12-PAGE PROTECTION GUIDE | NO MAILING LIST | PRINT & KEEP

THE *shield* GUIDE

Twelve plain-language pages on how to stop being inventory — what to click, where to click it, and what changes when you do.

SHIELD · 7 / 12 NOTCHES CLOSE THE BIGGEST LEAKS

FORMAT **FIELD GUIDE**	PAGES **12**	PLATFORMS COVERED **14+**	EST. READING TIME **22 MIN**
EST. DOING TIME **2–7 DAYS**	DIFFICULTY **LOW · MED**	REQUIRES **A PHONE · COFFEE**	REVISION **R4 · 05·26**

00 FROM THE FIELD

A SHORT *letter* BEFORE THE ACTUAL STEPS.

If you read the experiment, you saw your photos turn into a *cluster*, a *price*, a *feed*. This guide is the inverse. It is the small, dull, very effective set of clicks that make all of that *worse data* — which is the only currency the system actually fears.

HOW TO *read* THIS

Each platform gets a page. Each page gives you the exact menu path, the toggles to flip, and what changes if you do. Things you absolutely should do are tagged `DO TODAY`. Things to do once a quarter are `CAL. REMINDER`.

If a step still works the way we describe it, lovely. If a menu has moved (and it will), search the same phrase from the settings home — the platform almost never deletes the toggle, only relocates it.

WHAT THIS *won't* DO

This won't get you off the grid. It will, however, make you a worse customer to the auction. Worse data → cheaper bids → fewer dollars extracted → quieter feed. You become a less-profitable target. That is the goal.

QUICK TIPS · LIVE EVERYWHERE

01	**Reset your ad ID**	on iOS & Android once a month. Breaks behavioural lookalike continuity.
02	**Use a browser that blocks third-party cookies by default**	(Firefox, Brave, Safari). This kills the simplest tracker.
03	**One email per tier:**	a real one for humans, an alias one for shops, a throwaway for one-time sign-ups.
04	**Decline "personalized ads" every time you see the prompt.**	It is never the default.

DID YOU KNOW

The single most predictive signal the auction uses isn't what you post — it's *what you scroll past slowly.* Closing the "off-platform activity" pipe (covered later) blinds about 60% of that.

THE *index.*

01 UNIVERSAL FIRST MOVES

FIVE MINUTES. *Biggest* DROP IN THE WHOLE GUIDE.

Before you log in to a single platform: do these. They sit underneath every app on your phone and every tab in your browser, and they leak quietly all day. Five things, five minutes.

YOUR *phone's* AD ID

IOS · ANDROID

01	**iOS:**	Settings → Privacy & Security → Tracking → Turn off **Allow Apps to Request to Track**.
02	**iOS:**	Settings → Privacy & Security → Apple Advertising → off.
03	**Android:**	Settings → Privacy → Ads → **Delete advertising ID**.
04		Set a recurring monthly reminder to repeat the Android step — fresh ID = broken lookalike trail.

YOUR *browser*

DESKTOP & MOBILE

01	Switch your default to	**Firefox** or **Brave**. Safari is fine on iOS. Avoid Chrome as a daily driver if you can.
02	Install **uBlock Origin**	(or use Brave's built-in shields). One extension; 80% of trackers gone.
03	In settings, turn on **Block third-party cookies**	and **Send "Do Not Track"** (mostly symbolic, but the legal weight is rising in 2025–26).
04	Set search engine to	**DuckDuckGo**, **Kagi**, or **Startpage**.

DID YOU KNOW

The "anonymous" mobile ad ID resets to a brand-new random string the moment you tell your phone to. To the auction, you become a stranger again — for a few weeks. That alone cuts personalised ad value roughly in half until the system re-clusters you.

your EMAIL TIERS

PRO TACTIC

Each address is a join key — every site that knows your email can be matched against every other site. Split it.

TIER 1 · HUMANS	Your real address. Friends, family, doctor, bank.
TIER 2 · COMMERCE	One alias. Shops, airlines, loyalty. Use +shop or Hide-My-Email / SimpleLogin / DuckDuckGo Email.
TIER 3 · ONE-OFF	Throwaway alias per signup. Burn it when spam starts.

CAMERA & *location*

IOS · ANDROID

01	**Camera geotag:**	Settings → Privacy & Security → Location Services → Camera → **Never**	(iOS) or off (Android).
02	**Per-app location:**	open each social app's permissions and set to **Never** or **Ask Next Time**	. They do not need it.
03	**Significant Locations**	(iOS) → off. **Timeline** (Google) → off.	Both keep a quiet map of every place you sleep.

QUICK TIPS

01	Use a **password manager**		. Different password per site means a leak at one shop doesn't unlock the rest.
02	Turn on **2-factor auth**	using an *authenticator app*	, not SMS. SMS is the leakiest factor.
03	On your router, set DNS to **1.1.1.1** (Cloudflare) or **9.9.9.9** (Quad9).		Stops your ISP from selling your browsing.

YOU ARE NOT *finished*. YOU ARE NOW *readier.*

Everything from here is per-platform. Do the platforms you actually use, in the order they appear. The first one (Google) is the biggest, so it earns its own page.

02 GOOGLE · YOUTUBE · GMAIL

THE SINGLE *biggest* PROFILE YOU OWN.

Most people's Google profile is older, deeper, and more accurate than their actual diary. Five years of search, every map route, every video watched, every Gmail receipt. The good news: Google lets you delete almost all of it, and most users never have. Today, you will.

YOUR ACTIVITY *vault*

GOOGLE.COM / MYACTIVITY

01 Go to `myactivity.google.com` .

02 Click **Web & App Activity** → set **Auto-delete to 3 months** . (Not 18, not 36. Three.)

03 Do the same for **Location History** (now called *Timeline*) → **Turn off & delete** .

04 Do the same for **YouTube History** → **Auto-delete: 3 months** .

05 At the top of the page, click **Delete activity by → All time** . Confirm. DO TODAY

AD *personalization*

ADSSETTINGS.GOOGLE.COM

01 Go to `myadcenter.google.com` .

02 Turn **Personalized ads** → **OFF** . (Ads don't go away. They get dumber, which is the goal.)

03 Scroll down — Google lists every category it thinks describes you. Read it. Wince. Click **Off** on each.

04 Under **Partner ads settings** , turn off ad personalization for partners as well.

DID YOU KNOW

Until you change it, Google's default for new accounts is to keep Web & App Activity *forever*. The 3-month auto-delete option has existed since 2020 — it has just never been the default, and the screen that asks you about it is the easiest screen in the product to skip.

YOUTUBE *algorithm* RESET

YOUTUBE.COM

01 Click your avatar → `Your data in YouTube` .

02 **Pause Watch History** & **Pause Search History** for 30 days. See how the homepage changes.

03 From any recommended video, click ⋮ → **Not interested** → **Tell us why** . The algorithm learns aggression faster than approval.

04 Quarterly: open the same page and **Delete all watch history** . The graph forgets you. CAL. REMINDER

GMAIL *scanners*

GMAIL.COM

01 `Settings → See all settings → General → Smart features` → uncheck both boxes (one for Gmail/Chat/Meet, one for other Google products).

02 Open `Manage third-party access` at `myaccount.google.com/permissions` . Revoke every app you don't recognize or haven't used in 6 months.

03 Search your inbox for `unsubscribe` . Unsubscribe in bulk for 10 minutes. You'll be surprised how much you stop opting in to.

QUICK TIPS

01 Use **Incognito mode** in Maps when looking up sensitive places (clinics, lawyers, AA meetings). It is buried in your avatar menu and it actually works.

02 If you have an Android phone, `Settings → Google → All services → Ads` → **Delete advertising ID** .

03 Run the **Privacy Check-up** at `myaccount.google.com/privacycheckup` every quarter.

03 FACEBOOK

THE TOGGLE THEY *hid* IS THE ONE THAT MATTERS.

If you do exactly one thing on Facebook this week, do the *Off-Facebook Activity* reset. It severs the pipe that lets other websites and apps report you back to the mothership. The rest of this page is gravy.

OFF-FACEBOOK *activity*

META · DO TODAY

01	Go to `accountscenter.facebook.com` .	
02	**Your information and permissions → Your activity off Meta technologies** .	
03	Click **Disconnect future activity** . Confirm.	
04	Then **Clear previous activity** . The list will surprise you — restaurants, dating apps, hardware stores. Wipe it.	DO TODAY

AD *preferences*

META · 10 MIN

01	From any ad on Facebook, tap →	**Why am I seeing this?** . Read it. Then tap **Manage your ad preferences** .
02	Open **Ad topics** . Set every sensitive one (Politics, Alcohol, Parenting, Body) to	**See less** .
03	Under **Audience-based advertising** , find every advertiser who has your contact info and	**Remove** them. (Yes, all of them. Yes, it takes a minute.)
04	Under **Data about your activity from partners** , turn it	**Off** .

WHO *sees* WHAT

PROFILE PRIVACY

01	`Settings & Privacy → Privacy Checkup`		. Walk all five sections.
02	Past posts:	`Privacy → Limit who can see past posts`	. One click. Everything ever public becomes Friends-only.
03	Face recognition: turn it	**off**	. They keep the embedding either way, but no new matches.
04	Search-engine indexing of your profile:	**off**	. (Under `How people find and contact you` .)

DID YOU KNOW

Meta calls the pipe of data flowing in from *other* apps and websites the *"Meta Pixel."* It sits on roughly a third of the entire commercial web. When you clear it, you don't just opt out of one ad category — you become invisible to the lookalike model that prices most of your future feed.

QUICK TIPS

01	Download your data first:	`Settings → Your Facebook information → Download Profile Information`	. Useful to know what they have on you.
02	Quit the	**Messenger**	app on your phone and use the web version. Far fewer permissions, same conversations.
03	Delete inactive Pages, Groups, and old reactions. The graph remembers everything you don't.		

FIELD NOTE

If you have not opened Facebook in two years, deactivating is more valuable than tweaking. `Settings → Account ownership and control → Deactivation and deletion → Deactivate`. You can come back at any time. **Deletion** is the permanent version and takes 30 days to process.

04 INSTAGRAM & THREADS

TWO APPS, *one* AUCTION. THREE SWITCHES THAT BITE.

Both apps feed the same Meta machine you just throttled on the previous page. Most of the work is already done. These are the platform-specific switches that the Off-Facebook-Activity sweep doesn't reach.

INSTAGRAM *basics*

META · IOS · ANDROID

01	**Private account:**	`Settings → Account privacy` → on. The single biggest reduction in passive scraping.
02	**Activity status:**	`Messages and story replies → Show activity status` → off.
03	**Story replies / mentions / tags:**	set to **People you follow** .
04	**Suggested content / topic prefs:**	Settings → `Content preferences` . Hide political and sensitive content. Snooze suggested posts.
05	**Read receipts in DMs:**	off. (Settings → Messages.)

ADS & *data*

ACCOUNTS CENTER

01	`Settings → Ads` → **Ad topics**	: dial each to **See less** .
02	`Ad activity`	shows which advertisers reached you. Use it to identify which sites are quietly sharing your data with Meta.
03	`Apps and websites`	→ revoke anything you no longer use.
04	Under **Camera roll sharing suggestions**	→ off. Stops Instagram from scanning your unposted photos for caption / location guesses.

THREADS *specifically*

META · 2026

01	Threads inherits a copy of your Instagram graph. Once you sign up, you can't undo that without deleting the Threads profile entirely.	
02	**Personalized ads**	(now in EU/UK and rolling out everywhere): toggle **off** when prompted. If you weren't prompted, check `Settings → Account → Other account settings` .
03	Threads honors your Instagram **Private** setting separately — re-check that `Privacy → Private profile` is on.	
04	Delete the Threads profile (not the Instagram one) at `Settings → Account → Delete or deactivate profile` .	

DID YOU KNOW

Instagram reads more than what you post. The model also clocks *how long you stop on a photo*, whether you screenshot, whether you re-watch a Reel, and whether you mute the sound — those four micro-signals together explain a startling amount of your inferred persona. None of them are visible to you, and none can be deleted.

QUICK TIPS

01	Strip EXIF data from photos before posting. iOS: Share → Options → **Location off** . Or use the *Metapho* app on iOS / *Scrambled Exif* on Android.	
02	Use a separate burner Instagram for following celebrities/brands. Keep your main one tight.	
03	Turn off **Allow others to share your story as a message** .	

05 TIKTOK

THE FASTEST *learner* IN THE BUILDING.

TikTok's For You algorithm gets a working model of you in about *40 minutes* of scrolling. That is its product and its problem. You cannot make it forget — but you can starve it, slow it, and tell it to stop selling what it learns.

ADS & *data*

DO TODAY

01	`Profile → ≡ → Settings and privacy → Ads`			. Turn off	**Personalized ads**	.	
02	`Settings → Privacy → Data`	. Turn off	**Sync contacts and friends**	. Then tap	**Remove your contacts**	. (TikTok keeps any phone book it has already swallowed unless you do this.)	
03	`Settings → Privacy → Personalization and data`			→ turn off	**Personalized ads from off-TikTok activity**	.	
04	Same screen →	**Data download**	. Request your archive. It's a useful jolt.				

RESET YOUR *algorithm*

SETTINGS

01	`Settings → Content preferences → Refresh your For You feed`			. The big red button. It rebuilds the model from scratch.			
02	Under **Filter video keywords**	, blocklist terms you don't want fed (e.g. specific topics, body-talk, political tags).					
03	Long-press any video on For You →	**Not interested**	→ **More details**	. The model weighs	*active dislike*	much higher than passive scrolling-past.	
04	Quarterly: re-refresh. CAL. REMINDER						

PROFILE *visibility*

PRIVACY

01	**Private account:** `Privacy → Private account`	→ on.
02	**Suggest your account to others:**	off.
03	**Downloads:**	off. (Stops anyone — including bot farms — from grabbing your videos at full quality.)
04	**Activity status:** off. **Read receipts:**	off.

DID YOU KNOW

TikTok records *watch-duration to the millisecond*, not just likes and saves. A video you watched all the way through but never liked counts as a stronger signal than one you liked but skipped halfway. The "like" you thought was the loud signal is actually the quiet one.

QUICK TIPS

01	Turn on **Screen time → Daily screen time limit**	. 30 min is plenty. The model learns slower if you scroll less.		
02	**Restricted Mode**	for younger users is genuinely useful — fewer adult inferences feed the cluster.		
03	If TikTok is banned, restricted, or removed in your jurisdiction in 2026, your data does not automatically delete. Submit a	**delete account**	request before uninstalling.	

FIELD NOTE · CREATORS

If you post for a living: open a separate creator account from a separate email and a separate phone number where possible. The algorithm cross-references your viewing patterns against your posting patterns to estimate your *own* audience class — which sets your ad floor. The cleaner your personal viewing, the better the recommendation health on your creator side.

06 X (FORMERLY TWITTER)

THREE SWITCHES AND A BRAND-NEW *data buyer*.

As of 2024–25, X explicitly added consent to use your posts as training data for AI models. That permission lives in a single checkbox. Most users have never seen it. Also worth knowing: X's "Topics" system is the most legible inferred profile any major platform shows you. Read yours. It's instructive.

DATA *sharing*

DO TODAY

01 `Settings & privacy → Privacy and safety → Data sharing and personalization` .

02 Turn off **Allow Grok and xAI to use your posts and interactions for training** . (Web only — the mobile app does not expose this toggle. Use the website.) DO TODAY

03 Turn off **Personalized ads** .

04 Turn off **Share device-level information with business partners** .

YOUR INFERRED *self*

EYE-OPENING

01 `Privacy and safety → Content you see → Topics` . Mute every topic that doesn't reflect you.

02 `Privacy and safety → Ads preferences → Interests` . The model lists every word it associates with your behavior. Untick the wrong ones; *especially* politics, finance, health.

03 Same screen → **Inferred identity** → **Don't personalize based on identity** . Switch off.

04 **Tailored audiences** → list of advertisers who have your contact data. Opt out of all.

DISCOVERABILITY

PROFILE

01 **Photo-tagging:** `Privacy and safety → Audience, media and tagging → Photo tagging` → off.

02 **Let others find you by email / phone:** both off.

03 **Discoverable by:** uncheck phone & email.

04 If you don't post: consider **protecting your posts** . It does not stop the model from training on you, but it stops scrapers.

DID YOU KNOW

X's *"Tailored audiences"* list is a literal inventory of every advertiser who already has your email or phone number from somewhere else and has chosen to target you specifically. Reading it tells you which of your other accounts have been shared without your remembering.

QUICK TIPS

01 Drafts on X are stored server-side. Anything you typed and didn't send is still there.

02 To leave: `Settings → Your account → Deactivate` . Deactivation reverses if you log in within 30 days; after that, it's deletion.

03 If you have years of old posts you can't bear to scrub by hand: tools like *Cyd* and *Redact* bulk-delete with filters. Run them on a private account.

07 SNAPCHAT · PINTEREST · REDDIT

THE *quieter* PIPES. STILL LEAKING — JUST SLOWER.

These three earn a shared page because the work is similar. They're smaller graphs but they each plug into the same ad exchanges. Same idea: turn off the personalisation, untick the partner data, prune the discoverability.

SNAP*chat*

SNAP INC.

01 `Profile → ⚙ → Privacy Controls → Ads` . Turn off **Audience-Based** , **Activity-Based** , **Third-Party Ad Networks** , **Lifestyle Categories** .

02 **Snap Map** → set to *Ghost Mode* . (You can still see friends; they stop seeing you.)

03 **My AI** chatbot: `Settings → My AI → Clear data` . Unpin it.

04 **Contact syncing** → off & **Delete all contacts** .

05 Quarterly: **Download My Data** from Settings. Useful audit. CAL.

PIN*terest*

PINTEREST INC.

01 `Settings → Privacy and data` . Turn off **Personalize ads using info from our partners** .

02 Same page → **Personalize based on websites you visit** → off.

03 `Settings → Account management → Search privacy` . Hide your profile from search engines.

04 Under **Notifications** , disable every email category you didn't ask for. Pinterest is the leakiest emailer of the three.

05 Pinterest reads your screenshots in the app — **Camera roll permissions** → tighten.

RED*dit*

01 `Settings → Pr` Personalize a from our part

02 Same screen → **Persona recomm based o activity**

03 **Profile visibility** → cons from s being

04 Reddit posts are *public and indexed by AI training scrapes*

05 Two-factor auth: app.

DID YOU KNOW

Snapchat's Snap Map shows your bitmoji on a map of friends by *default* for many account types. People who think they've "always had it off" frequently haven't. Open the map. Look for your own face. Hide it.

QUICK TIPS · ALL THREE

01 None of these need access to your contacts. Revoke at the OS level: `Settings → Privacy → Contacts` .

02 If you don't post: lurking is fine, but the account still earns its keep. Inactive accounts are worth less to the ad system than active ones — keep yours inactive if you can.

03 Email aliases (Hide My Email, SimpleLogin, DDG) work beautifully on all three signup forms.

08 LINKEDIN

THE CAREER FILE. *also* THE INSURANCE FILE.

LinkedIn looks like a résumé site. It also feeds Microsoft's broader advertising stack and is increasingly bought by background-check and underwriting vendors. The cluster it builds on you doesn't only price your next job — it prices your next loan.

DATA *privacy*

DO TODAY

01 `Me → Settings & Privacy → Data privacy` .

02 **Data for Generative AI improvement** → **Off** . (Yes, this is on by default in most regions as of 2024.) DO TODAY

03 **Social, economic, and workplace research** → off, unless you actively want LinkedIn sharing your data with academic and corporate researchers.

04 **Sync contacts** & **Sync calendar** → off. **Manage and remove** any contacts already synced.

05 **Personal demographic information** → review what gender / disability / ethnicity inputs you provided. You can blank them.

ADVERTISING *data*

SETTINGS

01 `Advertising data` . Walk every section. Turn off: *Interest categories, Audience insights, Connections, Profile data for ad personalization, Third-party data, Ads outside LinkedIn* .

02 Same path: **Data collected on partner sites and apps** → off.

03 **Personalized ads in the LinkedIn Audience Network** → off.

VISIBILITY

PROFILE

01 **Profile viewing options:** private mode (or semi-private). Useful when researching companies you don't want to alert.

02 **Edit your public profile:** `https://www.linkedin.com/public-profile/settings` . Toggle off the fields you don't want to be in Google.

03 **Who can see your connections** → **Only you** . Recruiters scrape this for prospecting.

04 **Profile discovery using email/phone** → set to **1st-degree connections** only.

05 Turn off **Career insights** notifications — these are also signals being collected on you.

DID YOU KNOW

LinkedIn data is one of the most actively purchased sets by background-check companies and small-business insurance underwriters. A "spotty job history" inferred from your timeline can change a quote you receive — without you ever being told that's where it came from.

QUICK TIPS

01 If you're not job-hunting: turn off **Open to work** entirely. The signal leaks into your ad cluster regardless of who you wanted to share it with.

02 Remove your phone number from your profile if it's there. It is one of the strongest cross-platform join keys in the entire ad ecosystem.

03 Yearly: `Get a copy of your data` → **The works** . Audit annually. CAL.

09 DATA BROKERS · THE HIDDEN TIER

THE COMPANIES THAT *have* YOUR ADDRESS — WITHOUT YOU.

Underneath the social platforms is a much older industry of *data brokers*: firms that buy public records, purchase histories, magazine subscriptions, voter rolls, and resell composites. You almost certainly have a file with every one of these. They are easy to opt out of. Just nobody tells you.

BROKER	WHAT THEY SELL	OPT-OUT URL	TIME
Spokeo	Aggregated "people search" — name, address, relatives, phone.	spokeo.com/optout	5 min
Whitepages / Whitepages Premium	Address history, age, household members.	whitepages.com/suppression-requests	5 min
BeenVerified	Background-style profiles bought by employers, landlords.	beenverified.com/app/optout	5 min
Intelius / TruthFinder / InstantCheckmate	Same parent. One opt-out covers all three.	suppression.peopleconnect.us	5 min
MyLife	"Reputation score" pages — frequently appear high in Google for your name.	mylife.com/ccpa/index.pubview	5 min
Acxiom	One of the largest commercial data brokers. Powers a lot of email marketing.	isapps.acxiom.com/optout/optout.aspx	5 min
LexisNexis / RELX	Underwriting data — insurance and credit-adjacent.	optout.lexisnexis.com	10 min · ID
Oracle Data Cloud (BlueKai)	Cookie-based identity graph powering many display ads.	oracle.com/legal/privacy/marketing-cloud-data-cloud-privacy-policy.html	5 min
Epsilon / Experian Mosaic	Postal & "lifestyle" segments — junk mail and credit pre-screen.	epsilon.com/us/consumer-information · experian.com/privacy	10 min
Radaris · Nuwber · PeopleFinders	Spammier people-search aggregators. Same playbook.	each: /control / opt-out at footer	5 min ea.
National Consumer Telecom & Utilities Exchange (NCTUE)	Used by ISPs & utilities to set deposits.	exchange-service.com → opt-out	10 min
Direct Marketing Association (DMAchoice)	Junk mail master list.	dmachoice.thedma.org	10 min · $4 fee

DID YOU KNOW

Brokers *re-import* your data from public records every few months. An opt-out is not permanent — set a calendar reminder twice a year to re-submit. The good ones (Acxiom, LexisNexis) honor a one-time opt-out indefinitely. The cheap ones (Spokeo, Radaris) do not.

QUICK TIPS

01 If 30+ brokers feels brutal: services like **DeleteMe**, **Optery**, and **Kanary** will do it for you for ~$10–15/month. Use the free tier first to see what they find.

02 In California, Colorado, Connecticut, Virginia, Utah, Texas, Oregon, and a growing list of US states, you have a **legal right** to opt out. Brokers must comply within 45 days.

03 In the EU/UK, the GDPR/UK-GDPR **right to erasure** is even stronger. Submit a DSAR (data subject access request) by email; one sentence suffices.

04 If you've ever had a stalker, an estranged ex, or job-search anxiety — start with MyLife, Spokeo, and Whitepages today. They rank highest in Google for most names.

10 THE 7-DAY SHIELD PLAN

TEAR THIS *page* OFF. TAPE IT TO YOUR FRIDGE.

Doing everything at once is the reason people don't do it at all. Here is the same guide, spaced over a week. About fifteen minutes a day, mostly while you're already drinking coffee or waiting for a meeting to start.

DAY *one*	**Universal first moves** — reset your ad ID, switch browser default, install uBlock, set 2FA app. PAGE 03	15 MIN
DAY *two*	**Google** — auto-delete activity to 3 months, kill ad personalisation, run Privacy Check-up. PAGE 04	20 MIN
DAY *three*	**Meta** — Off-Facebook Activity wipe + disconnect, ad preferences sweep, Instagram private. PAGES 05–06	25 MIN
DAY *four*	**TikTok & X** — both ad-personalisation off, Refresh For You, opt out of Grok/xAI training. PAGES 07–08	15 MIN
DAY *five*	**Quieter pipes** — Snap, Pinterest, Reddit. Ten minutes each. PAGE 09	20 MIN
DAY *six*	**LinkedIn** — Generative AI opt-out, advertising data sweep, hide your connections. PAGE 10	15 MIN
DAY *seven*	**Data brokers** — pick the top 6 from the list. Free coffee. Set a 6-month recurring calendar reminder. PAGE 11	30 MIN

WHAT YOU GET BACK

Per the experiment: at this level of effort, the *shield* meter sits around **seven of twelve notches**. Monthly extraction drops from ~$254 baseline to roughly **$60–80**. Ads served per day fall by half. Manipulation index — the system's confidence that it can change your behavior with a nudge — drops by about a third. None of this is theoretical. It's just where the buttons are.

A LAST FIELD NOTE

You are not trying to disappear. You are trying to be *worse data*. Worse data → cheaper bids → fewer dollars extracted → quieter feed. You become a less-profitable target, which is the only language the auction speaks. Print this page. Tape it up. Come back next quarter.

COLOPHON · SET IN ARCHIVO BLACK · SPACE GROTESK · JETBRAINS MONO · INSTRUMENT SERIF

END · 12 / 12