

Digital Security and Privacy for Beginners

An introduction to safer mobile phone and
computer use in 2025

Our Privacy and Security is a human right, not a crime!

- Privacy is not about wrong doing. It is about consent and control.
- Privacy is about reducing invasive profiling done against us and without our consent.
- Privacy is about having autonomy over OUR DATA. It is rightfully ours to begin with.

Privacy is Self Defense and laying claim to our personal sovereignty

We may not have anything to hide, but we have everything to protect.

We must be the gatekeepers of our digital life and must not cede that role to big tech, governments or any other potential bad actors.

Privacy tools help us control who can see our data, where our data is stored and how it is used.

Evaluation of your risks and goals

- Why are you here? What are your goals?
- What are you afraid of? What are your risks?
- How can you improve the security of your current phone/tablet/computer?
- Burner Phone? No Phone?

HOW YOUR PHONE EXPOSES YOU



MOBILE RADIOS

Wifi

Cellular

GPS

Bluetooth

HOW YOUR PHONE EXPOSES YOU

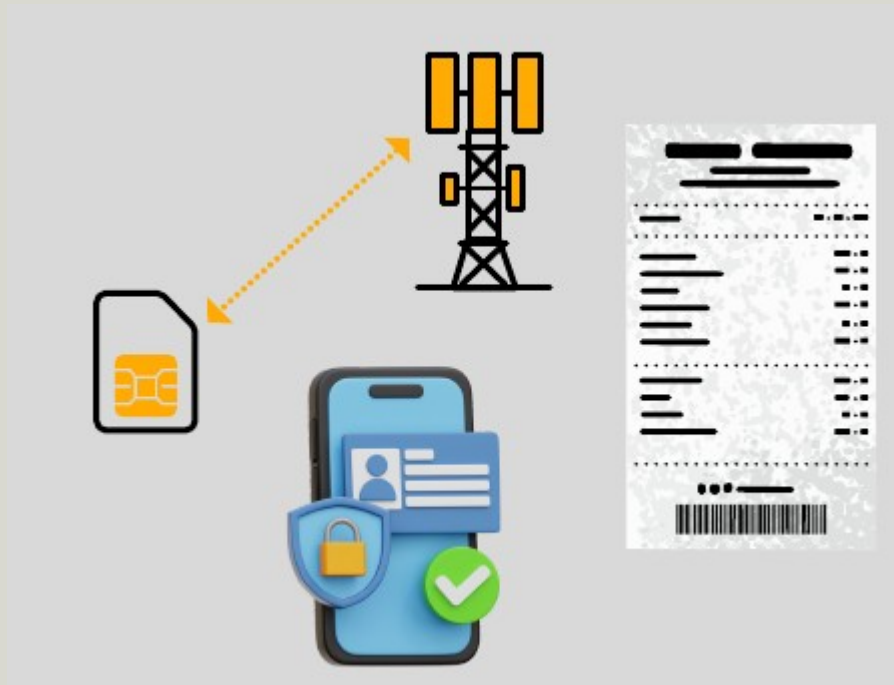
Wifi

Cellular

GPS

Bluetooth

Identity



Device ids make true phone anonymity nearly Impossible

- IMSI tied to your sim & cell tower access
- IMEI tied to your hardware

Identifiers: Payments/Contracts, phone number, Digital id.

Exposed by: Carriers, sim, registration, tower logs, biometrics.

HOW YOUR PHONE EXPOSES YOU

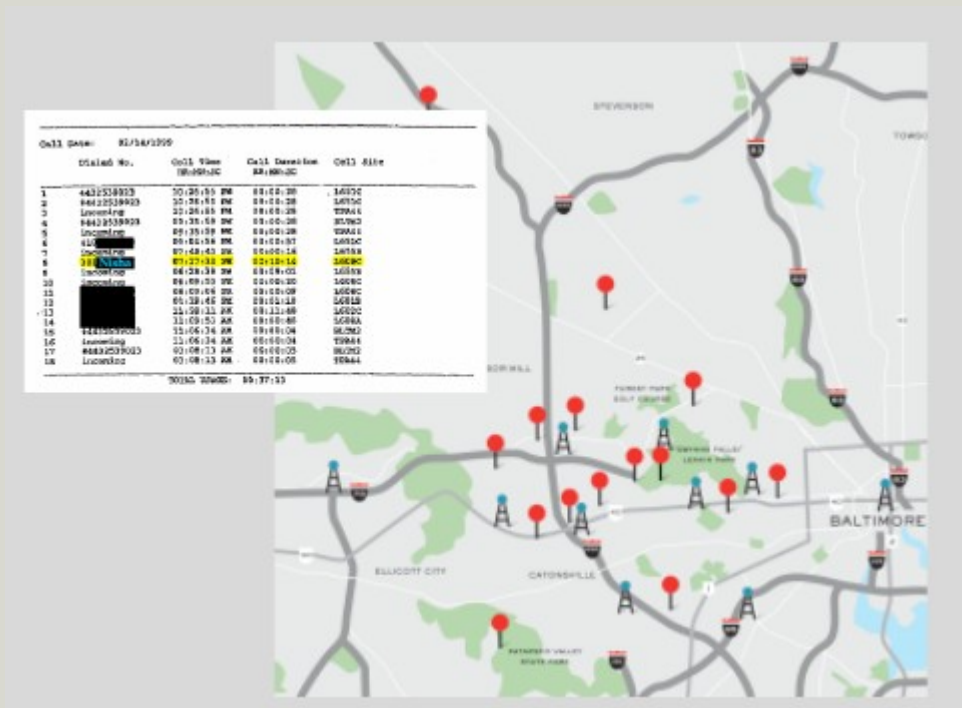
Wifi

Cellular

GPS

Bluetooth

Location



Identifiers: GPS, wi-fi, bluetooth, cell towers, sensors.

Exposed by: Apps, websites, spyware, stalkerware, tower dumps & data brokers.

HOW YOUR PHONE EXPOSES YOU

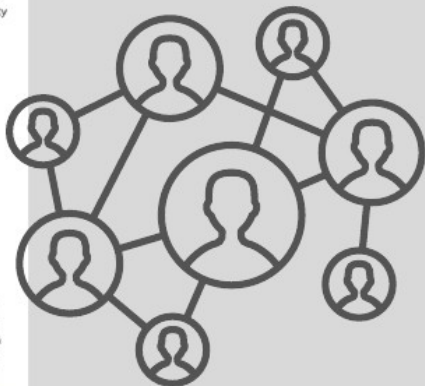
Wifi

Cellular

GPS

Bluetooth

Communications



Identifiers: Calls, texts, messaging links, contacts, email

Exposed by: Apps, spyware, stalkerware, phone breaking software, data brokers.

HOW YOUR PHONE EXPOSES YOU

Wifi

Cellular

GPS

Bluetooth

Content and Storage

Table 2: Android OS Access Support Matrix – Locked devices 7.69.1

Vendor (Chipset)		Section 1: COLD - turned off (Secure startup or FBE)		Section 2: HOT (AFU or FDE without secure startup)		Comments and exceptions		Fully Supported
		BFU extractions (for FBE devices)	Brute-Force Password to get the user data (CE) decrypted	All Extractions (Even without BF)	Brute-Force password (not needed for extraction)			
Samsung (Exynos / MTK / Qualcomm)	Android 6	✗	✗	✓	✓		✗	✗
	Android 7-14	✓	✓	✓	✓	Added BF support for Q2 S24, S24+, S24 Ultra		✓
Huawei (Kirin / Qualcomm / MTK)		✓	✓	✓	✓	PAQ family is supported for Brute-force only up to -04-2021 SPL		✗
Pixel	Pixel, Pixel XL	✓	✓	✓	✓			
	Pixel 3 - 5	✓	✓	✓	✓	Added AFU support for Android 14 Official and Pixel 8. BF support for Pixel 3-5 extended to latest SPLs		
Non-Samsung Q including Huawei, Motorola, Xiaomi, OnePlus and many		✓	✓	✓	✗			✗

For Non-Samsung/Pixel, Qualcomm FBE devices, there may be a requirement for 24hr waiting of the device prior to brute force attack. Affected devices: SM4350, SM7180, SM7180, 150 and newer.

Leaked Docs Show What Phones Cellebrite Can (and Can't)

The leaked April 2024 documents, obtained and verified by 404 Media, show Cellebrite could not unlock a large chunk of modern iPhones.

Identifiers: Accounts, apps, photos, backups, files

Exposed by: Apps, spyware, forensic tools (Cellebrite, Graykey), Cloud subpoenas

Re-frame the use and purpose of your devices

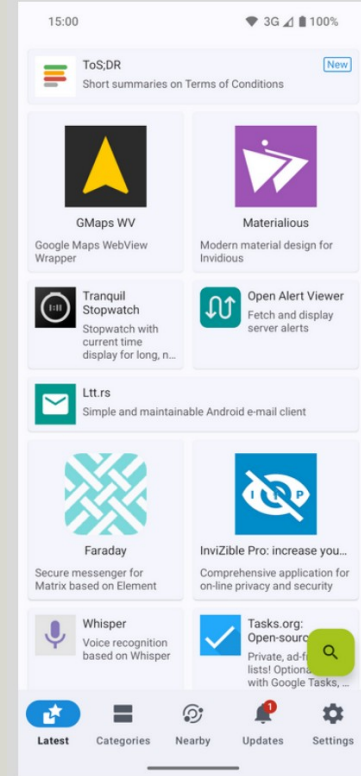
- 1.What is the purpose of you device?
- 2.How does the purpose determine our use?
- 3.How does the use affect your security and privacy practices for the particular device?
- 4.What is the role of your mobile OS computer/phone (Android, iOS)
- 5.What is the role of your desktop/laptop computer (Windows, Mac, Linux)

TIPS FOR ALL MOBILE DEVICES

1. KEEP Device & OS as updated as possible
2. STRONG Pin, not biometrics
3. DISABLE Cloud backups / use encrypted backups
4. ENFORCE Strict app permissions (deny mic, camera, location) unless needed
5. RADIOS Off (gps/wi-fi/bluetooth) unless needed
6. STORE Minimal sensitive data
7. REMOVE unneeded apps
8. REVIEW apps, permissions after software updates or, at least quarterly
9. CHANGE your search engine from Google to an alternative
10. Restrict use of sms texting which is not secure. Only use encrypted messaging services such as Signal

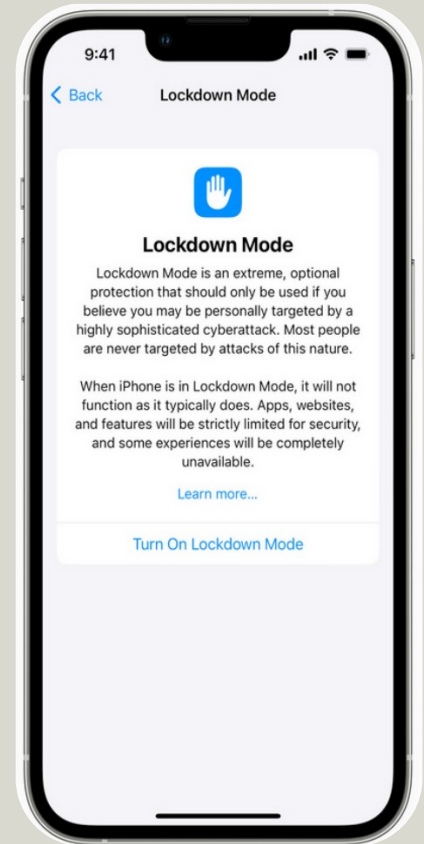
TIPS FOR ANDROID DEVICES

1. Disable google location history and ad personalization
2. Use Firefox or Brave instead of Chrome
3. Restrict Gemini / Google Assistant
4. Consider F-DROID for trusted apps
5. Consider a “Hardened” OS Alternatives like GrapheneOS

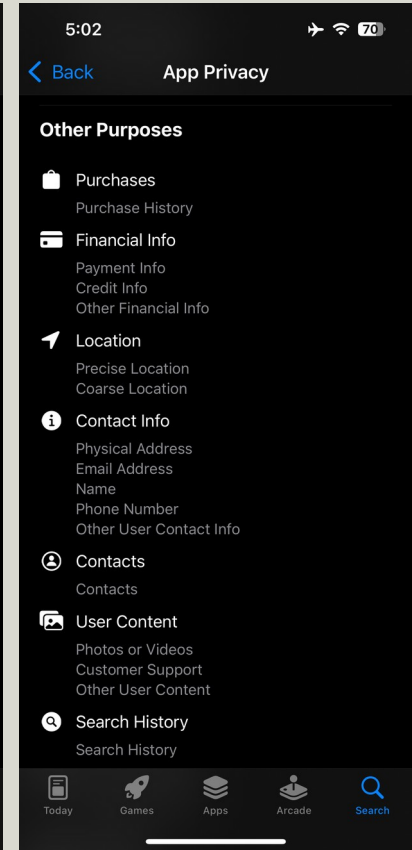
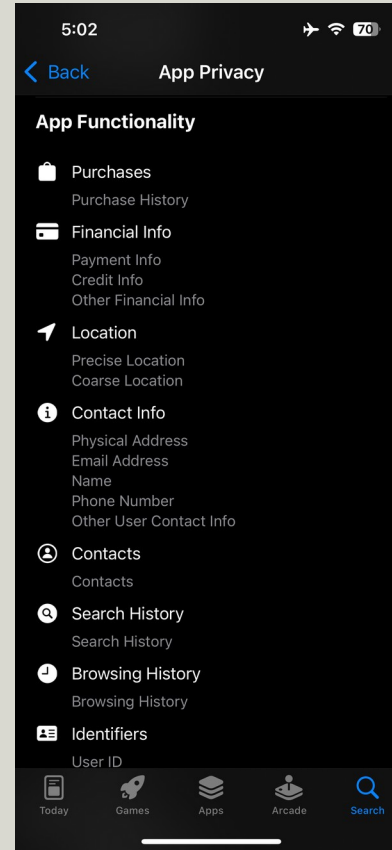
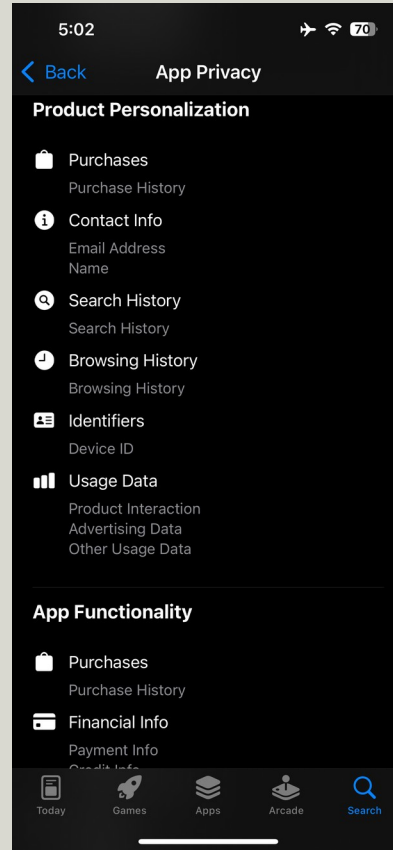
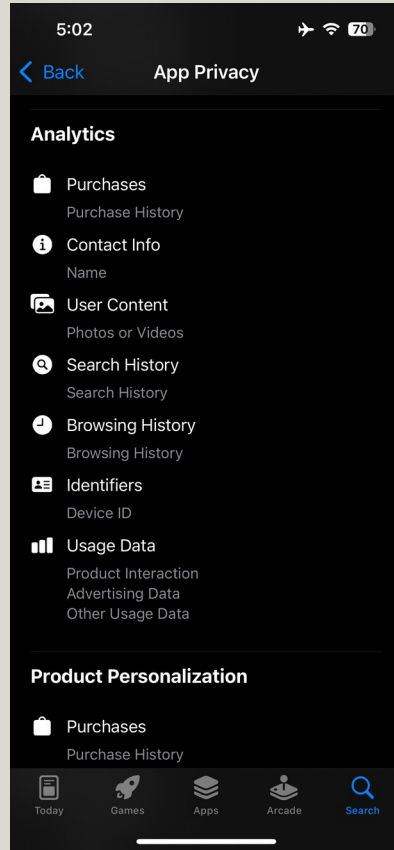
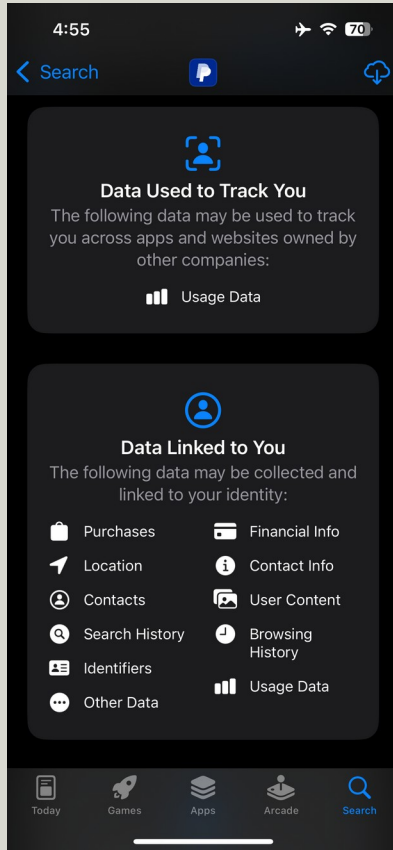


TIPS FOR iOS DEVICES

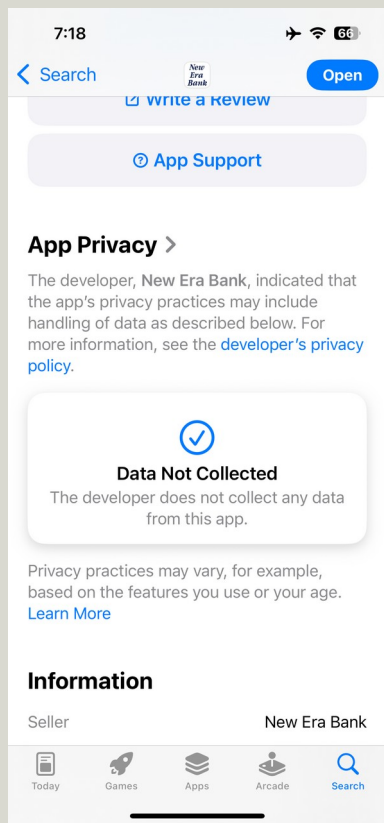
1. Enable “ask app not to track”
2. Restrict Siri & Apple intelligence
3. Turn off iPhone Analytics Data
4. Turn off Personalized Ads
5. Turn off “Allow Apps to Request to Track”
6. Turn off “Enable Sensor & Usage Data Collection”
7. Turn off “Improve Siri & Dictation”
8. Erase after 10 failed passcode attempts
9. Use lockdown mode (ios 16+) if high-risk



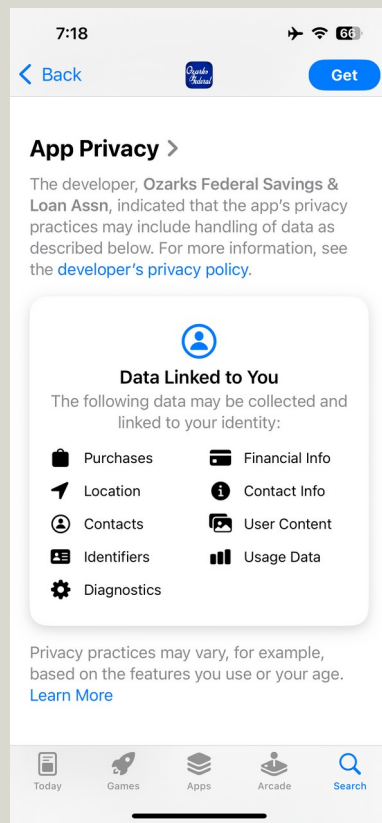
APPS AND PRIVACY



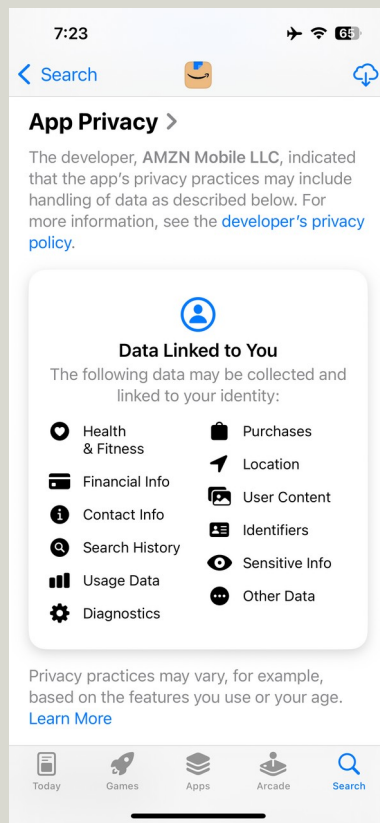
APPS AND PRIVACY



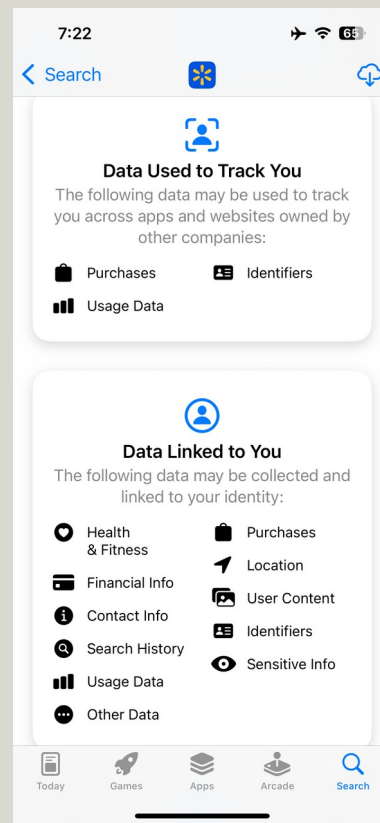
New Era



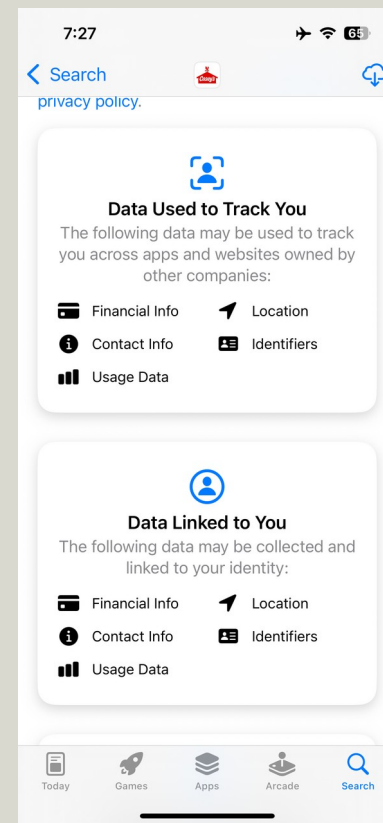
Ozarks Federal



Amazon



Walmart















Casey's

COMPUTERS

1. START WITH YOUR BROWSER One of the first and best things you can do for your privacy and security is to switch from Chrome. Export your bookmarks and, if you've saved your passwords in Chrome export those as well. Like all Google products, Chrome shares your private user data with Google. It's not private. Remember, Google's entire business model is based on data collection.

What are the alternatives?

1. LibreWolf, Mullvad, Brave are all well regarded. LibreWolf is as a fork of Firefox that has various default settings that improve it over Firefox. Firefox is also an improvement over Chrome. My preference is LibreWolf.
2. Install the Privacy Badger Plugin created by the well regarded privacy and security advocate Electronic Frontier Foundation.
3. Import bookmarks and passwords.
4. Browse the web with greater privacy!

Desktop													
Browsers		Brave	Chrome	Duckduckgo	Edge	Firefox	Librewolf	Mullvad	Opera	Safari	Tor	Ungoogled	Vivaldi
		1.81	139.0	1.150	139.0	141.0	141.0	14.5	120.0	18.6	14.5	139.0	7.5
Tracker content blocking tests													
Which browsers block important known tracking scripts and pixels?													
Adobe	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Adobe Audience Manager	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Amazon adsystem	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
AppNexus	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Bing Ads	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Chartbeat	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Criteo	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
DoubleClick (Google)	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Facebook tracking	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Google (third-party ad pixel)	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Google Analytics	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Google Tag Manager	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Index Exchange	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
New Relic	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Quantcast	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Scorecard Research Beacon	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Taboola	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Twitter pixel	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗
Yandex Ads	✓	✗	✓	✗	✗	✓	✓	✗	✗	✗	✗	✗	✗

Browser Testing Reviews/Ranking: <https://privacytests.org>

COMPUTERS

2.CHANGE YOUR SEARCH ENGINE If you're still searching with Google, stop. Change your default search engine to one of the alternatives that are more respectful of your privacy.

What are the alternatives?

- DuckDuckGo.com
- Startpage.com
- Search.brave.com
- Ecosia.org

COMPUTERS

LOCAL FILE STORAGE OVER CLOUD STORAGE This is a change that may take more planning and effort if you have been using cloud-based storage for a while. Apple, Google, Microsoft all encourage users to store their photos, documents and other important data in their cloud storage offerings. It's tempting because it is very convenient.

Why choose local data storage?

Managing your own data locally is more effort especially at the initial set-up. Even after set-up a user needs to pay some attention to taking care of a locally stored data. But it is more private and secure.

The scope of this change is beyond this presentation but you should begin thinking about it now.

COMPUTERS

Free and Open Source software and a Free OS

Consider an alternative to the proprietary Operating Systems offered by Microsoft, Apple and Google. **GNU/Linux**. Because it's open source it is open to constant scrutiny.

- Especially useful for older hardware because it will continue to receive updates for a much longer period.
- No ads, no malware, no back-doors
- No unwanted settings changes made by the OS manufacturer to benefit the manufacturer
- No analytics or other tracking

COMMUNICATIONS

Email and Messaging

Email was never designed to be secure! Even the few that offer encryption are only fully encrypted when communicating with users of the same service. But services, most notably Google, are designed so that your data can be collected by the provider. Given almost everyone needs at least one email account why not choose the most private, secure option?

In contrast to email, there are messaging services that are actually very secure by design. Most are not! We'll come back to this after email.

EMAIL

Gmail has become a near default email service for many people but is it private? **NO, it is not.** Both Chrome and Gmail are products provided by Google and both are intentionally designed to provide Google full access to your data.

After you switch from Chrome your second step should be to transition away from Gmail. Remember, Google's services are free because **they collect all of your data.**

What are the alternatives?

1. **Tuta, Mailfence and Proton** are well regarded email providers that offer enhanced levels of security. But you should be prepared to pay! They do offer a free plan but it is limited in storage. Personally, I think private email is well worth the \$3-6 per month. It's one of the few services I pay for.
2. Also worth checking: Mailbox and Runbox

MESSAGING

Signal. That's the one to use and I recommend it without hesitation over all others.

- **End-to-end encrypted**
- **Run by a non-profit** Signal is a service and software provided by a non-profit.
- **Cross platform and supports any device** Signal works on Windows, macOS, Android, iOS. While initial set-up needs to happen on a phone via a phone number, the Signal application can then be installed on tablets or computers and linked to the phone number based account.
- **Text, Audio and Video** A secure way to make audio calls to other Signal users
- **Free and open source** Signal is not a proprietary application but, rather, is free and open source software open to security and privacy audits.

Yes, it's free but they accept and encourage donations. I donate several times a year. Like email, I value a private, secure messaging service and am happy to donate.

LINKS AND RESOURCES

Browsers:

- LibreWolf: <https://librewolf.net>
- Mullvad: <https://mullvad.net/en/download/browser/linux>
- Tor: <https://www.torproject.org>
- DuckDuckGo: <https://duckduckgo.com/>
- Brave: <https://brave.com/download>
- Firefox: <https://www.firefox.com/en-US>

Browser Extensions:

- EFF Privacy Badger: <https://www.eff.org/pages/privacy-badger>

Browser Testing Reviews/Ranking:

<https://privacytests.org>

LINKS AND RESOURCES

Email Providers:

- Tutanota: <https://tuta.com>
- Mailfence: <https://mailfence.com>
- Proton: <https://proton.me>
- Mailbox: <https://mailbox.org>
- Runbox: <https://runbox.com>

Messaging

- Signal: <https://www.signal.org>

LINKS AND RESOURCES

Learn more:

- **Electronic Frontier Foundation:** <https://www.eff.org>
- **Ludlow Institute:** <https://www.ludlowinstitute.org>
- **NBTV:** <https://www.nbtv.media/episodes>

Getting Started Play List:

- Privacy 101: <https://odysee.com/@NaomiBrockwell:4/privacy-101:3>
- Dump the Apps: <https://odysee.com/@NaomiBrockwell:4/dont-migrate-from-backup:f>
- Show your papers: <https://odysee.com/@NaomiBrockwell:4/KYC:9>
- Secret Code In Your Apps: <https://odysee.com/@NaomiBrockwell:4/Byron-Tau:1>

LINKS AND RESOURCES

In Depth Topics:

- EFF Surveillance Self Defense: <https://ssd.eff.org/module-categories/basics>
- EFF: Encryption: <https://ssd.eff.org/module/what-should-i-know-about-encryption>
- Ludlow Institute: <https://www.ludlowinstitute.org>
- NBTv: <https://www.nbtv.media/episodes>

Getting Started Reading List:

- *Means of Control*, Byron Tau
- *Privacy is Power*, Carissa Veliz
- *Extreme Privacy: What It Takes to Disappear*, Michael Bazzell