July 13, 2023

The Honorable Rohit Chopra
Director, Consumer Financial Protection Bureau
1700 G Street NW
Washington, DC 20552

Re: Request for Information Regarding Data Brokers and Other Business Practices (Docket No. CFPB-2023-0020)

Dear Director Chopra,

Consumer Reports[1] appreciates the opportunity to comment on the Consumer Financial Protection Bureau's (CFPB) request for information (RFI) regarding data brokers and other business practices. As previously noted in a February 2023 letter to the CFPB from a coalition of consumer and privacy advocacy organizations,[2] the scope and scale of the data broker industry is staggering. Data brokers aggregate and sell personal data, amassing "billions of public and proprietary records from thousands of different places"[3] and creating dossiers on millions of people, including more than two-thirds of U.S. residents.[4] Such information is often gathered and sold without consumer consent (or without even consumer knowledge) and without accountability for when there are mistakes in the data or the data is used in a manner that causes harm to consumers.

In response to the RFI's individual-level inquiries (in particular, questions #1, #4, #5, and #6), CR asked its members to share their experiences with data brokers, particularly with respect to attempting to remove their data from a data broker's repository. Selected responses from consumers are provided below. The full set of consumer comments is attached to this letter in Appendix A.

Incorrect data

[1] Founded in 1936, Consumer Reports (CR) is an independent, nonprofit and nonpartisan organization that works with consumers to create a fair and just marketplace. Known for its rigorous testing and ratings of products, CR advocates for laws and company practices that put consumers first. CR is dedicated to amplifying the voices of consumers to promote safety, digital rights, financial fairness, and sustainability. The organization surveys millions of Americans every year, reports extensively on the challenges and opportunities for today's consumers, and provides ad-free content and tools to 6 million members across the U.S.

[2] https://advocacy.consumerreports.org/wp-content/uploads/2023/02/2023-02-08-Coalition-Letter-to-CFPB.pdf

[3] Sarah Lamdan, Data Cartels: The Companies That Control and Monopolize Our Information (2003), Stanford University Press, at page 27.

[4] Sarah Lamdan, Data Cartels: The Companies That Control and Monopolize Our Information (2003), Stanford University Press, at page 35.

Several consumers noted that information contained in data brokers' databases is often incorrect. For example, Troy from Miami, OK told CR:

> "More times than I could ever count in recent years, my personal data, and many times incorrect, has appeared in numerous databases. These data brokers don't bother to check or verify whether or not that information is factual."

Elle from Pahrump, NV noted that:

> "Luckily about 1/3 of the info is incorrect, but some of the errors I see make me wonder if police forces use it and that has resulted in some of the mistakes they make in raiding the wrong households.

Barbara from Conway, SC told CR:

> "Oftentimes, the data is incorrect, such an address belonging to my ex-husband or a relative of his present wife being ascribed incorrectly to me. I sometimes point this out, but mostly I just want my privacy."

Similarly, Steve from Englewood, CO told CR:

> "Also the information these sites use is often inaccurate and misleading - with my name and address linked to email addresses and phone numbers I've never used."

Attempting to remove data from a data broker's repository

A number of consumers noted having taken steps to try to remove data from data brokers' databases, in some cases resorting to paying third-party service providers to help with this process. Consumers' experiences indicated that they are often left frustrated by these efforts. Common challenges faced include difficulties in figuring out the process for opting-out from their personal data being included in databases, long response times from data brokers, and their data only being temporarily removed or not removed at all.

Several consumers noted that they found trying to permanently remove their personal data from data brokers' databases to be futile or impossible. For example, Troy from Miami, OK told CR:

> "Trying to get personal data removed is nearly impossible. I have had to pay a firm that specializes in removing information from databases, and although they do a good job, it still does not stop the proliferation of my personal data including social security number, addresses, phone numbers, etc. from appearing in these databases. My personal data should be Just that, personal! There should be a federal law against data brokers, and data harvesting!!! Why should I have to spend money, not to mention all the time and hassle and headache, because of greedy #@$&@/!"

Similarly, Mark from Vancouver, WA told CR:

> "I have tried many times to remove my data from various data websites. It's like trying to stop a river. You get it removed and it comes back in a month when they refresh their databases. They trying to figure out how or who to contact to get rid of it is next to impossible."

Consumers have also run into problems when trying to get in contact with data brokers or using opt-out forms or removal processes provided. For example, Elle from Pahrump, NV told CR:

> "I have a lot of issues with Instant Checkmate. I have asked them repeatedly to remove my data from their website but they don't reply. I tried to use the suppression/removal process, but all they do is remove the email account from the data and then say that there's no email account associated so they can't remove the data. I have tried to use the contact information to deal with them directly but it gives a no reply error. Even the page to report errors comes up with a 404 page…

Michelle from Fairfield, CA also experienced challenges in getting a response from data brokers despite following all the steps required, telling CR:

> "I have been trying to get my personal information off of the internet for the past year and a half I'm even paying Norton to get my information off the internet and it's still not coming off that's how difficult it is to get your information removed I've tried following all the steps that each of these websites tell you to follow to have your information removed and either you can't get a response there's no one to call if you call it's not the correct number if you email somebody the email won't go through. How are they getting away with this?"

Georgia from Eureka, CA told CR about consistently running into problems when trying to utilize Private Eye's opt-out form:

> "I have tried numerous times to use their opt out form on both Firefox and Chrome browsers. Every time I get the same error message, 'There was a problem with the opt out form, please retry.'
>
> Consequently I have not been able to remove my information from their search engine. I am angry."

Unfortunately, these consumer experiences are in line with research conducted by CR in 2020 on implementation of the California Consumer Privacy Act (CCPA). Even under the CCPA, which provides consumers with the right to opt-out of sale of their information to third parties, consumers still faced many challenges. These challenges included struggling to locate the required links to opt-out of the sale of their data (for 42.5% of sites tested, at least one of three testers was unable to find a Do-Not-Sell (DNS) link) and data broker opt-out processes that were so onerous that they substantially impaired consumers' ability to opt out.[5]

Steve from Englewood, CO expressed a range of concerns to CR, including his requests for removal being ignored for months and personal information only being temporarily removed or not removed at all:

> "Sadly the burden is currently on consumers to identify and individually opt out of dozens of these sites. I have spent countless hours submitting opt-out requests only to be ignored for months or to have my information temporarily removed for just a few weeks until the site updates its data - forcing me to submit a new request.

[5] Mahoney, Maureen. *California Consumer Privacy Act: Are Consumers' Digital Rights Protected?* Consumer Reports, October 2020.

> Submitting an opt out to just one of these sites is a convoluted process with the opt out link often hidden. Usually, the request requires the URL of the webpage to remove - which often requires enduring a lengthy search while bombarded with ads. Typically, submitting a request also requires providing an email address or phone number, providing these companies with even more personal data.
>
> Sometimes these sites will not actually remove personal information - merely "suppressing" it while still trading and selling it to similar sites…
>
> Another issue with these sites is that personal information they provide is often cached by search engines. Thus, even after the people finder site removes a consumer's information, it is still readily available until the search engine's data has been refreshed - which could be weeks or months later."

Only one consumer indicated being successful in removing her personal data from data broker websites, despite having to jump through a few hurdles. Barbara from Conway, SC told CR:

> "I use DuckDuckGo and an ad blocker, so I have seldom noticed ads or offers related to my internet searches. However, I search my name periodically and have found it on websites of data brokers where background data including phone numbers can be purchased for a small fee.
>
> When I find my name, I ask for it and all related data to be removed… There are some hurdles to jump over on some sites, but in general, I have been successful in having my name and data removed when I request this. I always search the site a few days after they confirm the removal to make sure my name does not show up. I am fully aware that my safety may depend on my data being kept private."

Harms experienced by data brokers

Consumers expressed a number of concerns regarding how personal information being readily available on the web could lead to identify theft, fraud and scams, spam, and other harms to consumers. For example, Steve from Englewood, CO told CR:

> "There are literally hundreds of people finder sites on the web that make personal information available to any identity thief, scammer, spammer and miscreant. These unaccountable and unregulated websites have undoubtedly contributed to the explosion of crimes such as: unemployment fraud; voter fraud and intimidation; identity theft; swatting; stalking and bullying."

Logan from Bradenton, FL told CR:

> "If you sell are personal data you should pay us for it and if you don't you must remove it. This has led to too much SCAM CALLS."

Multiple consumers also expressed concerns with data brokers contributing to data breaches. Elle from Pahrump, NV told CR:

> "They collect this info from the dark web so their claims that the info is just a compilation of data available on the internet is not true. Their purchase of this data comes from security breaches so they are the ones funding this type of constant hacking of personal

data. Without companies like InstantCheckmate.com these hackers wouldn't receive the huge payouts that make it worth it to keep collecting our info illegally."

David from Milwaukee, WI told CR about his personal experience with a data breach involving data brokers:

> "The data brokers involved are Truthfinder and Instant Checkmate both entities are owned by PeopleConnect Holdings, Inc. that affected 20.22 million users, with the sole purpose of finding information about people.
>
> On 4/20/2023, I was notified by Experian IdentityWorks that my personal info was compromised and found on the dark web directly related to Truthfinder and Instant Checkmate's data breach. None of the 20.22 million breached users were notified of the alleged breach, as of this date.
>
> I have not found any class action taken against PeopleConnect Holdings, Inc.or its two entities that were breached. I am considering filing a class action, as soon as I locate appropriate legal counsel that are willing to take this matter further."

Joseph from Reno, NV flagged a number of broader harms enabled by data brokers' practices, including with respect to algorithmic discrimination, data privacy, and targeted marketing. He told CR:

> "As a Special Agent (Retired-DHS) turned Private Investigator for the past 15 years I cannot count how many times I have assisted clients and potential clients on the current activities that Data Brokers are deploying. Data Brokers analyze demographic information, purchasing patterns, and online behavior to identify trends and patterns specifically related to elderly consumers. By examining data points such as age, health-related searches, or interest in retirement planning, they can create profiles that target or (and or) categorize older individuals. In my view, as a layman, I present the following to our elected officials and legal professionals.
>
> Consumer segmentation: Data brokers often employ consumer segmentation techniques to group individuals based on similarities in their behavior, preferences, and demographics. They may create segments specifically tailored to elderly consumers, considering factors such as spending habits, healthcare needs, or technology adoption. This very "segmentation" is being used in further big-data marketing strategies, "targeting" products and services for the elderly.
>
> Analysis: Data brokers are currently conducting analyses to determine if their data practices and (or) algorithms disproportionately affect elderly consumers. This involves comparing the outcomes or consequences experienced by different age groups to identify potential disparities. For example, if certain marketing campaigns or product recommendations result in significantly different outcomes for elderly individuals compared to younger age groups, it can be argued that a disparate impact exists.
>
> Privacy concerns and consent: Data brokers are making their own rules, thus attempting to address the issue of potential disparate impact by highlighting the importance of privacy protections and obtaining informed consent. They often argue that their data collection practices are intended to provide personalized experiences and improve consumer satisfaction for all age groups, including the elderly. By emphasizing the

> voluntary nature of data sharing and the ability for individuals to opt-out or control their data, they aim to demonstrate that any potential disparate impact is not intentional. In my view, this conduct is unethical and clearly reveals the deceitful conduct being played upon Americans every day.
>
> Industry regulations and self-regulatory measures: Data brokers are attempting to emphasize their compliance with relevant regulations and industry self-regulatory measures. For example, they may adhere to guidelines set by data protection authorities or industry associations that aim to prevent discrimination and promote fair practices. By demonstrating their commitment to ethical and responsible data usage, they argue that any disparate impact on elderly consumers is unintentional and mitigated through compliance measures. Self-regulation through their control of the AI is clearly not working, the human side of the equation is being totally neglected.
>
> The impacts of data-driven profiling on different consumer groups, including the elderly, should be carefully examined, thus ensuring fair treatment and protection of individual rights. These practices clearly raise concerns about privacy, data ethics, and potential discrimination."

Difficulties in unsubscribing from or blocking unsolicited emails and calls

In addition to concerns regarding data brokers, many consumers highlighted broader frustrations with being inundated with spam emails and unwanted calls and feeling helpless to stop the deluge. A large number of consumers expressed being subject to a barrage of unsolicited emails, texts, or calls from companies they had never heard of, often after signing up for an unrelated product or service. These unwanted communications range from unsolicited marketing to more dangerous phishing efforts.

For example, Paul from Sacramento, CA told CR:

> "I subscribe to a stock advisory service. I receive offer after offer of unwanted advice on investments of all kinds. I'm sure my advisor's support company is selling my information and generating all the unwanted emails. I have asked them specifically not to share my email or address with others. Probably a waste of effort because the flood continues!!!"

Michael from Lake Angelus, MI told CR:

> "I think one investor newsletter I subscribed to sold my email address. I was receiving 5-6 unwanted, unsolicited emails a day and I made the mistake of unsubscribing to one. Now they know I am real and am now receiving 60 a day. I don't dare try and unsubscribe. They say they come from India, the UK, Delaware is a big one, Indiana, all over the place. I am at a loss to know how to stop it."

Of greater concern, some consumers indicated becoming the target of phishing efforts after signing up for an unrelated product of service. For example, Evan from Aberdeen, WA told CR:

> "Ever since signing up for Career Builder, I've gotten phishing e-mails that pretend to be for job applications."

Similarly, Rowan from Cataula, GA told CR:

> “Since putting my information on job boards, actively seeking ERP software positions, I have received everything from ‘mysterious’ loan/grant phone calls to foreign recruiter scams seeking my government -issued ID to solicitations for all kinds of ‘side-hustle’ nefarious ads. This is more than simply opting-in with basic information. I removed myself from various sites, blocked other calls and re-established my DNC listing. The issues have lessened, but still persist!”

Many consumers noted being unsuccessful in trying to subscribe from or block such messages, in some cases receiving even more unwanted communications after submitting a request to unsubscribe.

Bill from Westminster, CO expressed his frustrations to CR about the futility in stopping unwanted communications and asking why it was not possible to prevent your data from being shared:

> “It is a constant barrage of email messages, texts or snail mail from Companies you've never heard of or come in contact with in the past. And when you have tried to categorize them as spam or unsubscribe from the URL in email, you are just inundated with even more unwanted email. Likewise, how many times have you responded to texts with "stop", but continue getting texts from the same or similar origins.
>
> Question for the Community: When you apply for a loan or credit, why is it you have very few options to stop those lenders from sharing your information. We all have received those pamphlets indicating what can or cannot be shared. Out of the many options they disclose there are only a couple that you have a choice not to share your VALUABLE information. Shouldn't it be just the opposite? That they can't share any of it unless you agree to it. Well that's my take and I hope it's yours too.”

Danny from Charlotte, NC expressed similar frustrations to CR regarding the inability to stop unwanted solicitations:

> “My spouse and I have one computer and no smart phones and she has been sick and bedridden, so I monitor her email for her for doctor appointments, test results, prescriptions being ready, etc.
>
> She gets about 30 email advertisements a day to sort through and, with her permission, I spent a month requesting they "Unsubscribe" her. Well, crap! Not only did None of them 'unsubscribe' her, I'll bet she started getting another dozen advertisement emails a day!!! It was like the data brokers said, 'Oh Yeah! We got a 'Live' email address here", and sold it to others and now she gets their junk too!
>
> What a Joke it is to take the time to put yourself on lists to:
> Do Not Call
> Do Not Mail
> Do Not Email
> Do Not Fax
> No Soliciting signs in our yard & neighborhood entrances
> Flyers under our car wipers while shopping
>
> I'd appreciate any Privacy any agency can get us, because right now, there is NONE.”

Peggy from Del Monte Forest, CA also noted that trying to stop unsolicited emails only led to more unwanted emails.

> "I have tried to be removed from unsolicited ads, marketing, false notices, inappropriate solicitations, and garbage that have taken hours away from my life. I try to clean up my mailbox and unsubscribe to these emails but the more I unsubscribe the more unwanted emails come in from other websites. It's horrible! This is a total invasion of privacy and enslavement to technological pirates. Get these hackers out of my life!"

Lastly, from a practical perspective, multiple consumers expressed difficulty in using their phone or email for day-to-day responsibilities and needs due to the deluge of unwanted calls and emails. For example, Lindsey from El Dorado Hills, CA told CR:

> "It seems every time a purchase is made they give you some sweet 20% off offer or better "by just submitting your email". Unfortunately it's a tactic used to capture your data and attempt to sell you more and more ads and share your email with others. It's gotten to a point where my email has thousands of spam advertisements and hundreds of junk emails per day. Sometimes a really important job offer or other correspondence is literally lost in a sea of junk e-mail clogging my mail and preventing me from seeing what I actually need to see.
>
> You can go ahead and try to unsubscribe but sadly your efforts are futile. Suddenly you will be bombarded with thousands of useless unwanted emails from similar companies that want your business.
>
> Some companies send multiple emails daily meaning I may have twenty emails from one business that I never signed up for.
>
> Don't fall for the bait! Be smart and reject these offers or any website that won't let you proceed to shop without providing your data."

Discussion and recommendations

The comments shared above clearly demonstrate consumers' widespread frustration and sense of helplessness with how their personal data is being shared and utilized. Personal data is often being collected and shared without consumer consent, resulting in unsolicited advertising and increased scams, and permanently removing personal data from data brokers' databases ranges from challenging to impossible. Consumers expressed a clear desire for stronger legal safeguards regarding how their personal data is shared, greater control over how their personal data is used, and consistent and simple opt-out processes to delete their data from data brokers' databases.

In fact, some consumers had specific recommendations on measures to address these issues. Mark from Vancouver, WA told CR:

> "This is MY DATA and should belong to me not someone else. There should be laws to restrict this data from being distributed without MY permission. There also must be laws that these data brokers have to spell out how to get your data removed and allow you to be PERMANENTLY removed from their data bases."

Steve from Englewood, CO told CR:

> "People finder and other data brokers should be required to register with the federal government and utilize a centralized and uniform opt-out process so that consumers can make a single request to permanently delete their information from all these sites. It is essential that these sites process these requests within a few business days and that all information be permanently deleted rather than merely hidden.
>
> Additionally, data brokers should not be allowed to sell, trade or transfer information belonging to consumers who have opted out. They must also be mandated to keep a list of consumers who have opted out to prevent their information from appearing again. These sites should be required to ensure that information is correct and to adhere to data security best practices. They should face stiff penalties if their information is stolen, leaked or compromised.
>
> Finally, as part of processing opt out requests, these sites should be required to send re-indexing requests to all search engines to quicken the removal of any cached data. Even better would be if search engines stopped linking to these sites in the first place. The less traffic these sites receive, the less profitable they will be."

CR urges the CFPB to take concrete action on these critical issues that are affecting millions of consumers in the U.S. The negative experiences of consumers highlight a number of related issues in the data broker industry that require regulatory attention. This includes stricter controls on what personal data is collected by data brokers, safeguards on how that data is analyzed and used (including with respect to algorithmic scoring, targeted advertising, and personalized pricing), and restrictions on how data is shared and sold. Greater control should be provided to consumers on how their data is used by data brokers, with user-friendly, standardized mechanisms provided to consumers so that they can easily exercise their rights.

Sincerely,

Jennifer Chien
Senior Policy Counsel, Financial Fairness
jennifer.chien@consumer.org

Consumer Reports
1101 17th St NW #500
Washington, DC 20036
www.ConsumerReports.org
(202) 462-6262