

# Privacy Policy Assistant: Analysis of Meta

## 🌟 Plain-language snapshot

Facebook’s (Meta’s) June 16 2025 privacy policy says it **collects a lot**—everything you post or view, device signals, location clues, in-app purchases, and even data that partners gather about what you do **off** Facebook and Instagram. Meta shares slices of that data with advertisers, measurement vendors, outside researchers, AI partners and other Meta brands, but states it “*never sells*” your info. You can delete posts or your whole account, yet Meta may hang on to certain records for legal or “safety & integrity” reasons. If you’re in Pennsylvania, no comprehensive state privacy law (like California’s CCPA) applies, but you still get the federal-level rights Meta lists in its “United States Regional Privacy Notice”—mainly access, download, and deletion tools.

Below are the key issues that jumped out, ranked by severity.

## 🔍 Top concerns

Severity	Issue & quoted policy text	Why it matters
High	<b>Long retention—even after deletion</b> “We keep information as long as we need it... We may preserve your information... even after you request deletion... and it may take up to 90 days to delete, plus another 90 days for backups”	Your profile data can linger for months —and longer for legal holds—so truly purging your digital footprint is slow and sometimes impossible.
High	<b>Broad third-party sharing for ads &amp; analytics</b> “We share certain information with advertisers... businesses we hire... researchers...” and provide aggregated ad-performance reports; Meta also shares limited data with AI partners	Even without “selling,” the breadth of sharing lets many companies profile or target you. Opt-outs reduce but don’t stop this.
Medium	<b>Off-Facebook activity from partners</b> Meta receives data about “websites you visit... apps you use... purchases... whether or not you’re logged in”	Your browsing or shopping elsewhere feeds Facebook’s ad system. You can curb this in “Off-Facebook Activity,” but it’s on by default.

<b>Medium</b>	<b>Deletion tools come with caveats</b> You can bulk-trash posts or permanently delete the account, but Meta warns backups may persist and some info may be retained for legal reasons	Good that tools exist, but expect traces to endure if Meta claims a legal need.
<b>Low</b>	<b>Retention linked to product features</b> Example: search history kept up to six months unless cleared manually	Routine, but worth clearing activity logs if you'd rather not have a long trail.

## Overall recommendation

If targeted ads and extensive data sharing don't bother you, Facebook's controls (Privacy Checkup, Off-Facebook Activity, Ad Preferences, Account Deletion) give reasonable self-service options. **But if you prefer minimal tracking, you'll need to actively prune data, review settings regularly, and accept that some records can still be stored or shared.**

**My take:** For privacy-conscious users, consider tightening every setting, turning off "Off-Facebook Activity," and periodically downloading & deleting past posts. If that still feels too invasive, you might rethink using the platform altogether.

## Next steps you can take

- 1 Run Facebook's Privacy Checkup** to review who can see your posts and profile info.
- 2 Clear Off-Facebook Activity** and turn off future connections.
- 3 Adjust Ad Preferences** to limit interest-based ads.
- 4 Set reminders** to sweep search history and old posts.
- 5 Download a copy of your data** before deciding on account deletion.

*Remember to validate these findings yourself—policies change, and only you can decide your comfort level.*

**Would you like assistance taking any of these recommended steps today?**