DIGITALLY UNDRESSED

FREE TOOLKIT

The Ten-Minute Privacy Cleanse

Five high-impact changes anyone can make right now

You do not need to be technical. You do not need to read a book first. These five changes take ten minutes total and close the biggest privacy gaps on your phone, your browser, and your accounts. Works on iPhone, Android, Chrome, Safari, Firefox, and every major platform.

Estimated time: 10 minutes

From the book *Why Am I the Only One Naked?*
thedreamerai.com/digitally-undressed
Share this guide freely. Privacy is not a privilege.

Why This Matters

Right now, your phone is sharing your location with apps you forgot you installed. Your browser is telling advertisers which medical conditions you searched for last Tuesday. Your email address is linked to a shadow profile that data brokers sell for fractions of a penny.

None of this requires a hack. It is the default. These five steps close the five widest-open doors in your digital life - the ones that 90% of people never think to check.

[Step 1] Kill Background Location Access

- **iPhone:** Settings > Privacy & Security > Location Services. Scroll through every app. Change anything set to "Always" to "While Using" or "Never." If you have not opened the app in a month, set it to Never.
- **Android:** Settings > Location > App permissions. Change "Allowed all the time" to "Allowed only while in use" or "Not allowed." Pay attention to weather apps, shopping apps, and games.
- **Why it matters:** Background location access means the app tracks where you sleep, where you work, where your kids go to school, and which doctor you visit - 24 hours a day, even when you are not using the app.
- **The real cost:** This data is packaged into "movement profiles" and sold to advertisers, insurance companies, law enforcement, and anyone willing to pay. In 2024, a data broker was caught selling location data from a prayer app that tracked churchgoers.

> **PRO TIP**
> Do this every 3 months. App updates silently re-request "Always" access. Set a calendar reminder.

> **IMPORTANT**
> Google Maps and Apple Maps need location while using them. That is fine. The danger is "Always" access for apps that have no business knowing where you sleep.

[Step 2] Disable Your Advertising ID

- **iPhone:** Settings > Privacy & Security > Tracking > toggle OFF "Allow Apps to Request to Track." Then: Settings > Privacy & Security > Apple Advertising > toggle OFF Personalized Ads.
- **Android:** Settings > Privacy > Ads > Delete advertising ID. On newer versions: Settings > Security & Privacy > More Privacy Settings > Ads > Delete advertising ID. Confirm when prompted.
- **What this does:** Your advertising ID is a unique number that follows you across every app on your phone. Disabling it breaks the single easiest method advertisers use to connect your behavior across dozens of unrelated apps.
- **Real example:** Without this change, a period-tracking app, a shopping app, and a news app can all report back to the same advertiser that you are the same person - and share what you did in each one.

> **PRO TIP**
> On Android, *deleting* the ID is better than resetting it. Resetting just gives you a new number to track. Deleting removes it entirely.

[Step 3] Harden Your Browser and Switch Your Search Engine

- **Chrome:** Settings > Privacy and Security > Third-party cookies > Block third-party cookies. Then install uBlock Origin from the Chrome Web Store. Note: Google is phasing out Manifest V2 extensions - if uBlock Origin becomes unavailable on Chrome, switch to Firefox or Brave.
- **Safari:** Settings > Safari > verify "Prevent Cross-Site Tracking" and "Hide IP Address" are both ON. Safari handles this well by default - just confirm it is active.
- **Firefox:** Settings > Privacy & Security > Enhanced Tracking Protection > Strict. Firefox in Strict mode blocks most fingerprinting and cross-site trackers automatically.
- **Change your search engine:** In any browser, go to Settings > Search Engine and switch from Google to DuckDuckGo, Brave Search, or Startpage. Google logs every search tied to your identity. These alternatives do not.
- **Why browsers matter most:** Your browser sees everything - medical searches, financial questions, relationship problems, political views. It is more intimate than any single app on your phone.

> **REALITY CHECK**
> Chrome is made by the largest advertising company in history. Its privacy defaults protect Google, not you. If you want one change with maximum impact, switch to Firefox or Brave.

[Step 4] Delete Apps You Have Not Opened in 30 Days

- **iPhone:** Settings > General > iPhone Storage. Sort by Last Used. Anything you have not opened in 30+ days - delete it. Not "Offload." Delete.
- **Android:** Settings > Apps > sort by last used. Same rule. If you have not opened it in 30 days, it is not serving you - it is serving its investors.
- **Why deleting beats offloading:** Offloading removes the app but keeps its data and permissions. Deleting removes everything - including the background connections it maintained without telling you.
- **The real number:** The average American has 80+ apps installed and regularly uses 9. The other 71 are collecting data, pinging servers, and draining battery while doing nothing for you.

> **PRO TIP**
> After deleting, watch your email for "We miss you!" messages. Each one is an app that was actively tracking whether you left. That tells you everything about its priorities.

[Step 5] Turn On Two-Factor Authentication for Your Email

- **Gmail:** myaccount.google.com > Security > 2-Step Verification > Turn On. Use Google Authenticator or a passkey - not SMS text messages.
- **Outlook:** account.microsoft.com > Security > Advanced security options > Two-step verification > Turn on. Use Microsoft Authenticator.
- **Apple ID:** Settings > [Your Name] > Sign-In & Security > Two-Factor Authentication. Apple enables this by default on newer devices - verify it is active.
- **Why email specifically:** Your email is the skeleton key to your entire digital life. Every "Forgot Password" link goes to your email. If someone gets into your email, they get into everything - bank accounts, medical records, social media, tax returns.
- **Why not SMS:** Text message codes can be intercepted through SIM-swapping attacks, where someone convinces your carrier to transfer your number to their device. Authenticator apps and passkeys cannot be SIM-swapped.
- **Password managers:** Use Bitwarden (free, open-source) or 1Password. One strong master password protects hundreds of unique passwords. Never reuse passwords across sites.

> CRITICAL
> If you use the same password on more than one site, change that today. Data breaches expose passwords constantly - and attackers automatically try stolen passwords on every major site within hours.

What You Just Did

In ten minutes, you closed the five biggest gaps in your digital privacy.

You stopped apps from tracking your location around the clock. You broke the advertising ID that linked your behavior across every app. You hardened your browser against the most common tracking techniques. You eliminated dozens of dormant data collectors. And you locked down the single account that controls access to everything else.

You are not invisible now. But you are no longer standing in the middle of the room with every light on and the doors wide open.

Want the full picture?

Why Am I the Only One Naked? covers 50 platforms, graded A through F, with step-by-step fixes for each one.

Free with Kindle Unlimited.

Scan the QR code or visit amazon.com/dp/B0DQJPPKGM