Wigington Security Group

Privacy consulting for individuals and families

Complete Data Broker Removal Guide

Step-by-step instructions to remove yourself from 100+ data broker sites

What You'll Learn:

- How data brokers collect and sell your information
- State-by-state opt-out rights and laws
- Direct opt-out links for 100+ major data brokers
- Template letters for CCPA/GDPR requests
- Tracking spreadsheet to monitor removal status
- When to use free vs. paid removal services

February 2025 • 24 Pages • Free Download

Contents

1 Why This Matters

1.1 The Data Broker Industry Explained

Data brokers are companies that collect, aggregate, and sell your personal information without your direct knowledge or consent. Unlike social media platforms where you voluntarily create an account, data brokers compile dossiers on you from:

- Public records (property ownership, voter registration, court filings)
- Commercial transactions (loyalty programs, warranty registrations)
- Online activity (browsing history, social media scraping)
- Third-party data purchases from other brokers
- Offline data (magazine subscriptions, charitable donations)

These profiles are then sold to marketers, employers, landlords, insurance companies, private investigators, and anyone else willing to pay.

1.2 What's At Stake

Important

Your data broker profile likely contains:

- Current and past addresses
- Phone numbers (mobile and landline)
- Email addresses
- Age, birth date, and relatives' names
- Property ownership and value
- Estimated income and net worth
- Political affiliation and donor history
- Shopping habits and interests

Real-world consequences:

- **Identity theft:** Criminals use this data to impersonate you
- **Stalking and harassment:** Abusers can locate victims who've relocated
- **Financial discrimination:** Higher insurance rates or loan denials based on profiling
- **Social engineering:** Scammers use accurate details to seem legitimate
- **Employment screening:** Inaccurate or outdated information affecting job prospects
- **Physical security:** Your home address exposed to anyone who pays $20

1.3 Who Should Use This Guide

2 Understanding Your Rights

2.1 State Privacy Laws

Data broker regulation varies dramatically by state. Here's what you need to know:

2.1.1 California (CCPA/CPRA)

California residents have the **strongest privacy rights** in the United States:

- Right to know what personal information is collected
- Right to delete personal information
- Right to opt out of sale of personal information
- Right to correct inaccurate information
- Private right of action for data breaches

Key detail: You do NOT need to provide a reason for deletion requests.

2.1.2 Virginia (VCDPA)

Effective January 1, 2023:

- Right to access, delete, and correct data
- Right to opt out of sale and targeted advertising
- Does NOT include private right of action (only AG enforcement)

2.1.3 Colorado (CPA)

Similar to Virginia, effective July 1, 2023:

- Covers businesses processing data of 100,000+ Colorado residents
- Right to opt out of profiling

2.1.4 Connecticut, Utah, Montana, Oregon, Texas

Each has passed comprehensive privacy laws with varying effective dates and provisions. All include deletion rights for residents.

2.1.5 Vermont Data Broker Registration

Vermont requires data brokers to **register with the state**. The public registry at https://ago.vermont.gov/ lists registered brokers—a helpful starting point for identifying companies.

2.2 Federal Rights (Limited)

The United States has no comprehensive federal privacy law. However:

- **Fair Credit Reporting Act (FCRA):** Regulates "consumer reporting agencies" but most data brokers operate outside this definition
- **Telephone Consumer Protection Act (TCPA):** Allows you to sue for unsolicited calls
- **CAN-SPAM Act:** Provides email opt-out rights

Pro Tip

Even if you don't live in a state with privacy laws, **data brokers often comply with opt-out requests anyway** because:

1. It's cheaper than verifying your residency
2. They face reputational risk for refusing
3. Many are preparing for federal legislation

3 The Removal Process: Overview

3.1 How Long This Takes

Be realistic about the time commitment:

- **Initial removal wave:** 10-15 hours over 2-3 weeks
- **Verification and follow-ups:** 5-8 hours over next 4-6 weeks
- **Ongoing maintenance:** 1-2 hours quarterly

Why it takes time: Each broker has different opt-out procedures, verification requirements, and response times. Some respond in 48 hours; others take 30+ days.

3.2 The Four-Phase Approach

1. **Discovery:** Identify which brokers have your information
2. **Documentation:** Prepare your opt-out requests and verification documents
3. **Submission:** Submit requests through each broker's specific process
4. **Verification:** Confirm removal and address rejections

3.3 Tools You'll Need

Checklist

Before starting, gather:

- Dedicated email address (create a new one for privacy requests)
- Phone number (Google Voice recommended for verification calls)
- Spreadsheet for tracking (template provided in Section 7)
- Government-issued ID (for some verification processes)
- Proof of address (utility bill for some requests)
- Password manager to track accounts created during opt-outs

Pro Tip

Privacy paradox: Some brokers require you to create an account and upload ID to remove your information. This is frustrating but legal. Use your dedicated privacy email and delete the account after confirmation.

3.4 Free vs. Paid Services

DIY (This guide): $0, requires 15-25 hours total time
Paid removal services ($100-$200/year):

- DeleteMe, Privacy Bee, Incogni, Optery
- Pros: Ongoing monitoring and re-removal, saves time
- Cons: Subscription model, may not cover all brokers, less control

Professional services ($500-$2,000):

- Privacy consultants (like WigSec) handle entire process
- Pros: Comprehensive, handles difficult cases, includes strategy
- Cons: Higher upfront cost

Our recommendation: Start DIY with this guide. If you get stuck on specific brokers or want ongoing maintenance, consider paid services for the subset you haven't completed.

4 Phase 1: Discovery

4.1 Find Yourself Before Removing

You need to know what's out there before you can remove it. This phase typically takes 2-4 hours.

4.1.1 Manual Search Strategy

Start with these searches using your real name:

1. Google: `"Firstname Lastname" city state`
2. Google: `"Firstname Lastname" phone number`
3. Google: `"Firstname Lastname" age`
4. Bing (different index than Google)
5. DuckDuckGo (for sites that block Google crawlers)

Important

Use a VPN or Tor for these searches. Some data brokers track who's searching for specific names and may prioritize keeping that data "fresh."

4.1.2 Major Data Broker Categories

People Search Sites (Primary Targets):

- Whitepages, TruePeopleSearch, FastPeopleSearch
- Spokeo, BeenVerified, Instant Checkmate
- Intelius, PeopleFinders, USSearch
- MyLife, Radaris, TruthFinder

Public Records Aggregators:

- PublicRecordsNow, FamilyTreeNow
- NeighborWho, AddressSearch
- VoterRecords.com

Background Check Services:

- CheckPeople, PeopleLooker
- PublicDataUSA, IDTrue

Marketing Data Brokers (Harder to Access Directly):

- Acxiom, Epsilon, Experian Marketing
- Oracle Data Cloud (BlueKai)
- These typically don't have consumer-facing sites; opt-outs are via dedicated privacy portals

4.1.3 Document Your Findings

For each site where you find your information, record:

- Site name and URL of your profile
- What information is displayed (addresses, phone, relatives, etc.)
- Whether the site requires account creation for opt-out
- Date discovered

Use the tracking spreadsheet in Section 7.

5 Phase 2: Documentation

5.1 Create Dedicated Privacy Email

Do NOT use your primary email for opt-out requests. Create a new email specifically for privacy activities:

- Gmail/Proton: `yourname.privacy@gmail.com`
- Use this ONLY for data broker communications
- Set up filtering to organize responses

Why? This email will receive confirmations, verification links, and unfortunately, spam. Keeping it separate protects your primary inbox.

5.2 Prepare Template Letters

Most data brokers accept opt-outs via web forms, but some require email or postal mail. Here are templates:

5.2.1 CCPA Deletion Request (California Residents)

```
Subject: California Consumer Privacy Act (CCPA) Deletion Request

To Whom It May Concern:

I am a California resident exercising my right to deletion
under the California Consumer Privacy Act (CCPA), Cal. Civ.
Code § 1798.105.

I request that you delete all personal information you have
collected about me, including but not limited to:

Name: [Your Full Name]
Current Address: [Address]
Previous Addresses: [List if known to be in their system]
Phone Numbers: [List all]
Email Addresses: [List all]

Please confirm completion of this deletion request within
45 days as required by CCPA.

If you require additional information to verify this request,
please contact me at [privacy email].

Sincerely,
[Your Name]
[Date]
```

5.2.2 General Opt-Out Request (All States)

```
Subject: Data Removal Request

To Whom It May Concern:

I am requesting removal of all personal information associated
with me from your databases and public-facing directories.

Name: [Your Full Name]
Address: [Current Address]
Phone: [Phone Number]
Date of Birth: [DOB if required for verification]

Please confirm when this removal has been completed and
provide confirmation to this email address.

If you require additional verification, please let me know
what information you need.

Thank you,
[Your Name]
[Date]
```

5.3 Prepare Verification Documents

Some brokers require identity verification. Have these ready:

Checklist

- Scan/photo of driver's license or state ID
- Recent utility bill showing name and address
- Redact unnecessary info (license number, account numbers)
- Save as PDFs: `ID_verification.pdf`, `address_proof.pdf`

Important

Only upload verification documents through HTTPS sites. If a broker requests documents via unencrypted email, push back and request a secure portal.

6 Phase 3: Submission (The Big 100)

This section provides direct opt-out links and instructions for 100+ major data brokers. Work through these systematically.

6.1 Tier 1: High-Priority People Search Sites

These sites have the most detailed information and are most commonly searched. Start here.

6.1.1 Whitepages

URL: https://www.whitepages.com/suppression-requests

Process:

1. Search for yourself at whitepages.com
2. Copy the URL of your listing
3. Go to suppression request page
4. Enter listing URL, phone, and email
5. Verify via email link (check spam folder)
6. Wait 24-48 hours for removal

Notes: Whitepages owns several other brands. After removal, check these owned properties:

- 411.com
- Addresses.com
- AllPeople.com

6.1.2 Spokeo

URL: https://www.spokeo.com/optout

Process:

1. Search for yourself at spokeo.com
2. Note your profile URL (includes ID number)
3. Visit opt-out page
4. Enter your listing URL and email
5. Verify via phone call OR email confirmation
6. Wait 72 hours for removal

Difficulty: Medium (phone verification is annoying but quick)

6.1.3 BeenVerified

URL: https://www.beenverified.com/app/optout/search
Process:

1. Find your listing on BeenVerified
2. Click "Opt Out" at bottom of the page
3. Enter your information
4. Verify via email
5. Wait 24 hours

Notes: Also check NumberGuru and NeighborWho (owned by BeenVerified).

6.1.4 Intelius

URL: https://suppression.peopleconnect.us/login
Process:

1. Requires account creation (frustrating but necessary)
2. Search for yourself within the suppression portal
3. Select all records to suppress
4. Wait 72 hours for removal

Notes: Intelius owns PeopleLookup, PublicRecordsNow, iSearch, DateCheck, and others. Your suppression request should cover all properties.

6.1.5 Instant Checkmate

URL: https://www.instantcheckmate.com/opt-out/
Process:

1. Find your record at instantcheckmate.com
2. Fill out opt-out form with record URL
3. Verify via email
4. Wait 48 hours

Also check: TruthFinder (same parent company)

6.1.6 TruePeopleSearch

URL: https://www.truepeoplesearch.com/removal

Process:

1. Search for yourself
2. Click "record details" on your listing
3. Scroll to bottom and click "remove this record"
4. Confirm your email
5. Removal is typically instant

Notes: One of the easiest opt-outs. Also covers FastPeopleSearch.

6.1.7 MyLife

URL: https://www.mylife.com/privacy-policy

Process:

1. Find your MyLife profile
2. Scroll to "Control Your Information"
3. Click "Remove my information"
4. Requires phone verification (they call you)
5. Wait 48 hours

Difficulty: High (phone verification, persistent re-listing)

Important

MyLife is notorious for re-adding information after several months. Set a calendar reminder to check quarterly.

6.1.8 Radaris

URL: https://radaris.com/page/how-to-remove

Process:

1. Find your profile
2. Click "Control Information" at bottom
3. Enter email and verify
4. Wait 72 hours

6.2 Tier 2: Background Check and Public Records Sites

These sites focus on aggregating court records, property records, and other public filings.

6.2.1 FamilyTreeNow

URL: https://www.familytreenow.com/optout
Process:

1. Search for yourself
2. Click "Opt Out" on your record
3. Enter information
4. Verify via email
5. Instant removal

Notes: Easy process, but they scrape public genealogy sites so you may reappear. Check quarterly.

6.2.2 PeopleFinders

URL: https://www.peoplefinders.com/opt-out
Process:

1. Requires creating account
2. Verify email and phone
3. Select records to remove
4. Wait 48 hours

6.2.3 CheckPeople

URL: https://www.checkpeople.com/do-not-sell
Process:

1. Find your listing
2. Click "Opt Out" at bottom of page
3. Enter info and verify email
4. Wait 72 hours

6.3 Tier 3: Marketing Data Brokers

These don't have consumer-facing sites but aggregate data for marketing. Opt-outs are via privacy portals.

6.3.1 Acxiom

URL: https://isapps.acxiom.com/optout/optout.aspx

Process:

1. Fill out opt-out form with name, address, email
2. No verification required
3. Wait 6-8 weeks (slow but comprehensive)

Impact: High—Acxiom supplies data to many other brokers.

6.3.2 Epsilon (CCPA Portal)

URL: https://www.epsilon.com/privacy/consumer-request

Process:

1. Submit CCPA-style request
2. Provide email and address
3. Wait 4-6 weeks for confirmation

6.3.3 Oracle Data Cloud (BlueKai)

URL: https://datacloudoptout.oracle.com

Process:

1. Browser-based opt-out (sets cookies)
2. Must repeat per browser/device
3. Instant but limited scope

Limitation: This only opts you out of targeted advertising, not data collection.

6.4 Full List of 100+ Data Brokers with Opt-Out Links

[Due to length constraints, the full table with 100+ brokers would go here in the actual PDF. The table would include: Broker Name — Opt-Out URL — Process Difficulty — Notes — Estimated Time]

Table format:

Broker	Opt-Out URL	Difficulty	Time
AdvancedBackgroundChecks	advancedbackgroundchecks.com/removal	Easy	10 min
Addresses.com	whitepages.com/suppression-requests	Easy	15 min
...continues for 100+ entries...			

Pro Tip

Download the complete spreadsheet version at:
https://wigingtonsecurity.com/resources/data-broker-list

7 Phase 4: Verification and Maintenance

7.1 Confirming Removal

Wait the specified time period (24 hours to 6 weeks depending on broker), then:

Checklist

- Search for yourself again on the broker's site
- Check if your profile still appears in Google search results (may take longer to de-index)
- Save confirmation emails in dedicated folder
- Update your tracking spreadsheet

7.2 Handling Rejections

Some brokers will reject your request. Common reasons and solutions:

"We need additional verification"

- Solution: Provide government ID and utility bill
- Only do this for legitimate brokers with HTTPS portals

"This information is from public records"

- Solution: Reference your state's privacy law (if applicable)
- Escalate: File complaint with state AG's office

"We don't have a record matching your information"

- Solution: Try alternate name formats (middle name, maiden name)
- Provide specific URL of your listing

"You must create an account to opt out"

- Solution: Bite the bullet and create it
- Use dedicated privacy email and password manager
- Delete account after confirmation (if possible)

7.3 Quarterly Maintenance Schedule

Data brokers re-aggregate information from public sources. Set calendar reminders:

Every 3 months:

1. Google yourself again
2. Check top 20 brokers from your initial removal
3. Re-submit opt-outs for any re-listings

4. Update tracking spreadsheet

Time required: 1-2 hours quarterly once initial removal is complete.

Pro Tip

Consider setting up a Google Alert for your name. When you get an alert, investigate whether it's a new data broker listing.

8 Tracking Spreadsheet Template

Create a spreadsheet with these columns:

Broker Name	Date Found	Opt-Out URL	Method	Date Submitted	Date Confirmed	Status
Whitepages	2/1/25	whitepages.com/suppression	Web form	2/1/25	2/3/25	Complete
Spokeo	2/1/25	spokeo.com/optout	Email verify	2/2/25	2/5/25	Complete
MyLife	2/1/25	mylife.com/privacy	Phone	2/2/25	Pending	Waiting

Status codes:

- Waiting for response
- Confirmed removed
- Rejected (with notes on why)
- Re-check needed (quarterly maintenance)

Download the template:
https://wigingtonsecurity.com/downloads/data-broker-tracking-template.xlsx

9 Special Situations

9.1 If You're a Victim of Stalking or Domestic Violence

Important

If you are fleeing an abusive situation, data broker removal is critical but may not be sufficient. Additional steps:

- Contact your state's Address Confidentiality Program (ACP) if available
- File for Safe at Home or similar protective address programs
- Work with victim services organizations for comprehensive safety planning
- Consider professional privacy consulting (WigSec offers pro bono assistance in DV cases)

Resources:

- National Domestic Violence Hotline: 1-800-799-7233
- Clinic to End Tech Abuse: https://www.ceta.tech.cornell.edu

9.2 Removing Information About Minors

Children's data on people search sites often comes from:

- Public records (birth records, property records listing household members)
- Scraped social media (parent posts)
- School directories

Removal approach:

1. Most brokers will prioritize removal of minors' data—mention age in request
2. Reference COPPA (Children's Online Privacy Protection Act) for children under 13
3. For California residents, reference CCPA provisions protecting minors
4. Consider using DeleteMe or similar service (they specialize in minor removals)

9.3 Law Enforcement and Public Officials

Many states have laws protecting LEO addresses from public disclosure, but data brokers often don't comply.

Enhanced approach:

1. Reference your state's LEO protection statute in opt-out requests
2. Provide badge number/ID as verification
3. Escalate non-compliance to your department's legal counsel
4. Consider professional removal service with LEO expertise

States with strong LEO protection laws: California, Florida, New York, Texas, Colorado, Arizona

9.4 Real Estate Professionals and Business Owners

You may want your business information visible but personal information private.

Strategy:

- Request removal of home address while keeping business address visible
- Use LLC or corporate structure to separate personal/business identity
- Consider registered agent service for business filings
- Establish professional website as the "authoritative" source for business info

10 Beyond Data Brokers: Comprehensive Privacy

Removing yourself from data brokers is just one piece of digital privacy. For comprehensive protection:

10.1 Public Records

Data brokers aggregate from public sources. Consider:

- Using business entity (LLC) for property ownership
- Opting out of voter registration public access (varies by state)
- Requesting anonymization of court records where permitted
- Using PO Box or PMB instead of home address for public filings

10.2 Social Media Privacy Lockdown

Review privacy settings on:

- Facebook, Instagram, Twitter/X
- LinkedIn (consider removing address/location)
- TikTok, Snapchat
- Venmo (make transactions private!)

Download our guide: *Social Media Privacy Configuration* (32 pages, free)

10.3 Ongoing Digital Hygiene

☑ Checklist

- Use unique passwords for every account (password manager)
- Enable 2FA everywhere possible
- Review app permissions quarterly
- Use email aliases (SimpleLogin, AnonAddy)
- VPN for sensitive activities
- Freeze credit with all three bureaus
- Monitor for breaches (Have I Been Pwned)

11 When to Hire Professional Help

11.1 DIY is Great For:

- General privacy improvement
- Learning how data brokers work
- Budget-conscious approach
- You have 20+ hours to invest

11.2 Consider Professional Services If:

- You're in a high-risk situation (stalking, harassment, threats)
- Your information is on 50+ sites and you don't have time
- You've tried DIY and got stuck on rejections
- You want ongoing monitoring and re-removal
- Your profession requires enhanced privacy (LEO, executive, etc.)

11.3 What WigSec Offers

Personal Exposure Assessment ($100):

- Comprehensive scan of 200+ data brokers and public records
- Detailed report of what's exposed
- Prioritized remediation plan
- Self-service implementation guidance

Complete Privacy Cleanup ($500):

- We handle all opt-out requests
- Verification and follow-ups
- Quarterly maintenance for 1 year
- Additional public records strategy
- NDA provided

Book at: https://wigingtonsecurity.com/services

12 Conclusion

Data broker removal is not a one-time task—it's an ongoing practice. But the initial heavy lifting (10-20 hours) dramatically reduces your exposure, and quarterly maintenance (1-2 hours) keeps you off the radar.

12.1 Key Takeaways

1. **Start with Tier 1 brokers:** These have the most detailed info and are most commonly searched
2. **Document everything:** Use the tracking spreadsheet religiously
3. **Be persistent:** Some brokers are difficult on purpose—don't give up
4. **Maintain quarterly:** Data re-aggregates; plan for ongoing effort
5. **Layer your privacy:** Combine data broker removal with other privacy practices

12.2 Additional Resources

Free WigSec Guides:

- Breach Response Playbook
- Social Media Privacy Configuration
- Password Manager Setup Guide
- Device Hardening Checklist

Download all at: https://wigingtonsecurity.com/guides
Recommended Reading:

- *Extreme Privacy* by Michael Bazzell
- *The Art of Invisibility* by Kevin Mitnick

Check for breaches:

- Have I Been Pwned: https://haveibeenpwned.com
- WigSec's breach checker: https://wigingtonsecurity.com/tools/breach-check

☑ Checklist

Questions or Need Help?

We're here to support your privacy journey.
Contact: https://wigingtonsecurity.com/contact
Schedule Assessment:
https://wigingtonsecurity.com/services

Privacy is a right, not a luxury.

Document Version 1.0 • February 2025

https://wigingtonsecurity.com