

Taking Control of Your Online Privacy

Reduce your digital footprint and protect your personal information

A Complimentary Guide
Version 2.0 | Updated: March 2026

WHAT THIS GUIDE COVERS

This guide helps you shrink your digital footprint and take back control of your personal information online.

You'll learn how to:

- Remove your information from people-finder and data-broker websites.
- Lock down privacy settings on Google, Facebook, Apple, and Amazon.
- Stop unwanted marketing calls, texts, and emails.
- Hide photos of your home from real estate and map sites.
- Protect your physical mail and vehicle data.

Part of the Smart Security Series

Other guides in this security series:

- Protecting Your Identity & Credit
- Securing Your Home Wi-Fi & Devices

Each guide in our Smart Security Series stands alone and addresses a specific area of protection.

WHY YOUR ONLINE PRIVACY MATTERS

Every time you go online, you leave a digital footprint that traces of your activity, locations, purchases, and personal details that companies, advertisers, and even scammers can use [1].

People-finder websites, social media platforms, apps, and big tech companies all collect and share data about you, often behind the scenes [2].

This information can be used for targeted advertising, sold to third parties, or exploited by criminals for scams and identity theft [3].

The Good News

You have more control than you think.

This guide provides practical steps to reduce unwanted exposure, stop annoying marketing, and protect your privacy.

TABLE OF CONTENTS

1	Stop Unwanted Calls, Texts & Emails	
	Who to Contact	5
2	Remove Yourself from People-Finder Websites	
	Directory of Sites	8
3	Protect Your Home Address & Physical Mail	
	Steps to Take	11
4	Lock Down Big Tech Privacy Settings	
	Google, Facebook, etc.	14
5	Clean Up Connected Financial Apps	
	What to Do	17
6	Social Media & AI Privacy	
	Best Practices	19
7	Simple Ongoing Privacy Checkup	
	Monthly, Quarterly, Annually	21
8	Mail Scam Awareness	
	What to Watch For	22
9	Next Steps	23
10	References	25

Stop Unwanted Calls, Texts, & Emails

National Do Not Call Registry

The National Do Not Call Registry blocks most sales calls from legitimate telemarketers [4].

How to enroll:

- **Online:** Visit www.donotcall.gov (requires email confirmation) [4].
- **Phone:** Call 1-888-382-1222 from the number you wish to register with [4].

Coverage: Personal landlines and cell numbers (not business numbers) [4].

Limitations: Does not block political, charity, survey, debt collection, or scam calls. It takes up to 31 days to take full effect [4].

State-level lists: Many states (California, Texas, Oklahoma, North Carolina) maintain their own Do Not Call lists. Check your state attorney general's website for details [5].

Company-Specific Opt-Outs

You can ask individual companies (banks, insurers, retailers) to remove you from their call or marketing lists [6].

How to opt out:

- Look for "Privacy," "Communication Preferences," or "Marketing" in your online account settings.
- Call customer service and request to opt out.
- Submit written opt-out requests for persistent companies.

Stop Unwanted Calls, Texts, & Emails (*continued*)

Email Marketing and Spam Control

1. Unsubscribe Links

- Legitimate marketing emails must include an unsubscribe link and must honor your request within 10 business days [7].
- **Limitation:** Scammers ignore this law, but legitimate businesses follow it [7].

2. DMAchoice (Email and Physical Mail Opt-Out)

- Managed by the Data & Marketing Association, this service lets you opt out of emails and direct mail from DMA members [8].
- dmachoice.thedma.org
- Free for general opt-out; \$2 fee for detailed preferences [8].

3. Unroll.me

- Aggregates email subscriptions and lets you bulk-unsubscribe (free) [9].
- **Note:** This service analyzes your data for ad targeting purposes [9].

4. Report Spam

- Report scam emails to the FTC at reportfraud.ftc.gov [10].

Stop Unwanted Calls, Texts, & Emails (*continued*)

Call and Text Blocking Tools

Robocall Blocking Apps:

- Nomorobo (free for landlines, paid for mobile)
- Hiya
- RoboKiller
- Your carrier's built-in tools:
 - AT&T Call Protect
 - T-Mobile Scam Shield
 - Verizon Call Filter

Caller ID Services

- Enable scam/fraud alerts in your smartphone settings.
- iOS and Android both have built-in scam detection [11].

Remove Yourself from People-Finder Sites

Why Data Broker Removal Matters

People-finder and data broker websites often list your name, home address, phone number, age, relatives, and property records publicly [12].

Here is who uses this information:

- Marketers and advertisers
- Scammers and fraudsters
- Stalkers and harassers
- Identity thieves
- Anyone who searches for your name

The good news: You have the right to request removal of your information from these sites [13].

Free DIY Removal Process

You'll need to visit each site's opt-out page individually and follow its process. Check back every few months, as your information can reappear[14].

See people-finder chart on next page.

Remove Yourself from People-Finder Sites (*continued*)

Major People-Finder Sites	
Spokeo	www.spokeo.com/optout
BeenVerified	www.beenverified.com/f/optout/search
Instant Checkmate	www.instantcheckmate.com/optout/
MyLife	Email privacy@mylife.com with your details and profile URL
Intelius	www.intelius.com/help/how-to-remove-information-from-intelius/ (requires ID)
PeopleSmart	www.peoplesmart.com/optout-go
FamilyTreeNow	www.familytreenow.com/optout
US Phone Book	www.usphonebook.com/removal

Remove Yourself from People-Finder Sites (*continued*)

Tips for Successful Removal

1. Look for "opt-out," "remove listing," or "do not sell my information" links at the bottom of websites [15].
2. Be prepared to provide your name, address, and sometimes proof of identity (redacted driver's license) [15].
3. Keep notes of where and when you submitted requests [15].
4. Set a calendar reminder to recheck these sites every 3 months; your information can reappear [15].
5. Be patient as removal can take 1-2 weeks per site [15].

Outsource It (Optional)

If you want to save time, paid services can handle data broker removal for you:

- **DeleteMe** (Around \$8.71/month): Automatically removes your information from 30+ major data broker sites with quarterly reports [16].
- **Aura** (Around \$10/month): Includes data broker removal plus comprehensive identity protection [17].

Protect Your Home Address & Physical Mail

USPS Informed Delivery

USPS Informed Delivery lets you see digital previews of your mail before it arrives, helping you spot missing or suspicious items [18].

What you get:

- Email notifications with scanned images of letter-sized mail
- Package tracking information
- Alerts if your mail doesn't arrive as expected

Sign up: informedelivery.usps.com/box/pages/intro/start.action

Update Your Address When You Move

Promptly update your address when you move to protect your identity and prevent sensitive mail from going to the wrong location [19].

Update with:

- USPS
- IRS
- Your state tax agency
- Banks and credit card companies
- Employers
- Insurance providers
- Healthcare providers
- Schools

Keeping your address current helps prevent lost mail, identity theft, account takeovers, and fraud related to unauthorized address changes [19].

Protect Your Home Address & Physical Mail *(continued)*

Hide Photos of Your Home Online

Real estate and map websites often display exterior and sometimes interior photos of your home, which can reveal your layout, security systems, vehicles, and daily patterns [20].

Why remove them:

- Reduces information available to burglars
- Protects your privacy from strangers
- Limits data used by scammers to impersonate you
- Reduces unwanted solicitation

Real Estate Website Privacy Removal	
Zillow	Use Owner Dashboard or submit a support request to manage listing visibility
Trulia	Submit a support request to update or hide photos
Instant Checkmate	www.instantcheckmate.com/optout/
Realtor.com	Create an account to control listing visibility
Movoto	Email customercare@movoto.com
PeopleSmart	Email support@homesnap.com

Protect Your Home Address & Physical Mail (*continued*)

Street View Photo Blurring

Google Street View

Request blurring of your home via Google's Street View privacy form [21].

Guide: www.wikihow.com/Opt-Out-of-Google-Street-View

Bing Streetside

Submit a privacy report at www.bing.com/maps/privacyreport [22].

Note: Blurring is permanent. Once applied, you cannot undo it.

Vehicle Data Privacy

Modern cars collect extensive data about you, including everywhere you drive, synced phone contacts, text messages, call logs, browsing history, and driving behavior [23].

Privacy4Cars

Use this free tool to:

1. Learn what data your specific car model collects.
2. Delete synced phone contacts and addresses from your car's infotainment system.
3. Submit data deletion requests directly to car manufacturers.

Website: privacy4cars.com

Assert Your Data Rights: privacy4cars.com/personal-use/assert-your-data-rights/

Lock Down Big Tech Privacy Settings

Why Manage Privacy Settings

Big Tech companies (Google, Meta/Facebook, Apple, Amazon) collect massive amounts of data about your searches, locations, purchases, and behaviors [24]. You can significantly limit this data collection through privacy settings.

Google Account Privacy

Google collects extensive data about what you search, watch, and where you go [25].

Start here:

- **Google Privacy Checkup (recommended first step)**
 - myaccount.google.com/privacycheckup
- **Google Safety Center**
 - safety.google/privacy/privacy-controls

Key Privacy Controls	
Setting	What It Controls
Activity Controls	What Google tracks about your activity
Location History	Your complete location tracking
Auto-Delete	Automatically delete old data after 3, 18, or 36 months
YouTube Privacy	Video watch history and recommendations
Ad Settings	Personalized ads based on your activity
Google Takeout	Download a complete copy of all your Google data

Lock Down Big Tech Privacy Settings (*continued*)

Complete List of Google Privacy Links:

- Activity Controls: myaccount.google.com/activitycontrols
- Dashboard (see all data): myaccount.google.com/dashboard
- Web and App Activity: support.google.com/websearch/answer/54068
- Location History: support.google.com/websearch/answer/3118687
- Auto-Delete: myactivity.google.com/myactivity?restrict=waa
- YouTube Settings: support.google.com/youtube/topic/9257518
- Download Your Data: takeout.google.com/settings/takeout
- Ad Settings: adsettings.google.com/authenticated
- Maps Timeline: support.google.com/maps/answer/6258979

Facebook and Instagram (Meta)

Privacy and security checklist:

- Go to **Settings → Privacy**.
- Change who can see your posts from "Public" to "Friends."
- Turn on **two-step verification** (Settings → Security and Login).
- Review **Apps and Websites** connected to your account.
- Remove apps you no longer use.
- Go to **Settings → Ad Preferences** and turn off unwanted ad topics.
- Check **Off-Facebook Activity** to see what other sites share about you with Meta.
- Review **Settings → Location** and disable location tracking if not needed.

Lock Down Big Tech Privacy Settings (*continued*)

Apple ID and iCloud

Privacy checklist:

- Go to **Settings → [Your Name] → Privacy**.
- Review apps that can access your location, photos, contacts, and camera.
- Turn off location access for apps that don't need it.
- Go to **Settings → Privacy → Tracking** and turn off "Allow Apps to Request to Track."
- Review devices signed into your Apple ID (**Settings → [Your Name] → Devices**).
- Verify **two-factor authentication** is enabled (Settings → [Your Name] → Password & Security).

Amazon Account

Privacy checklist:

- Go to **Account → Privacy Settings**.
- **Manage Alexa Privacy** (if you have Alexa devices).
- Review and delete voice recordings regularly.
- Go to **Account → Advertising Preferences** and opt out of personalized ads if desired.
- Review **Manage Your Content and Devices** to see purchase history and connected devices.

Clean Up Connected Financial Apps

Why Audit Connected Apps

Many budgeting, payment, and shopping apps request broad access to your financial accounts and data [26]. Over time, you may forget which apps are still connected [27].

Security risks:

- Apps you no longer use can be compromised in data breaches.
- Excessive permissions give unnecessary access to your financial data.
- Old apps may share your data with third parties.
- Dormant apps create an unnecessary attack surface.

What to Do

- **In your bank and credit card apps:**
 - Look for "Connected Apps," "Linked Services," or "Third-Party Access" and remove any you no longer use [28].
- **In payment apps (Venmo, PayPal, Cash App):**
 - Review authorized merchants and connected apps. Remove old connections [29].
- **In budgeting tools (Mint, YNAB, Personal Capital, Monarch Money):**
 - Review connected accounts and disconnect any that are no longer needed [30].

Clean Up Connected Financial Apps (*continued*)

Best Practices for Financial App Security

- Only connect apps you trust and actively use [31].
- Share only the minimum data the app needs to function [31].
- Remove apps you haven't used in 6+ months [32].
- Close old app accounts and request data deletion when possible [33].
- Read privacy policies to understand what apps do with your financial data [34].

Review these connections at least quarterly.

Social Media & AI Privacy

Social Media Posting Habits

The photos and posts you share can unintentionally expose personal information, making you and your family more vulnerable to scams or social engineering [35].

Simple protective steps:

- **Clean up old posts** - Remove content that reveals routines, addresses, or frequent locations [36].
- **Limit travel updates** - Avoid posting real-time travel or exact dates when away from home [37].
- **Respect privacy** - Think before posting images of children, coworkers, or friends [38].
- **Watch location data** - Turn off automatic location tagging and review privacy settings regularly [39].

Why this matters:

Digital photos contain location information (GPS coordinates) that bad actors can use to find your home, work, or favorite locations [40]. Social media posts can reveal...

- When you're away from home (vacation posts)
- Your daily routine (gym check-ins, commute patterns)
- Family relationships (tagging relatives)
- Workplace and colleagues
- High-value purchases (new car, jewelry, electronics)

Social Media and AI Privacy (*continued*)

Using AI and Chatbots Safely

AI tools and chatbots can be helpful, but treat them like public spaces on the internet—anything you share might be stored, analyzed, or reused later [41].

Never enter:

- Personal information (SSN, account numbers, passwords).
- Confidential work details.
- Customer data.
- Medical information.
- Financial account details.

Before using any AI tool:

- Review its privacy policy.
- Make sure it's company-approved for work use.
- Understand how it stores and uses your data.
- Remember: If you wouldn't post it publicly, don't share it with a chatbot [42].

Simple Ongoing Privacy Checkup

To keep your online privacy in good shape, set a recurring calendar reminder monthly or quarterly to review these areas [43].

Monthly Tasks

- Review privacy settings on key accounts (Google, Facebook, Apple, Amazon).
- Review and revoke access for apps you no longer use.
- Check for new exposures (home photos, address listings).

Quarterly Tasks

- Recheck major people-finder sites and submit removal requests if needed.
- Review connected financial apps and disconnect unused services.
- Clean up old social media posts.
- Check vehicle data and delete synced information.

Annual Tasks

- Review all major tech platform privacy settings.
- Update opt-out preferences.
- Verify that your Do Not Call registration is still active.

Mail Scam Awareness

Watch Out for Solicitation Scams

Be alert for scams sent through the mail, often disguised as mortgage protection, insurance offers, or official-looking notices [44].

These scams typically:

- Use official-looking letterhead.
- Reference your actual loan or property information.
- Include urgent language or limited-time offers.
- Request you call a specific number.

How criminals get your information:

Bad actors retrieve public records from home loans, home equity lines of credit (HELOCs), and other loans [45].

Best Practices

- **Do NOT call** the number listed in the letter [46].
- **Confirm with your actual lender** or government authority associated with the loan [47].
- **Destroy or securely shred** the letter [48].
- **Monitor your credit** for unusual activity over the next 30-60 days [49].

Next Steps

Start Today

1. Complete Google Privacy Checkup (10 minutes).
2. Register with the National Do Not Call Registry (5 minutes).
3. Review and adjust Facebook/Instagram privacy settings (15 minutes).

This Week

- Begin removing your information from people-finder sites (start with the top 3).
- Set up USPS Informed Delivery.
- Review and disconnect unused financial apps.
- Turn off location tracking on social media.

This Month

- Complete data broker removal for all major sites.
- Request the removal of home photos from real estate sites.
- Request street view blurring (Google and Bing).
- Use Privacy4Cars to delete vehicle data.
- Set up quarterly privacy checkup reminders.

Next Steps (*continued*)

Remember

You don't have to do everything at once. Start with the areas that concern you most and work through the other steps over several weeks.

Privacy is an ongoing process, not a one-time fix. Your information will reappear on some sites, requiring periodic removal requests.

Every action you take reduces your exposure. Even small steps make a meaningful difference in protecting your privacy and reducing scam risks.

Other Guides in this Series

Protecting Your Identity & Credit

Learn how to freeze your credit, respond to fraud, protect your tax information, and monitor your financial accounts effectively. Includes step-by-step instructions for credit freezes and free credit monitoring.

Securing Your Home Wi-Fi & Devices

Protect your home network, smart devices, and personal technology with practical steps like securing your router, using strong passwords, enabling two-factor authentication, and recognizing phishing attempts.

Visit our Customer Security & Privacy page for all guides:

<https://firstoklahomabank.com/fraud-prevention/>

Questions?

Contact First Oklahoma Bank at 918-392-2500.

References

- [1] Privacy Rights Clearinghouse. (2024). Your digital footprint and privacy. <https://privacyrights.org>
- [2] Electronic Frontier Foundation. (2024). Data brokers and consumer privacy. <https://eff.org>
- [3] Federal Trade Commission. (2024). Data brokers: A call for transparency and accountability. <https://ftc.gov>
- [4] Federal Trade Commission. (2024). National Do Not Call Registry. <https://donotcall.gov>
- [5] National Association of Attorneys General. (2024). State Do Not Call programs. <https://naag.org>
- [6] Direct Marketing Association. (2024). DMAchoice opt-out preferences. <https://dmachoice.org>
- [7] Federal Trade Commission. (2024). CAN-SPAM Act compliance. <https://ftc.gov>
- [8] Data & Marketing Association. (2024). DMAchoice service overview. <https://dmachoice.thedma.org>
- [9] Unroll.me. (2024). Email subscription management. <https://unroll.me>
- [10] Federal Trade Commission. (2024). Report fraud online. <https://reportfraud.ftc.gov>
- [11] CTIA. (2024). Robocall and spam protection on smartphones. <https://ctia.org>

References

[12] Privacy Rights Clearinghouse. (2024). People-finder and data broker sites. <https://privacyrights.org>

[13] California Privacy Rights Act. (2024). Consumer data removal rights. <https://oag.ca.gov>

[14] Consumer Reports. (2024). How to remove yourself from people-finder sites. <https://consumerreports.org>

[15] Electronic Frontier Foundation. (2024). Data broker opt-out guide. <https://eff.org>

[16] Abine DeleteMe. (2024). Data broker removal service. <https://joindeleteme.com>

[17] Aura. (2024). Identity theft protection and privacy services. <https://aura.com>

[18] United States Postal Service. (2024). USPS Informed Delivery. <https://informedelivery.usps.com>

[19] Federal Trade Commission. (2024). Change of address and identity theft. <https://identitytheft.gov>

[20] Privacy4Cars. (2024). Home address privacy protection. <https://privacy4cars.com>

[21] Google. (2024). Street View privacy and blurring. <https://support.google.com>

[22] Microsoft. (2024). Bing Maps Streetside privacy. <https://bing.com/maps>

References

- [23] Mozilla Foundation. (2024). Privacy not included: Cars edition. <https://foundation.mozilla.org>
- [24] Electronic Frontier Foundation. (2024). Big Tech data collection practices. <https://eff.org>
- [25] Google. (2024). Privacy and security help center. <https://myaccount.google.com>
- [26] Consumer Financial Protection Bureau. (2024). Third-party app access to financial data. <https://consumerfinance.gov>
- [27] Federal Trade Commission. (2024). Managing app permissions. <https://consumer.ftc.gov>
- [28] American Bankers Association. (2024). Connected apps security guide. <https://aba.com>
- [29] PayPal. (2024). Authorized apps and websites. <https://paypal.com>
- [30] Consumer Reports. (2024). Budgeting app security review. <https://consumerreports.org>
- [31] Federal Trade Commission. (2024). Financial app security tips. <https://consumer.ftc.gov>
- [32] National Cybersecurity Alliance. (2024). App hygiene best practices. <https://staysafeonline.org>
- [33] Privacy Rights Clearinghouse. (2024). Data deletion requests. <https://privacyrights.org>

References

[34] Consumer Financial Protection Bureau. (2024). Understanding app privacy policies. <https://consumerfinance.gov>

[35] Federal Trade Commission. (2024). Social media privacy tips. <https://consumer.ftc.gov>

[36] National Cybersecurity Alliance. (2024). Digital footprint management. <https://staysafeonline.org>

[37] AARP. (2024). Social media safety for seniors. <https://aarp.org>

[38] Common Sense Media. (2024). Social media privacy guide. <https://commonsensemedia.org>

[39] Electronic Frontier Foundation. (2024). Location privacy on social media. <https://eff.org>

[40] Privacy Rights Clearinghouse. (2024). Photo metadata and privacy. <https://privacyrights.org>

[41] National Institute of Standards and Technology. (2024). AI privacy considerations. <https://nist.gov>

[42] Federal Trade Commission. (2024). Using AI chatbots safely. <https://consumer.ftc.gov>

[43] National Cybersecurity Alliance. (2024). Privacy maintenance checklist. <https://staysafeonline.org>

[44] Federal Trade Commission. (2024). Mortgage and loan scams. <https://consumer.ftc.gov>

References

[45] Consumer Financial Protection Bureau. (2024). Public records and privacy. <https://consumerfinance.gov>

[46] AARP. (2024). Mail scam recognition. <https://aarp.org>

[47] Federal Trade Commission. (2024). Verify before you trust. <https://consumer.ftc.gov>

[48] Federal Trade Commission. (2024). Document shredding guide. <https://consumer.ftc.gov>

[49] Federal Trade Commission. (2024). Credit monitoring after fraud attempts. <https://identitytheft.gov>