Big Ass Data Broker Opt-Out List

<u>,≯now mirrored on GitHub‼</u>,≯

= crucial
= high priority
= requires driver's license (cross out your ID #!)
= must pick up a (gasp!) phone
= must go back in time and find a fax machine
= must use snail mail
= site charges money for access or removal (whaaaat?)

*This list, also known as BADBOOL, was started in September 2017 and was most recently updated on October 12, 2024 to update Clustrmaps since it no longer requires a physical address, added a form for Ancestry.com, and to add the genealogy site FamilySearch. We also clarified the options for opting out of Nuwber.

How to use this page: We recommend opting out of high-priority sites first. If you only have the time and patience for 14, start with sites marked \swarrow . If you can do 22, go to sites marked \Re . Once you've completed all of those, you can start to work your way through the rest of the list.

Please send corrections or updates to <u>yael@yaelwrites.com</u> using the subject line "BADBOOL," or file pull requests on GitHub. (You can find other ways to reach me <u>on the contact page on my website</u>.) Screenshots in emails are incredibly helpful. I add opt-out info only if users can verify that the data broker has their information before sharing additional data, and where removal is not limited to local laws like GDPR, CCPA, etc.

Disclaimers: Some of these opt-outs take a long time to go through. Sometimes, information is pulled from other sources and you'll need to opt out multiple times for the same site. Data brokers come and go (and are bought out by others), and they also often change their opt-out pages. I update this regularly, but it's not always current. There are sites I either don't know about or do not include because there is no free way to see if they have data before requesting removal, or to provide the specific URLs needed for removal. Finally, even opting out of these sites doesn't mean that your address is secure. In many states, real estate data and voter registration information is public (or easy to obtain). And, of course, location data can be found by physical means (e.g., following you home) and through other people who know it (i.e., social engineering). That said, removing your home address from data broker sites can significantly lower your attack surface and make it harder for people to find it.

<u>CC BY-NC-SA</u>: This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format for noncommercial purposes only, and only so long as attribution is given to the creator. If you remix, adapt, or build upon the material, you must license the modified material under identical terms.

Search Engines

If you've been doxed, you can remove your contact info <u>from Google</u> <u>Search</u> and <u>from Bing</u>.

Google also allows you to remove non-consensual or intimate personal images, involuntary fake pornography, irrelevant pornography from Google search results for your name, content about you on sites with exploitative removal practices, and several other categories of information.

Google has a free service called <u>Results About You</u>, that allows you to search for your data and ask for it to be deindexed.

People Search Sites:

Acxiom: It is hard to find your own info for free, but people in some countries can opt out using the following links: Portail des droits des consommateurs | Acxiom (France) Portale delle preferenze dei consumatori | Acxiom (Italy) Portal de preferencia del consumidor | Acxiom (Spain) US Consumer Opt Out | Acxiom (U.S.)

Users in Austria, Germany, India and Switzerland may email <u>Datenschutz@acxiom.com</u>.

Other international requests should go to the <u>Acxiom Consumer</u> <u>International Rights Portal</u>.

If you don't have an email address, call (877) 774-2094 and follow the prompts.

AdvancedBackgroundChecks: First, <u>search for your information</u>. Remember that you can leave your city, state, and age blank. If your information shows up, <u>remove your data</u>.

Ancestry.com: While you can't see all of your data without a paid account, Ancestry will delete information if you email links that would redirect you to the proper site if you had an account. Sign up for a free account (not a free trial!), and then search for your information on the sidebar. Click on everything that includes a state you have ever lived at, even if it's not your current state. Cut and paste the URLs, even if they all direct to a sales page, and email them to privacy@ancestry.com. Alternatively, you can submit individual URLs via this content removal form.

Archives: To find your information, you must <u>sign up for a free trial</u> (and then cancel). Then, <u>opt out</u> if you found your data.

BackgroundAlert: <u>Find your information</u> and opt out.

BeenVerified: Find your information and opt out of <u>people search</u> and <u>property search</u>. BeenVerified also owns PeopleLooker and PeopleSmart. Be aware that BeenVerified only allows one opt-out per email address, so you may need to reach out via email for additional opt-outs. You will need to confirm your opt-out request by clicking on a link sent to you via email.

CheckPeople: Look for your contact info. If it shows up, select "remove record." You will need to fill out your name and email and solve a captcha. You will receive an email which will require you to confirm your opt-out request.

Classmates.com: Cancel your free or paid membership following <u>these</u> <u>instructions</u>.

Solution Clustrmaps: Find your information, and then remove it. It will ask you to check off anything associated with your account that you want removed.

CocoFinder: <u>Look for your information</u> and then <u>opt out</u>. You will be sent to a <u>Google form</u>.

Cyber Background Checks: Look for your information and opt out.

Dataveria: Find your information. Opt out by entering the specific profile URL you find into the <u>opt-out form</u>. You will need to confirm your opt-out request by clicking on a link sent to you via email.

Facecheck: Facecheck.id is reverse image search software that uses an uploaded image to locate your face across in photos and videos on major social media platforms. If this type of search is something you are concerned about, you can remove your face from its search engine by searching for your image, uploading a driver's license or ID card (you can hide your name, address and ID number) or a selfie with your face and two fingers touching your chin. Note that this will not remove your image from the various websites on which it was found, but simply will not allow people to search for it on the Facecheck site. Facecheck also states that it makes an exception for violent criminals.

FamilySearch

<u>Sign up for a free account</u> and <u>search historical records</u>. Copy the URLs for the records with your information, and <u>submit this opt-out form</u>. You will need to verify your email address.

FamilyTreeNow: Search for yourself and <u>remove your information</u>.

FastPeopleSearch.com: Look for and <u>remove your information</u>. You may need to solve a captcha.

FreePeopleDirectory: <u>Search for your information</u>. If you find it, you can opt out on <u>Spokeo's opt-out page</u>. Make sure to scroll down to the grammatically incorrect "opt out your information" section.

Solution and the follow the instructions to remove your data. You can remove your information without downloading your free report, and email support@gladiknow.com for assistance.

HudwayGlass: Look for your home address. If your name is listed alongside your address, click on the "information control" link. Opt out of

applicable phone numbers and names. There's a limit per each opt out and each email you use to opt out. You will need to click the verification link they email you to finalize the opt out.

IDTrue: Find your information and <u>opt out</u>.

InfoTracer: Find your information and opt out by filling out the form. You can also mail in <u>a different form or</u> fax it to 1-617-933-9946.

Support@mailer.intelius.com, calling 1-888-245-1655, or filling out a form. If you're told that Intelius can't find your account, you may need to confirm your mailing address, phone number, old email addresses, or other information via email. (As always, make sure Intelius already has the information before providing it.) Intelius owns Addresses.com, Addresssearch.com, Anywho, Classmates, DateCheck, Instant Checkmate, InstantPeopleFinder, iSearch, LookUpAnyone, Peopleconnect.us, PeopleFinder, PeopleLookup, Phonesbook, Publicrecords, Spock, Truthfinder, US Search, and Zabasearch.

Set Set MyLife: Find your information, and then opt out. Although this is CCPA-focused, non-California folks have successfully removed their profiles. However, another option is to email your removal request to privacy@mylife.com with your name and a link to your profile. MyLife will try to get you to create an account with a copy of your driver's license to submit a profile removal request, and we've received reports that emailing the info@mylife.com or removalrequests@mylife.com email addresses will require a phone call to (888) 704-1900. Previously, calling that number and pressing 2 allowed you to be removed from MyLife (and Wink.com) after providing your name, age, date of birth, email address, current mailing address, and a previous mailing address, but this no longer appears to be the case. (It also appears that you can sign up for a free membership to

remove your reputation profile, though not your personal information such as your home address.)

NeighborReport: <u>Search for your name, address or phone number</u>, and then <u>remove the report</u>. You will need to verify the opt-out request via email.

Nuwber: Find your information. Try to opt out on the removal form. If the URL you generate doesn't work in the form or you run across other problems take a screenshot of your results and send them to <u>support@nuwber.com</u>, asking them to opt you out.

ReekYou: Look for your information and opt out. You will need the letters at the end of your profile's URL in the "unique ID" field. Make sure to check "remove my entire listing." You can also remove your information from the sites that it says it has aggregated information from.

PeopleByName: Look up your name or fill in your name in the URL like this: <u>https://www.peoplebyname.com/people/[Last_Name]/[First_Name]</u> Opt out <u>for each record</u>.

PeopleFinders: Find your information and then opt out. (PeopleFinders includes Advanced People Search). The opt-out link also includes information on finding your profile, after you hit next. You will need to confirm your opt-out request by clicking on a link sent to you via email.

PeopleSearchNow: Find your information and opt out.

PimEyes: PimEyes is an online face search engine that uses face recognition to perform a reverse image search, finding pictures of your face (or others like it) throughout the Internet. If you want to see if your

photographs are in PimEyes' database, consider <u>uploading a photo</u>. (I used a very public photo that I know is already online, but you can also take a photo with your camera—which PimEyes claims it does not store.) To opt out, you'll need to upload an image of your face on the <u>opt-out</u> request form, and also attach a photo ID with all sensitive data (other than your name and photograph) blurred. The easiest way to do this, in my opinion, is through Signal, the encrypted messaging app, which has a blur feature described <u>in its blog</u>. You can also use tools such as Photoshop or even make a copy of your ID and use a Sharpie. Finally, you'll need to provide your email address.

Pipl: Find your information. Then, opt out. After that, remove your information from any sites it's aggregated from. You can also email support at support@pipl.com.

PrivateRecords: Search for your name and state and opt out.

PropertyRecs: Search for your name and state in the <u>opt-out page</u>, then opt out if needed.

PublicDataUSA: Find your information. Copy the URL with your results and enter it along with your name and email address on the <u>opt-out</u> page.

Radaris: Find your information. Click on "control information" and "remove information" by clicking on the X next to it or by removing specific listings. You can also privatize your account. You unfortunately need to register to remove information, and are limited to removing six items at a time. (I recommend removing items even if you privatize your account because these settings don't always stick.) See Radaris' removal details. You will need to confirm your opt-out request by clicking on a link sent to you via email.

Rehold: Look up your home address. If there is a number or name next to it you'd like removed, click on the red "remove" button next to it. You will need to enter your name and email address and solve a captcha.

Searchbug: Unfortunately, you have to sign up with a credit card to <u>search for your information</u>, though your first search is free. You can contact Searchbug using the <u>contact form or chat link</u> or via phone or text at (760) 454-7301 or via fax at (760) 454-7341 to ask them to block the display of your personal information.

SearchPeopleFree: <u>Find your information</u>, making sure to search by name, phone number, address and email address. Then, <u>opt out</u>.

SearchQuarry: <u>Find your information</u>. If it's listed, <u>opt out</u>. You will need to click the verification link in your inbox to finalize the opt out.

SmartBackground Checks: Find your information and opt out.

Social Catfish: Find your information. Record the URL of each page that has your information. Then, go to <u>the opt-out page</u> and scroll down to the instructions for removing URLs, email, phone number, and address. (Make sure to only ask for information to be removed if you already see it on the site.) You'll need to provide your email address and click on a confirmation link to complete the opt-out process.

Spokeo: Find your information. Remove it by entering the URL of the profile you want removed and your email address on the <u>opt-out page</u>. Make sure to scroll down to the grammatically incorrect "opt out your information" section. You will need to confirm your opt-out request by clicking on a link sent to you via email.

SpyFly: Look for your data and then <u>opt out</u>. You can also try emailing support@spyfly.com. You'll need to provide your name, age, address, and email address. Make sure SpyFly has information you'd like removed before volunteering these things.

That's Them: Find your information and then <u>opt out</u>. Do not click on the Spokeo identity theft protection link, as it is an ad for a paid product.

TruePeopleSearch: Follow the <u>removal instructions</u>. You will need to enter your name, city and state, and email address, and then you'll need to solve several captchas to see if you are listed, after which you can remove your information.

United States Phone Book: <u>Search for your information</u>. If your address is listed and you want it removed, enter the telephone number and zip code listed on the above site into the <u>removal form</u>.

USA-Official: After finding your information, enter your name and URL.

USA People Search: Find and remove your information.

Section 2018 Secti

Verecor: Find your information. To opt out, enter the profile URL (along with your name and email) on the <u>opt-out page</u>. You will need to fill out a captcha, and confirm the email link to finalize your request. If it doesn't go through, you may need to email <u>assist@verecor.com</u>. If you opt-out of Verecor and try to out-out of Vericora (or the reverse), you will get an error stating: "You have exceeded the maximum number of requests per person." It's not clear if either site respects an opt-out on the other, so use a separate browser session and email to opt-out of each.

Vericora: Find your information and then opt out. Note that if you opt-out of Verecor and try to out-out of Vericora (or the reverse), you will get an error stating: "You have exceeded the maximum number of requests per person." It's not clear if either site respects an opt-out on the other, so use a separate browser session and email to opt-out of each.

Veripages: Find your information. To opt out, copy and paste the specific URL you found along with your name and email address on the <u>opt-out</u> <u>page</u>.

VoterRecords: Go to <u>VoterRecords.com</u>, find your information, scroll to the bottom of the page and click on the "record opt-out" link. This will lead to an opt-out form, which you'll need to submit. You may receive a verification link you'll need to click on to verify your opt-out request.

Sometimes, information is removed from White Pages but not White Pages Premium, so make sure to double-check for your listing. Unfortunately, it may not be possible to opt out of White Pages also owns <u>411.com</u>, so check for your information there. The U.S. Retailers opt-out is the same. You may need to verify your opt-out by receiving an automated voice call and entering a four-digit code into your phone.

ZoomInfo: Opt out if the company has an email on record—it will email you a code. ZoomInfo appears to have moved towards focusing primarily on business rather than individuals.

Special Circumstances

If you're a **victim of violent crime or identity theft**, it's often possible to opt out of information that others can't opt out of. You may, however, need to provide court orders or other information. It may be worth checking <u>more complete data broker lists</u>.

If you are **experiencing or have experienced domestic violence, sexual abuse, or stalking**, you may be able to keep your address private through state programs that provide a substitute address and mail forwarding. To see if a program exists in your state, look up "address confidentiality program" along with the name of your state in a search engine.

If you are a **healthcare worker with a National Provider Index (NPI) number**, your personal cell phone number or home address may be showing up on various online directories and websites because they were listed as primary contact information when you filled out your NPI profile (or when someone else filled it out on your behalf). CMS now provides the option of using a post office box instead of a home address if you do not have a physical practice address. Look up your information. You can update or remove information by filling out a form. You'll also need to reach out to any sites aggregating this data, like Doximity, where you may be able to <u>edit</u> or <u>delete</u> your profile.

Preventing Identity Theft & Opting Out of Marketing Sites

Consider freezing your credit, which prevents creditors from accessing your credit report. (It also prevents credit, loans, and services from being approved in your name. You can receive a pin to unfreeze your credit, if needed. Note that you will need to do so in order to conduct business with entities requiring access to this information.)

To freeze your credit, you will need to provide personal information such as your name, address, date of birth, and social security number. While you can sometimes initiate this online, it's better to do it by phone. Fees for freezing your credit <u>vary by state</u>.

To freeze your credit, contact:

- Equifax: 1 (800) 349-9960, Freeze or Unfreeze Your Credit
- Experian: 1 (888) 397-3742, <u>Freeze or Unfreeze Your Credit</u> <u>File for Free</u>.
- TransUnion: 1 (888) 909-8872, <u>Freeze My Credit</u> or the form page.
- Innovis: 1 (800) 540-2505, <u>Add or Manage a Security Freeze</u> or <u>Security Freeze Request Online</u>.
- ChexSystems: 1 (800) 428-9623, <u>Place a ChexSystems</u>
 <u>Security Freeze.</u> This will prevent approval of accounts, loans, and services being approved in your name without your consent.

Explore any privacy options offered by your state's motor vehicle department.

Contact your home and mobile phone companies to see if they offer privacy options, such as not listing your number on caller ID or allowing you to opt out of sales of phone numbers.

Consider opting out of direct marketing and telemarketing. Griffin Boyce has <u>compiled a list</u> with a lot of information on doing so. It was last updated in 2019.

You can also opt out of targeted ads using cookies and similar technology at the browser.

Opt out of prescreened credit offers.

Get on the <u>Do Not Call Registry</u>.

Paid Opt-Out Services

While there are over a dozen different data broker opt-out services, I personally use and recommend <u>EasyOptOuts</u>. For more information on people search site removal services, <u>see the evaluation I conducted at</u> <u>Consumer Reports in partnership with Tall Poppy</u>. In general, note that removal services are not comprehensive, as some data brokers do not allow third parties to remove listings, and removal services do not include every data broker on this list, let alone outside of it. You can fill in the gaps <u>using this handy chart</u>.

There are services for media mail as well. For a fee, <u>PaperKarma</u> will remove your name from common direct mail vendors, including charity solicitations, direct mail and catalogs. You can also remove your name from <u>Valpak coupon packs</u>, for free. Sign up for a <u>free CatalogChoice</u> <u>account</u> to cancel catalogs you no longer wish to receive. For a fee, <u>DMAChoice</u> will remove your name from prospective mailers, not including political mail or mail from companies you've done business with in the past two years. DMAChoice also maintains a <u>Deceased Do Not Contact</u> <u>list</u> to allow you to remove names of deceased individuals for marketing lists. (I am sorry for your loss!)

There are several free services available as well. <u>Have I Been Pwned</u> allows you to check to see if your email address has been involved in a data breach. The free tier of <u>Mozilla Monitor</u> allows you to search up to five email addresses to see if your information is exposed in data breaches or found on data broker sites, and gives step-by-step instructions on removal.

Shameless self-promotion

Online privacy and security work hand in hand. There are important steps to take to secure your personal data beyond finding and removing it from people search sites. For my day job, I manage Consumer Reports' <u>Security Planner</u>, a free, easy-to-use guide to staying safer online. Check it out for personalized recommendations and expert advice on topics such as keeping social media accounts from being hacked, locking down smart speakers and home security cameras, and reducing intrusive tracking by websites. This tool builds upon the work of the Citizen Lab, which originally launched and managed the project.

If you'd like to learn more about me and my other work, feel free to check out my website, <u>Yael Writes</u>.

Further reading:

Data Defense: Evaluating People-Search Site Removal Services (Consumer Reports)

Doxxing: Tips To Protect Yourself Online & How to Minimize Harm (EFF)

Here are the data brokers quietly buying and selling your personal information (Fast Company)

Personal Data Removal Workbook and Credit Freeze Guide (Michael Bazzell)

Preliminary results are in! CCPA testers provide important insights into the landmark privacy law (Medium/Consumer Reports)