Privacy 2026

For Apple Devices (Mac, iPhone, iPad, etc)

Introduction:

- Back in April of 2026 I gave a presentation on security. I mentioned I did not have the space and time to discuss the related privacy concerns and issues.
- First let me discuss that you can never have absolute privacy.
  - Social security and Medicare know about you
  - If you pay taxes the IRS and corresponding State Tax authorities know about you
  - If you drive a vehicle the DMV knows about you
  - If you are on social media, likely many know about you.
  - If you hold other licenses or training certificates those organizations know about you.
  - If you have Credit cards those financial organizations know about you
  - If you own a home there is a lot of information about you because of it.

Introduction (cont'd):

- I'm going to have to restrict this presentation to topics to Apple devices, Apps, and the Internet tools you use.
  - There is a lot of discussion in the News lately on privacy concerns and issues.
  - Things like commercial companies with surveillance cameras in the streets
  - Smart TV and vehicles, and other appliances reporting details back to the manufacturer, who then sells data to others
  - The government itself taking away privacy, warrantless searches etc.
  - These are important issues, but these would take too much time to discuss and on the last one, start getting into politics.

Apple already has Privacy tools!

- Because of Apple's privacy philosophy, Apple has many Privacy tools built in.
- Let's start with the Safari browser
  - There is another browser, called Duck Duck Go, that has a VPN built in. It is a paid subscription browser. If you are interested research, it for yourself.
- The Safari browser is built into the Mac, iPad, iPhone, and Vision Pro operating systems. You do not have to buy it separately.
- In Safari, Go to Settings under the Safari Menu. Choose the Privacy button at the top of the settings box. You will see two items checked on by default
  - Prevent cross-site tracking: In Safari, "Prevent cross-site tracking" is a privacy feature that stops third-party companies, ads, and social media widgets from following your web browsing habits from one site to another. It blocks hidden tracking cookies and data collectors so companies cannot build a profile of your interests.
  - Hide IP address from trackers: Hides your IP address from known online trackers that load when you visit a website.
  - Best I can tell, these override Accept All Cookies on website privacy cookie banner

Apple already has Privacy tools! (cont'd)

- Apple has a feature called Private Browsing. It has been around since 2005; introduced on Safari 2.
- Important: This does not make you invisible on the internet. What it does is keep your browsing history private for the safari browser you are using. Safari won't remember the pages you visited, your search history, or your autofill information.
  - Obvious if you are on a public Apple device.
  - Good if searching or buying an anniversary gift, or something for the grandkid, who uses your mac when visiting
- There is another privacy tool in Safari. It is called iCloud Private relay.
  - It was introduced in September 2021 on Mac Monterey, IOS and iPad 15
  - It requires an iCloud plus subscription; however, the $0.99 tier supports this, no need to go to a higher more expensive tier.

Apple already has Privacy tools! (cont'd)

- Rather than me type all the info, let's go to Apple's own article on this topic:
- https://support.apple.com/en-us/102602
- Note the downside is that it only works on Safari. If your bank, utility company, or other site that uses its own application to access, you can't use private relay. Even if you are using the Safari browser, many of these sites check IP addresses, so you may not be able to use private relay.

VPNs:

- We discussed this in the security presentation I gave in April 2026
- As I said back then: Big concern on ”Free” – They need to make a profit. So, in many cases the free VPNs will sell your browsing habits to companies for profit.

Apple App Store:

- Nutrition labels for food came into existence in the early 1990's. Apple introduced privacy labels in 2020 in their Mac, iPhone, iPad, Apple TV, etc, App stores. They list the following:
  - **Data Used to Track You:** Information shared with other companies for targeted ads or ad measurement.
  - **Data Linked to You:** Information tied to your identity, like your name, address, or account ID.
  - **Data Not Linked to You:** Information collected anonymously that is not tied to your personal identity.
- Apple has a listing for its own apps:
  - https://www.apple.com/privacy/labels/
- Use this as a guide. A greeting card program probably needs your contact list. Other apps probably do not.

Other Applications:

- While most all iPhone, iPad, Watch apps come from their respective App stores, Mac apps can be obtained else ware.
- For these apps, look at the license agreement, or go the the Vendors website to see the privacy information
  - I checked my Eazydraw application, very direct in the privacy part of the agreement. Microsoft office was on their website and complex.

Common Sense on Social Media:

- Social media apps have been around for a while
- The rise of social media has had a major impact on privacy
- Here is a good guide from Harvard:
  - https://privsec.harvard.edu/best-practices-social-media
- Think about what you say on social media. News reports criminal gangs breaking into homes in an area. You go on Nextdoor an mention that the house just west of you owned by Jane Smith was hit a few days ago. You say that you are worried about the $250,000 heirloom you just got as an inheritance. Not only have you outed the victim, the gang uses Real estate listing to figure out your address and robs you.

Data Brokers (New Drop Platform):

- No doubt a lot of information about you has been already been obtained and is in the hand of Data Brokers. The data brokers then sell your information to other companies, marketers, Insurance companies, and the like.
- You can try and go after data brokers individually, but that is a lot of work, since there are many of them.
- To opt out of data brokers, California residents can use the official Delete Request and Platform (DROP) tool provided by the state to submit a single deletion request to hundreds of registered brokers.
- I just went though on this. You will need to know all your email address, and VIN's of your vehicles if you want them included, as well as things like your smart tv id, and android devices.
- Note they don't state that the previous info that the companies buy from data brokers is still in their hands. Time will make this older information less accurate and valuable.

Final Thoughts:

- There is far more to go into privacy than I can go into here.
- There is a lot of information available on the Internet.

