Staying Private Online

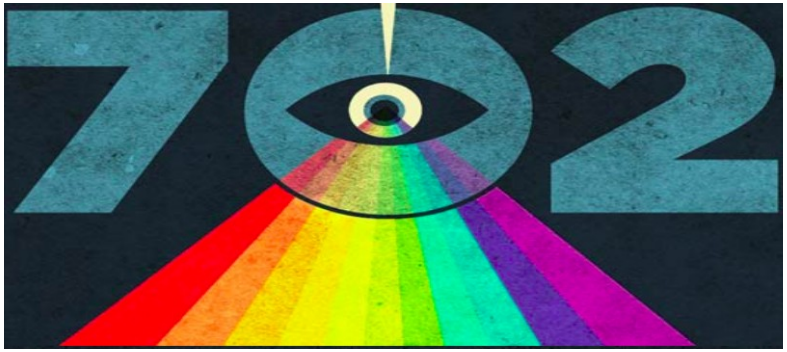
Staying private online in a world where Big Tech and the government want a digital window into your private life

How do they get your data?

- **Online ads**
- **Email and other “free” services**
- **Social media**
- **Mobile apps**
- **Everyday calls and texts**
- **Internet service provider**

How do they get your data?

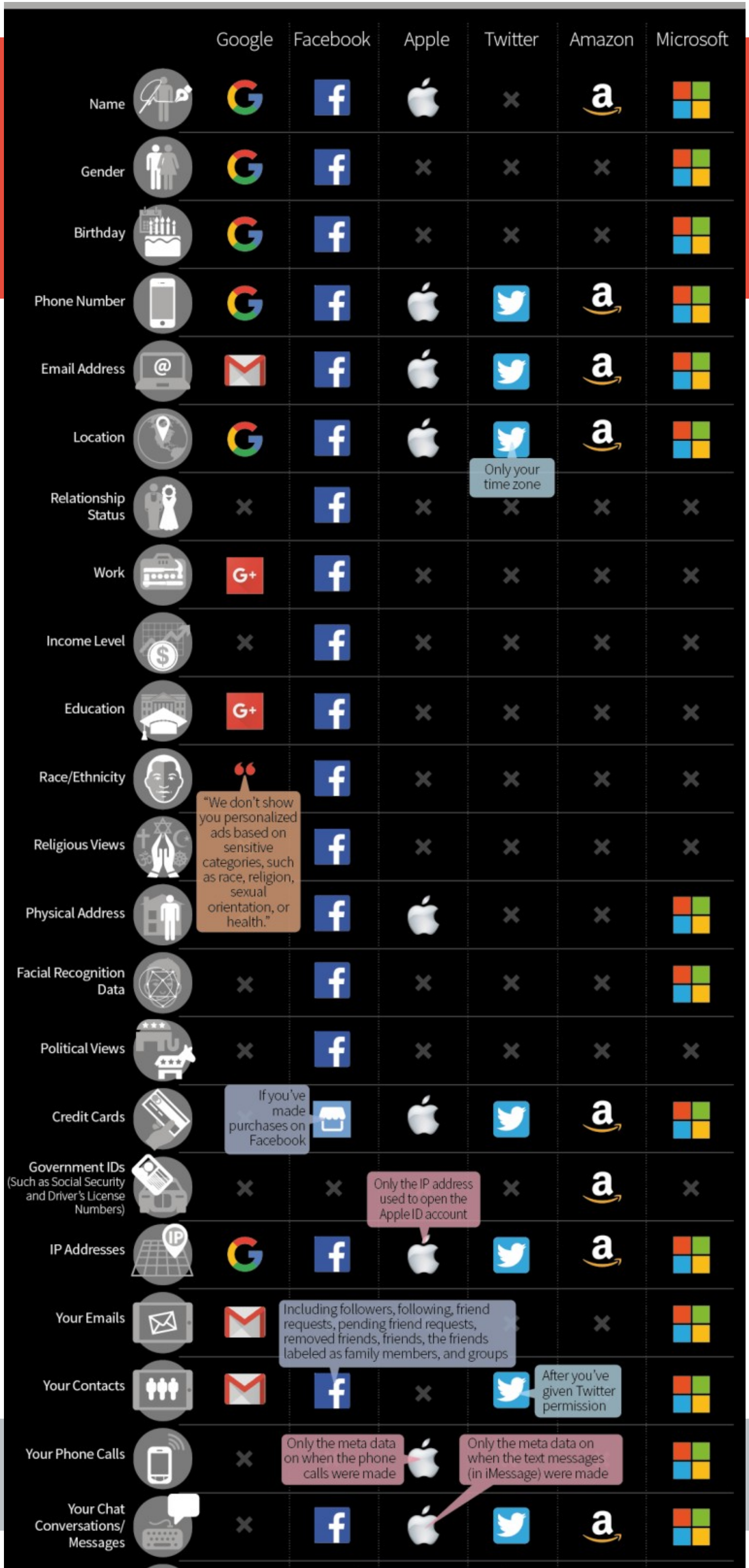
- **Trackers: cookies, pixels, IP address logging, browser fingerprinting**
  - Example: Just one provider, Acxiom, keeps 3k+ data points per person, on over 500 million people
- **Apps and services**
  - Reading messages and documents, facial recognition on photos, etc.
  - Actions, including voice commands, and preferences while using the service and after logged out
  - Data YOU provide in a profile
- **Government programs**
  - PRISM
    - US government collects data from partner companies
  - 2008 FISA amendment, section 702
    - Bulk collection of internet communications by US government

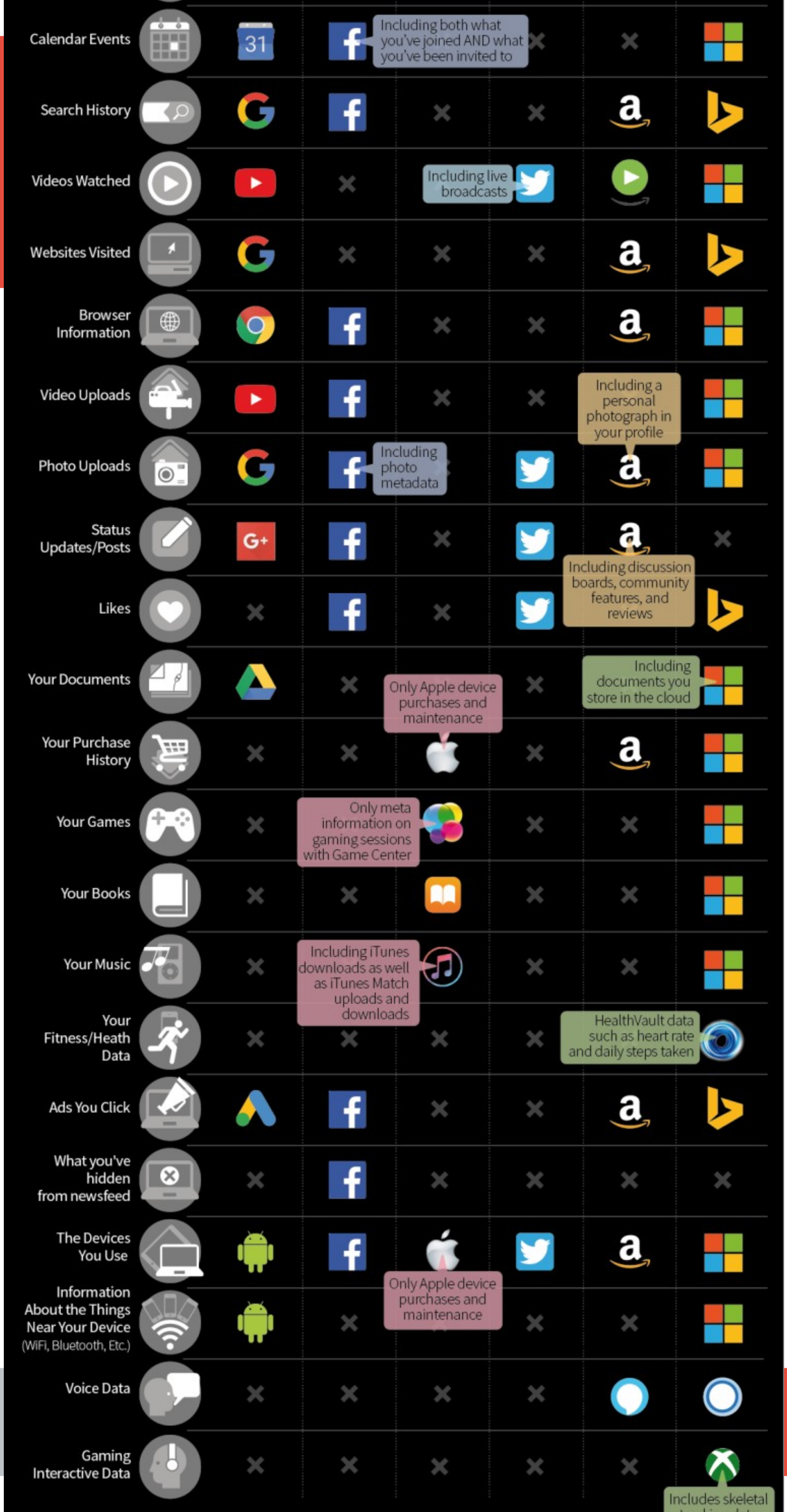


Want to be even more paranoid?

- Online shopping
- Credit cards
- Loyalty cards
- Video surveillance with facial recognition
- Traffic/stop light cameras
- (This list pretty much never ends)

Social Media



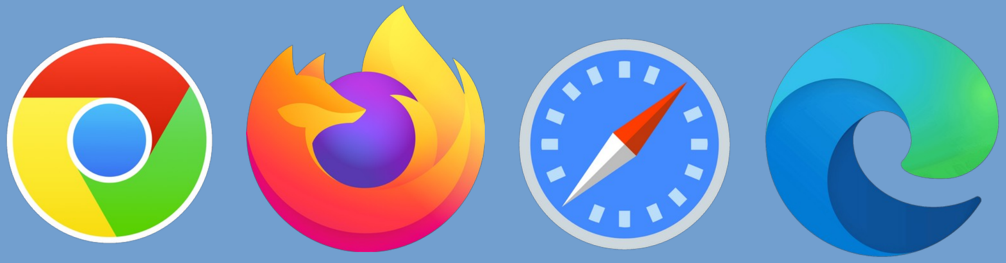


	Google	Facebook	Apple	Twitter	Amazon	Microsoft
Name	✓	✓	✓	×	✓	✓
Gender	✓	✓	×	×	×	✓
Birthday	✓	✓	×	×	×	✓
Phone Number	✓	✓	✓	✓	✓	✓
Email Address	✓	✓	✓	✓	✓	✓
Location	✓	✓	✓	✓ Only your time zone	✓	✓
Relationship Status	×	✓	×	×	×	×
Work	✓	✓	×	×	×	×
Income Level	×	✓	×	×	×	×
Education	✓	✓	×	×	×	×
Race/Ethnicity	“We don't show you personalized ads based on sensitive categories, such as race, religion, sexual orientation, or health.”	✓	×	×	×	×
Religious Views		✓	×	×	×	×
Physical Address		✓	✓	×	×	✓
Facial Recognition Data	×	✓	×	×	×	✓
Political Views	×	✓	×	×	×	×
Credit Cards		✓ If you've made purchases on Facebook	✓	✓	✓	✓
Government IDs (Such as Social Security and Driver's License Numbers)	×	×		×	✓	×
IP Addresses	✓	✓	✓ Only the IP address used to open the Apple ID account	✓	✓	✓
Your Emails	✓				×	✓
Your Contacts	✓	✓ Including followers, following, friend requests, pending friend requests, removed friends, friends, the friends labeled as family members, and groups	×	✓ After you've given Twitter permission		✓
Your Phone Calls	×		✓ Only the meta data on when the phone calls were made			✓
Your Chat Conversations/ Messages	×	✓	✓ Only the meta data on when the text messages were made (in iMessage) were made	✓	✓	✓
Calendar Events	✓	✓ Including both what you've joined AND what you've been invited to		×	×	✓
Search History	✓	✓	×	×	✓	✓
Videos Watched	✓	×		✓ Including live broadcasts	✓	✓
Websites Visited	✓	×	×	×	✓	✓
Browser Information	✓	✓	×	×	✓	✓
Video Uploads	✓	✓	×	×		✓
Photo Uploads	✓	✓ Including photo metadata		✓	✓ Including a personal photograph in your profile	✓
Status Updates/Posts	✓	✓	×	✓	✓ Including discussion boards, community features, and reviews	×
Likes	×	✓	×	✓		✓
Your Documents	✓	×		×		✓ Including documents you store in the cloud
Your Purchase History	×	×	✓ Only Apple device purchases and maintenance	×	✓	✓
Your Games	×		✓ Only meta information on gaming sessions with Game Center	×	×	✓
Your Books	×	×	✓	×	×	✓
Your Music	×		✓ Including iTunes downloads as well as iTunes Match uploads and downloads	×	×	✓
Your Fitness/Heath Data	×	×	×	×		✓ HealthVault data such as heart rate and daily steps taken
Ads You Click	✓	✓	×	×	✓	✓
What you've hidden from newsfeed	×	✓	×	×	×	×
The Devices You Use	✓	✓	✓ Only Apple device purchases and maintenance	✓	✓	✓
Information About the Things Near Your Device (WiFi, Bluetooth, Etc.)	✓	×		×	×	✓
Voice Data	×	×	×	×	✓	✓
Gaming Interactive Data	×	×	×	×	×	✓ Includes skeletal

Source: https://bit.ly/2VePStR

Web browsing

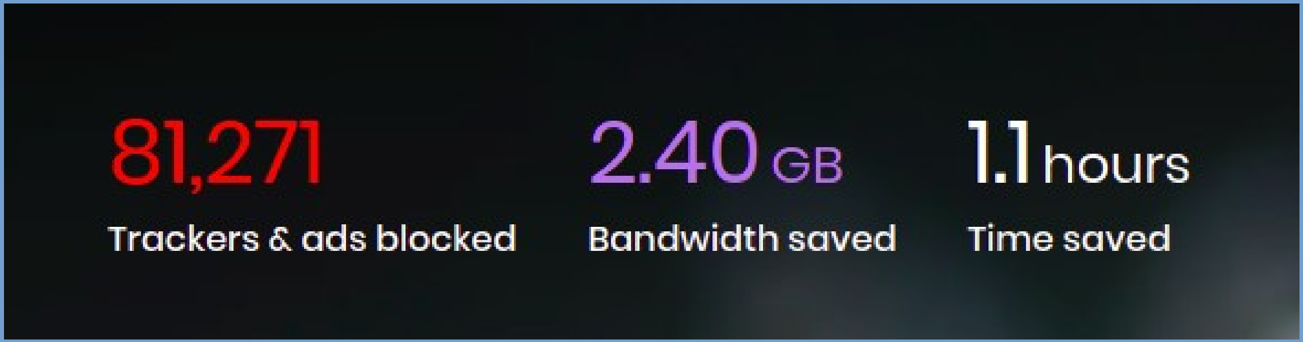
Instead of:



Try:

brave

Duck Duck Go



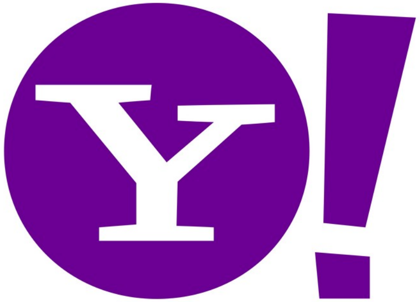
81,271
Trackers & ads blocked

2.40 GB
Bandwidth saved

1.1 hours
Time saved

Search

Instead of:

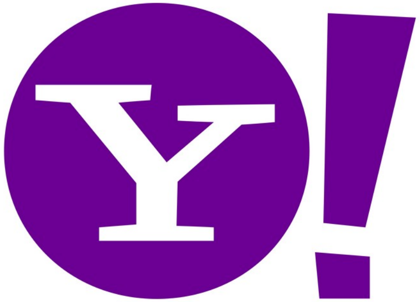


Try:

DuckDuckGo

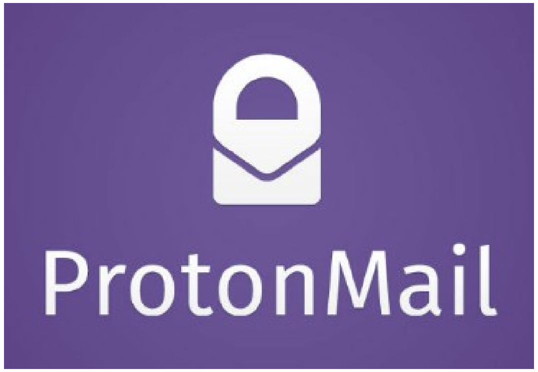
Email

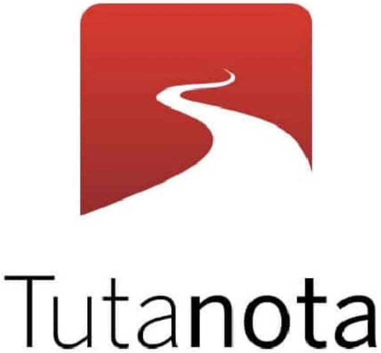
Instead of:



Windows Live
Hotmail

Try:





Mobile phones

- **Easy option**
  - Go low-tech, with an old style flip phone (no smart phone)
  - This option is suitable for most people and won’t require learning any new apps or phone layouts
- **De-Googled Androids**
  - Preferred method for those who still want a smart phone but also want privacy
  - Building your own requires technical skills, time, and research
  - Or, some retailers do this:
    - https://brax.me/prod/host.php?f=_store&h=rob&p=&version=
    - https://esolutions.shop/
    - https://www.freedomphone.com/

Apps and software

- **App stores**
  - Using Google and Apple app stores subjects you to their tracking
  - F-Droid store
    - Download from https://f-droid.org/
    - All apps are open source
    - Community members can see the code
  - Aurora store
    - Download using F-Droid store
    - Access to Google Play Store apps without using Google
    - Trackers in each app are listed
    - Note: Some apps from here might not work optimally when the phone is de-Googled

App highlights

- **DuckDuckGo privacy browser**
  - Privacy-friendly web search and web browsing
  - Clear tracking cookies on exit
- **ProtonMail*, TutaNota email apps**
  - Both ProtonMail and TutaNota can send encrypted emails when the recipient also uses that service
- **Signal***
  - If both people use Signal, text messages, calls, and even video calls are encrypted end-to-end
- **ProtonVPN**
  - Good for getting your feet wet; VPN service by ProtonMail. One of the few free ones that won’t log the sites you visit. Paid plan = better speed.

*The * indicates apps not found on F-Droid, use Aurora Store*

A few specific apps to get started

- **F-Droid apps**
  - DuckDuckGo – Web browser/search
  - Tutanota - Email
  - K-9 Mail, FairEmail – Email from other services
  - AntennaPod – Podcasts
  - Feeder – RSS news reader
  - LibreraReader – PDF reader
  - NewPipe – De-Googled Youtube app
  - Bible Study App by AND Bible Open Source Project – Offline Bible, Bible study app
  - Vigilante – Detects usage of phone’s mic or camera
  - Etar Calendar – Open source calendar app
  - OSM And – Maps and navigation, (need to know cross streets or be able to find and tap destination on map)
  - OpenVPN – VPN client that is compatible with a variety of VPNs, check yours to find out
  - ProtonVPN – VPN app for ProtonMail’s VPN service
- **Privacy-friendly apps on Aurora store**
  - ProtonMail - Email
  - Signal – Text messages/SMS
  - Mega – Cloud storage with zero-knowledge encryption

Notes on going further

- **VPN**
  - Criteria: No logs, zero knowledge, trustworthy, avoid being blocked by anti-VPN detectors on many sites
  - Recommendations: https://www.vpntierlist.com/vpn-tier-list-2-0/
- **Password managers**
  - Never reuse passwords. Never use easy-to-guess passwords. Use a password manager to keep track of them all:
  - https://keepass.info/download.html
  - https://lastpass.com
  - https://1password.com/
- **Burner mobile phones**
  - Prepaid phone bought in cash with cheap monthly plan, using gift cards to refill
- **Burner credit cards**
  - Standard brand-name gift cards often work for online purchases
- **Facial recognition**
  - The normalization of face masks may be to your advantage when wishing to be in public while legally exercising your right to privacy
- **Be careful who you email**
  - Using a non-spy email service like ProtonMail is of no use if you use it to send sensitive data to spying email services, such as Gmail and Microsoft
- **Consider using Linux for your computer**
  - Ubuntu and Linux Mint are probably the most beginner-friendly, but you should have computer familiarity or regular support from someone who does before committing to this route.
- **Free/open source software when possible**
  - There is a lot of free/open source software available to replace common computer apps: Thunderbird for email/calendar, LibreOffice instead of Microsoft Office, VLC player for media, GIMP for photo editing, etc.
- **Always back up your files**
  - Back up your files AT HOME using an external hard drive, or use an encrypted cloud storage provider with zero-knowledge of your uploaded data

Questions?