Data Brokers: What They Are and What You Can Do About Them

If you've ever Googled your own name, you might have seen sites in search results that said that they "found" you, or offered information from a background check. Those sites are data brokers - sites that let the user search for information on specific people, phone numbers, or addresses. They get information from a wide variety of public records and consumer data, including voting records, property records, the information that you provided when you signed up for a loyalty card at the grocery store, etc.

Data brokers typically provide information such as:

- Your name (and possibly aliases or former names)
- Current and past home addresses
- Current and past phone numbers
- The names, and links to data broker profile pages, of your close relatives or "associates" (the latter often, in practice, meaning roommates)
- Current and past email addresses
- Links to your social media accounts like Facebook, Twitter, and LinkedIn

Typically, these sites provide a partial version of your profile for free, and a full version for paid users. The partial version may still include information like full name, a phone number, close relatives, or even a home address. Most people's information gradually appears on these sites while the person is in the 18 to mid-20s age range. People of any age may find that their record is blended with other people's information, especially that of relatives that they have lived with.

You might assume, if someone discovers you at a new address, that you are being tracked using stalkerware, or that your devices are compromised. Those are possibilities that you can read more about in our Survivor Toolkit. However, your

new address may have been found through data brokers, as they are easy for even people who have never heard of them to find and use.

The good news is that it's possible to significantly reduce your privacy risk from data brokers, through measures to keep your information out of data brokers, and requests to opt out. This resource includes steps to take for both options.

An important note: Removing information from data brokers doesn't delete the original records the data brokers used to get your information. Someone could request court, property, or voter records - but it means that it would require more effort, knowledge of how to navigate government systems, and/or money, to obtain the information in them.

Risks, Possibilities, and Preventative Action

Risks depend on many factors that can change over time. For example:

- Is there one stalker looking for your information, or have they also enlisted friends, relatives, or online supporters?
- How knowledgeable are they about finding information online?
- Is the threat specifically to you? Or also to your family? Friends?
- What information are you trying to protect? For instance, have you relocated away from the abusive person, and are trying to protect your new address? Are you living with the person and trying to prevent them from learning your safe second phone or alternate email address?

Removing information from data brokers is mostly a preventative step to increase privacy and stop an abuser, stalker, or harasser from accessing your personal information. For instance, removing information from data brokers may prevent a stalker who is a stranger or acquaintance, or a new date about whom you're still

unsure, from ever learning this information about you. This can also stop someone from finding out about a *new* email address, phone number, or address.

Especially in situations like relocating to a new safe address, these preventable measures may be critical to maintain control over your information. There are some sources of data, like property records, where your options are limited. But for consumer data sources, like grocery loyalty cards or magazine/mailing list subscriptions, you may wish to use a partial version of your name (e.g. first and middle name, or middle and last name) or, if allowed, a made-up name. You can also use an email address created solely for this purpose, or a tool like Mozilla Relay or SimpleLogin to provide "masks" for your email address. If a phone number is required, you can use a VoIP number (Internet-based, like Google Voice, MySudo, or TextNow).

Most US states have an address confidentiality program (ACP) that allows victims of certain crimes (usually domestic violence, sexual assault, or stalking) to receive mail at a special address that is not where they live, and to use that address for various government purposes that ordinarily require a real address, such as being listed on a driver's license or registering to vote. That way, your real address is kept out of those public records, which also helps keep it away from data brokers. ACPs differ in scope and eligibility requirements. It can help to work with an advocate or other case manager while applying for or interacting with these programs. Some states require the application to be filled out by an advocate.

Finally, even if you don't qualify for your state's address confidentiality program, companies called Commercial Mail Receiving Agencies (CMRAs) allow you to rent a virtual address. A virtual address is a rented mailbox at a real street address (not a PO Box) which will either forward your mail to your real address, or digitize your mail and send it to you online. CMRAs include UPS, US Global Mail, iPostal, Physical Address, and many others. Some states may allow you to use a virtual

address for your driver's license or other government needs, but you will need to check with government agencies in your state. Even if you can't use it for government purposes, using it to sign up for consumer services can reduce the information flow to data brokers about you.

Manual (Do-It-Yourself) Opt-Outs

There are dozens of data brokers. Although burdensome, you can manually opt out of them one at a time. Some pose more risks than others due to popularity, amount of information provided, or rank in search results. Some have a "trickle down" effect, where opting out of one will automatically opt you out of others. Depending on your concerns, you may want to opt out of only the most popular data brokers, or those most easily discoverable in current search results for your name, or as many as possible. In the next few paragraphs, we will talk about the following strategies, which can be used separately or together:

1. Assessing search engine results to identify what someone using Google or other search engine searches will be able to find and prioritizing opt-outs from those data brokers.
2. Opt-out prioritization to quickly lower risk from someone who may be aware of data brokers and is likely to go straight to well-known or high-quality data brokers.
3. Complete or near-complete removal of your info from data brokers.

An important note: Even if you opt out of a particular data broker, your information may eventually re-appear in it due to new data coming in. If you are doing manual opt-outs, you can keep a list and check those sites every 3-6 months. Paid subscription-based privacy services will do this for you.

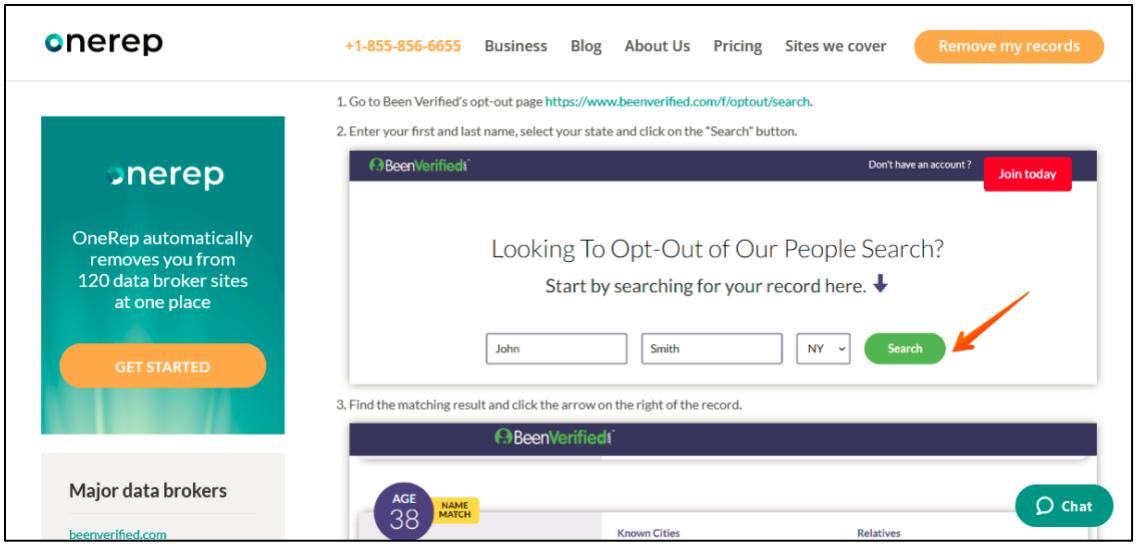
You may wish to repeat your chosen strategies for any relatives who live with you or have lived with you in the past. Someone may search for them in the hope of finding clues about you, and sometimes a search for your name will take a searcher to their records or vice versa. You may want to discuss this with those relatives, since most data brokers require you to attest that you are opting out for yourself or for someone who has given you permission to opt them out.

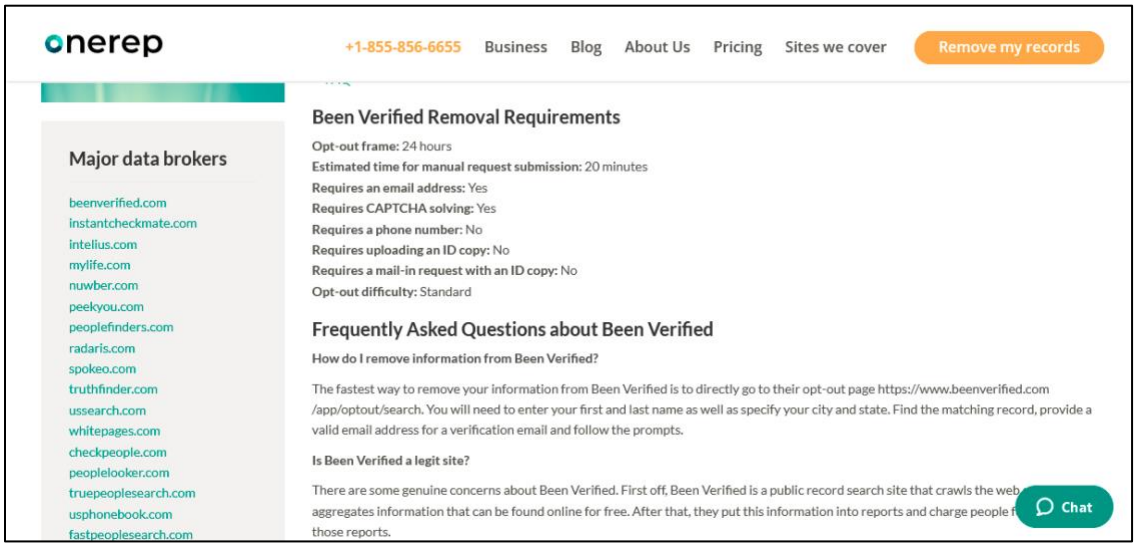
Doing opt-outs can be stressful, especially while dealing with an active or expected threat of danger. You may be able to get help with the work from an advocate or a friend, or process emotionally through a hotline like the National Domestic Violence Hotline.

Assessing Search Engine Results

A helpful method for those who expect an abuser to use search engines to find them, is to search different combinations of your name and current or former towns you've lived in. For example, if Sydney Doe, who goes by Syd, lives in Houston, Texas, after having previously lived in Dallas, Texas, they might search "sydney doe houston texas," "sydney doe dallas texas," "sydney doe texas," "syd doe houston texas," and so on. Try this, and make a list with the sites and profile links with current information on yourself or close relatives that you find in the first two pages of these searches. Then, do the opt-out procedure for each site (in most cases, this will require providing an email address and/or phone number - if this worries you, you can create an email address specifically for this purpose).

You can find detailed and usually-current instructions for opting out of most data brokers on the OneRep Wiki. OneRep also runs a paid removal service, and the first thing the site will suggest is subscribing. Instead, go to the "manual" instructions for each data broker to find a video and text. The following two screenshots of partial instructions for opting out of the popular data broker BeenVerified, illustrate what the instructions look like.





Prioritization of Well-Known Data Brokers for Opt-Outs

Another way to privacy plan, especially if a possible stalker/harasser is aware of data brokers or may be working with a friend or investigator who is – is to focus on opt-outs for popular data brokers and those whose data trickles down to other data brokers. The process of doing opt-outs is the same; the difference is in which ones you are prioritizing. Michael Bazzell's digital privacy workbook lists the most "bang-for-buck" data brokers for this purpose.

Complete Removal

Either strategy discussed above, lowers your risk. You can take the further step of opting out of other data brokers to nearly or completely remove your information. Some resources you can use are:

- The OneRep Wiki
- The DeleteMe DIY opt-outs guide.
- Michael Bazzell's free digital privacy workbook which includes a comprehensive list of data brokers and opt-out instructions. This lists over a hundred data brokers, so if you opt out of a few per day, it will take a month or two to complete.

Paid Subscription Services

Another option is companies that you can pay to opt you out. They will remove you from a large number of data brokers and keep you out for as long as your subscription lasts. We do not endorse any specific subscription service.

DeleteMe

DeleteMe is a service of the company Abine. They offer subscription-based opt-out services for one, two, or four people, allowing you to cover family members or others as well. They remove your information from many data brokers, and allow you to request a custom removal if you discover your information on a site they don't cover. DeleteMe uses human agents to do removal and monitoring.

OneRep

OneRep offers month-to-month plans for one or several people. They are very low-cost for this type of service, and use an automated process. They cover 120 data brokers as of this writing.

Safe Shepherd

Safe Shepherd, like OneRep, uses an automated process, along with the ability to consult with a "privacy expert" on an as-needed basis. They send alerts when they find or remove your info from a site, and information for removal for sites where their automated process won't work. They have a free trial period and several different pricing plans with very different levels of privacy protection.

After Opting Out

Once data brokers have removed your information, there may be a period of time during which search engine results still show previews of the pre-removal information. You can learn why this happens and what to do about it with our Removing Sensitive Content from the Internet resource.

Supported by US DOJ-OVW Grant #15JOVW-21-GK-02216-MUMU. Opinions, findings, and conclusions or recommendations expressed are the authors and do not necessarily represent the views of the U.S. Department of Justice.

We update our materials frequently. Please visit TechSafety.org for the latest version of this and other materials.