi

Public Wi-Fi

- Avoid public Wi-Fi for sensitive activity
- Turn-off auto-connect
- Disconnect when not in use
- Logout of accounts
- Use a VPN or a mobile hotspot
- What is my IP?



https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html?action=click&module=Opinion&pgtype=Homepage



https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html?action=click&module=Opinion&pgtype=Homepage

https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html?action=click&module=Opinion&pgtype=Homepage

https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html?action=click&module=Opinion&pgtype=Homepage

Mobile Privacy

- Example: Application requests access to location
- Once you grant it, how often can it read it? How accurate is it? Who can it send your location to?
- Contacts: What information is in your contacts?
- Photos: What information is in your photos?
- Once the data is gone, you can’t take it back

- Consider time spent in the applications

What's In an Image?

What is in an Image?

Select a Photo

Browse... No file selected.

Submit

Type	Data
FileName	phpdcXEYq
FileDateTime	1743012042
FileSize	1419501
FileType	2
MimeType	image/jpeg
SectionsFound	ANY_TAG, IFD0, THUMBNAIL, EXIF, GPS
COMPUTED	width="1536" height="2048" 2048153611f/1.52image/jpeg
Make	Apple
Model	iPhone 14
XResolution	72/1
YResolution	72/1
ResolutionUnit	2
Software	17.2.1
DateTime	2024:01:18 12:52:29
HostComputer	iPhone 14
YCbCrPositioning	1
Exif_IFD_Pointer	216
GPS_IFD_Pointer	2466
THUMBNAIL	672/172/1228709600
ExposureTime	1/60

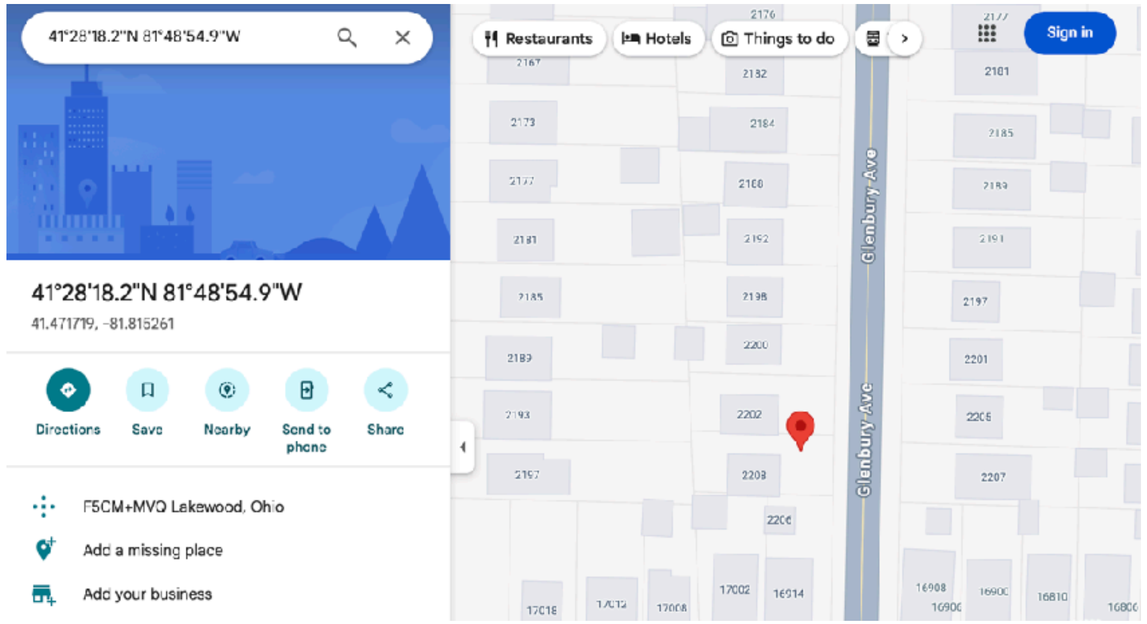
UndefinedTag:0xA432	807365/5242632988413/5242833/212/5
UndefinedTag:0xA433	Apple
UndefinedTag:0xA434	iPhone 14 back dual wide camera 5.7mm f/1.5
UndefinedTag:0xA460	2
GPSLatitudeRef	N
GPSLatitude	41/127/13938/100
GPSLongitudeRef	W
GPSLongitude	81/154/15631/100
GPSAltitudeRef	
GPSAltitude	334327/1499
GPSTimeStamp	17/152/125/1
GPSSpeedRef	K
GPSSpeed	0/1
GPSImgDirectionRef	T
GPSImgDirection	483226/1737
GPSDestBearingRef	T
GPSDestBearing	483226/1737
GPSDateStamp	2024:01:18
UndefinedTag:0x001F	35/1

Location Sharing Example

The Weather Channel Application

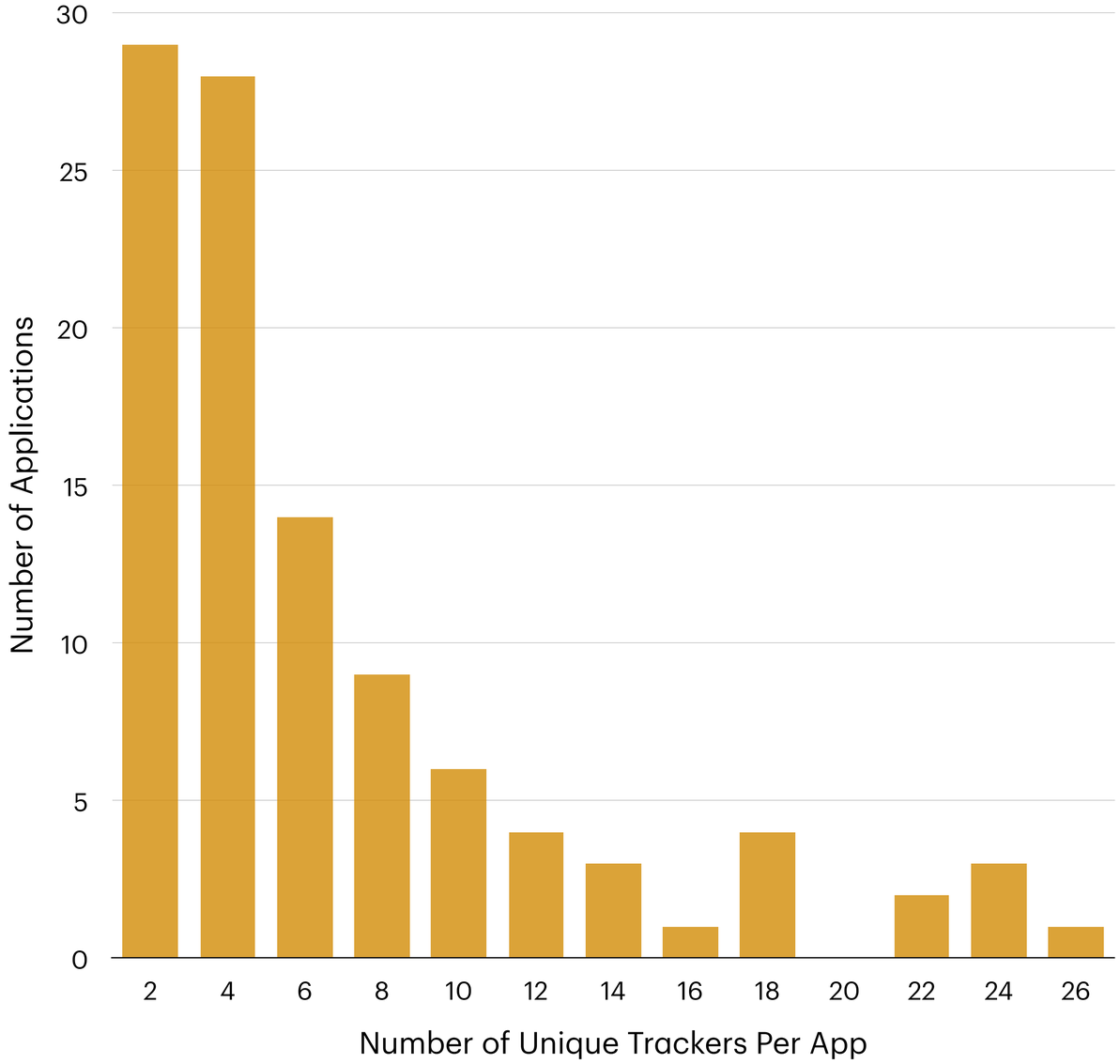
- INFO (SPERequestApprover.java:356) - Detected the following location data going to : geopulse.factual.com:/geopulse/7620026f-cfb6-4d0c-9f8e-434ff0cd34d0?audience=false&proximity=true

- INFO (SPERequestApprover.java:357) - **41.47171848812904, -81.81526106015584**



Trackers in Mobile Applications

- Tested 124 most popular applications in iOS
- Most applications used a small number of unique trackers (median = 4)
- Several applications used 22 or more unique trackers



Top 10 Tracking Domains in Applications

- Google and Facebook dominate the top 10 (Amazon ranks #10)
- Most prevalent among applications with high total requests

Domain	Company	# Of Applications	Total Requests
googleads.g.doubleclick.net	Google	46	897
graph.facebook.com	Facebook	45	520
tpc.googlesyndication.com	Google	33	310
www.googletagservices.com	Google	29	47
pagead2.googlesyndication.com	Google	28	350
pubads.g.doubleclick.net	Google	20	310
www.facebook.com	Facebook	19	115
ssl.google-analytics.com	Google	19	149
www.googletagmanager.com	Google	16	46
mads.amazon-adsystem.com	Amazon.com	15	27

Mobile Carriers

- Not just the phone, but the carrier tracks you as well:
- Exercise: Review the following options:
  - AT&T: Login → Profile → Privacy Choices
  - Verizon: Account → Account Overview → Edit Profile and Settings → Manage Privacy Settings
  - T-Mobile → My Account → Profile (Scroll to Bottom) → Privacy and Notifications → Privacy Dashboard

- https://www.cnet.com/tech/mobile/data-privacy-your-wireless-carrier-knows-more-than-you-think-heres-how-to-take-back-control/

What You Can Do - Mobile

- Delete social media apps and accounts (or, at least limit their use)
  - Dark patterns - Designed to keep you on platform
  - You are addicted if you cannot use
- Review application permissions
- Be wary of any location sharing (can the zip code be good enough?)
- Limit sharing of personal data like photos and contacts
- Disable Ad ID Tracking:
  - https://www.eff.org/deeplinks/2022/05/how-disable-ad-id-tracking-ios-and-android-and-why-you-should-do-it-now
- Switch Search Engine: DuckDuckGo or Ecosia or Brave Search
- Use apps where company's revenue is not from your data
- Phone and Devices: Check Out Cheat Sheets from DuckDuckGo
  - https://duckduckgo.com/download/iPhone_Privacy_Tips.pdf
  - https://duckduckgo.com/download/Android_Privacy_Tips.pdf
- Privacy Guides:
  - https://www.privacyguides.org/en/os/ios-overview/
  - https://www.privacyguides.org/en/os/android-overview/

Social Media & Privacy

- Limit who can see your posts
- Regularly audit your friends list
- Assume data is evergreen
- Avoid quizzes and surveys
- Think before you post — would you share it with a stranger?
- Ask permission including others in your post
- Attackers piece together online artifacts to learn about you

Social Media

- Social media applications perform invasive tracking
- Your data is their revenue
- Do not properly protect data
- Make more revenue the more emotional its **users** are
- Hide negative stories on their business
- Block researchers into their platform
- Promote false stories (more clicks → more ads → more revenue)

Facebook Knows Instagram Is Toxic for Teen Girls, Company Documents Show

Its own in-depth research shows a significant teen mental-health issue that Facebook plays down in public

Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead.

Facebook stored hundreds of millions of passwords in plain text

Why A.I. Should Make Parents Rethink Posting Photos of Their Children Online

Artificial intelligence apps generating fake nudes, amid other privacy concerns, make "sharenting" far riskier than it was just a few years ago.

No More Apologies: Inside Facebook's Push to Defend Its Image

Mark Zuckerberg, the chief executive, has signed off on an effort to show users pro-Facebook stories and to distance himself from scandals.

Bad Design

- How do you refresh Facebook or Twitter or other apps?
- Pull down like a slot machine!
  - Do you think this design was intentional?
- Do you check how many retweets you have? How many likes you have?
- Do you get notifications?
- How do these make you feel?
- Do you get emails when you "miss" something?
- How many steps does it take to share a photo on your social media application?
- How many steps does it take to make your account private? Limit personalized ads?

Spotting Scams & Phishing Attempts

🚩 Red flags

- Urgency or threats (“Act now!” “Your account will be closed!”)
- Unusual sender address
- Typos, odd grammar, or weird logos
- Links not matching the company
- Unexpected attachments
- Requests for passwords or MFA codes

Surveillance Pricing

- Another way your privacy, via surveillance, can affect you
- Should a ride-hailing company such as Uber or Lyft be able to charge you more because its AI thinks your phone is about to die?
- What can be used?
  - Battery Life
  - Apps Installed
  - Older Model
  - Time of Day
  - User Location
  - Where User Lives and more

Artificial Intelligence

Should Lyft and Uber charge more if your battery is low? California may soon ban that

California lawmakers want to ban companies from using data about consumers' devices like battery life, model and geolocation to set fluctuating prices. Proponents say such "surveillance pricing" is discriminatory.

MA bill would ban 'surveillance pricing' in grocery stores. Here's how it would work

Alison Kuznitz State House News Service

Aug. 19, 2025, 10:22 a.m. ET

AI as Surveillance

- Data collected can be used in AI models to do influence you
  - https://www.npr.org/programs/ted-radio-hour/2025/05/30/ted-radio-hour-for-may-30-2025
- Personal chats may not be private
- Personal data on existing platforms my be used to train current models
- There are some recommendations, but be careful:
  - https://www.privacyguides.org/en/ai-chat/#ollama-cli

What Else You Can Do

- TVs
  - Disconnect from Internet if possible, or use services that respect privacy
  - https://arstechnica.com/gadgets/2025/06/all-the-ways-apple-tv-boxes-do-and-mostly-dont-track-you/
- Blur street images in Google Maps, Bing, and others
  - https://www.popsci.com/diy/hide-home-map-apps/
- Check Out Cheat Sheets from from Privacy Guides
  - https://www.privacyguides.org/en/os/macos-overview/
  - https://www.privacyguides.org/en/os/windows/

- Check for breaches:
  - https://haveibeenpwned.com/
- Uninstall apps you don't need/use
- Limit social media (or delete)
- Email: Disable loading remote content, use privacy focused service (ProtonMail)
- Limit overall use!