Should I use a DNS Resolver?

What is Surveillance Capitalism?

Surveillance capitalism is an economic system where companies collect, analyze, and monetize personal data obtained from users' online activities. This data is used to predict and influence consumer behavior, often without the user's full understanding or consent. Big tech companies employ this model to offer free services (like search engines or social media) in exchange for user data, which they sell to advertisers or use to improve targeted advertising.

Key Features of Surveillance Capitalism:

1. **Data Exploitation**: Every click, search, and interaction is tracked to build detailed profiles.
2. **Behavior Prediction**: Companies use data to predict and influence user behavior for profit.
3. **Privacy Concerns**: Users often have little control over how their data is used.

What is a DNS Resolver?

A **DNS resolver** is a service that translates human-readable domain names (e.g., www.example.com) into machine-readable IP addresses (e.g., 192.168.1.1) so computers can communicate and load the requested website or service.

Why Should Anyone Use a Privacy-Focused DNS Resolver?

1. **Prevent Tracking**: Many DNS resolvers log user queries, which can reveal browsing habits. Privacy-focused resolvers avoid or minimize this tracking.
2. **Enhanced Security**: They block access to known malicious websites and phishing domains.

3. **Censorship Bypass**: Some ISPs or governments block access to specific websites. A private DNS resolver can help bypass these restrictions.
4. **Ad and Tracker Blocking**: Many privacy DNS resolvers block ads and trackers at the DNS level, reducing invasive data collection.
5. **Faster Browsing**: High-quality resolvers are optimized for speed, improving website loading times.

DNS Resolver	Signed Apple Profile	Signed Google Profile	Protocols Used	Privacy & Logging Policy	ECS Usage
Quad9 (9.9.9.9)	Yes	Yes	DoH, DoT, DNSCrypt	No logging of personal data	No (disabled to preserve privacy)
Cloudflare (1.1.1.1)	Yes	Yes	DoH, DoT	No logging of identifiable data, logs deleted within 24 hours	Yes (opt-in, anonymized)
NextDNS	Yes	Yes	DoH, DoT	No logging of personal data	No (disabled to preserve privacy)
AdGuard DNS	Yes	Yes	DoH, DoT, DNSCrypt	No logging	No (disabled to preserve privacy)
OpenDNS (208.67.222.222)	No	No	Standard DNS, DNSCrypt	Logs anonymized and used for security analysis	Yes
DNS.Watch (84.200.69.80)	No	No	Standard DNS	No logging	No
UncensoredDNS	No	No	Standard DNS	No logging	No
Mullvad DNS	No	No	DoH, DoT	No logging	No
CleanBrowsing (Family Filter)	Yes	Yes	DoH, DoT	No logging	No
Google Public DNS (8.8.8.8)	No	No	DoH, DoT, Standard DNS	Logs data temporarily for performance, no permanent PII storage	Yes

In summary, surveillance capitalism thrives on personal data, and using a privacy-focused DNS resolver is a step toward protecting your online activity from being monetized or misused. Protect your privacy and consider using DNS Resolver.