June 13, 2023

Mr. Rohit Chopra, Director
Consumer Financial Protection Bureau
1700 G Street, NW
Washington, DC 20552

Re. CFPB's Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information (Docket No. CFPB-2023-0020)

Dear Mr. Chopra,

On behalf of Asian Americans Advancing Justice | AAJC, we submit our views on the Consumer Financial Protection Bureau's (CFPB) request for information regarding data brokers docket number CFPB-2023-0020.

Asian Americans Advancing Justice | AAJC ("Advancing Justice | AAJC") is dedicated to furthering civil and human rights for Asian Americand and to promoting a fair and equitable society for all. We provide the growing Asian American community with multilingual resources, culturally appropriate community education, and public policy and civil rights advocacy. In the technology and telecommunications fields, Advancing Justice | AAJC works to promote access to critical technology, services, and media for our consumers. How data is collected, processed, used, and stored can have serious repercussions on our communities and their well being.

Examining Consumer's Control of their Personal Data (Question 9)

Data brokers have immeasurable influence over consumers' lives as they collect, store, and sell personal data that can include a childhood home address, email, phone number, browsing activity, credit card purchases, and more. As data brokers have commodified the collection and sale of personal information, it is crucial that the CFPB use its regulatory power through the Fair

Credit Reporting Act (FCRA) to address the deceptive exploitation of consumers' personal information by data brokers.

When examining the impact that data brokers' activities have on consumers' lives, it is critical for the CFPB to take into consideration the unique challenges that historically marginalized communities face. Looking at the Asian American and Pacific Islander (AAPI) community for example, the CFPB should take into consideration that 34% of individuals have limited English proficiency (LEP) and the impact this has on an individuals' ability to control and prevent when their personal data is collected. Furthermore, disaggregated data shows the LEP rates among Asian Americans and Pacific Islanders vary significantly suggesting that some individuals within the AAPI community may be at greater risk of not being able to control the collection, aggregating, sale, resale, or licensing of their personal information.

- Among Asian Americans, nearly 12.3% of Japanese Americans have LEP while 57.6% of Burmese Americans have LEP.[1]
- The average LEP rate among Pacific Islanders also varies among different ethnic groups, from 14% of Micronesian Americans to 2.3% of Native Hawaiians.[2]

Due to language issues, it can be more difficult for individuals with LEP to fully understand and exercise their privacy rights which puts them at increased risk to digital privacy threats. This poses a particular issue for the six million LEP Asian Americans who speak over 100 different languages other than English and who must navigate terms and services, privacy notices, and cookie settings that are already laden with technical jargon, which is often inaccessible for even English proficient users. Unfortunately, this means that opt-out choices are not an effective way to protect those with limited English language abilities as they likely cannot understand the language used in cookie notices well enough to successfully refuse data collection. In instances where translations exist, notices are still difficult to comprehend, as they are often written in technical jargon or they are grammatically incoherent without review by a native speaker.

Language access is critical to address this problem because it would allow people in these communities to better understand what rights they have. For example, during the COVID-19 pandemic, some AAPI small businesses that applied for the Paycheck Protection Program (PPP) resorted to uploading their social security number and tax information to google drive because they were unaware of the harm that comes with sharing their personal information on public sites. There were also reports of scammers taking advantage of AAPI community members with limited digital literacy skills by convincing them to hire someone to complete their unemployment application and file weekly unemployment claims. Information centers, learning modules, notices, and other consumer resources available in non-English languages and tested by

[1] https://data.census.gov/table?t=-04:-05:012:031&tid=ACSSPP1Y2021.S0201&moe=false
[2] https://data.census.gov/table?t=-04:-05:012:031&tid=ACSSPP1Y2021.S0201&moe=false

native speakers will help ensure that historically marginalized communities have the resources needed to be informed consumers.

Transparency around data practices is necessary for consumers to understand how their sensitive data is being collected and stored. It is necessary that data transparency information is accessible in non-English languages, so that all users can exercise their privacy rights. Companies have an obligation to ensure users fully understand how their data is being collected, stored, and sold, and to give them the ability to easily make choices about their personal data. Unless users' rights are actually accessible and exercisable, their rights and any processes built around them will not be meaningful.

Examining the Harms of Data Brokers: Vulnerable Populations (Question 13)

In 2022, House Judiciary Committee Chair Jerrold Nadler and House Homeland Security Committee Chair Bennie Thompson sent a letter seven government agencies - the FBI, DOJ, DHS, CBP, ICE, DEA, and ATF - requesting information about their role in purchasing Americans' personal data from data brokers and private companies.[3] These agencies have used the data they purchased from private data brokers in a wide variety of ways including everything from microtargeting to real-time location tracking that otherwise would be unavailable without a court order.[4] Government agencies having the ability to purchase data that should only be available through a court order is harmful to us all but is particularly dangerous for historically marginalized communities.

As companies collect troves of sensitive personal data of its users, much of that data is also for sale, undermining consumer privacy and eroding Fourth Amendment rights**.** As they currently operate, data brokers scrape public records to create their databases which they then sell to private companies, government agencies, and others. Without the CFPB regulating their practices,"the strong financial incentive to sell data, with virtually nonexistent limitation, gives these companies every reason to share their data with others, including those who use it for harm."[5] For example, the religious application Muslim Pro - which had more than 98 million downloads worldwide - sold users location data to a data broker called X Mode, who then sold this data to their client list which included U.S military contractors without the knowledge or consent of users.[6] Out of 50 Muslim prayer apps, only five of them encrypted personal data,

---

3 https://democrats-homeland.house.gov/news/correspondence/thompson-and-nadler-send-letter-requesting-information-on-government-purchase-of-americans-private-data

4 https://democrats-homeland.house.gov/news/correspondence/thompson-and-nadler-send-letter-requesting-information-on-government-purchase-of-americans-private-data

5 https://www.wired.com/story/opinion-data-brokers-are-a-threat-to-democracy/

6 https://www.latimes.com/business/technology/story/2020-11-23/muslim-pro-data-location-sales-military-contractors

while almost all of them shared data with third parties.[7] The collection, storing, and selling of personal data is a threat to privacy and religious freedom. The harvesting and selling of this data by tech companies threatens both a user's religious freedom and privacy. Profit-driven commercial data collection harms AAPI communities and will continue to do so in the absence of federal action.

Moreover, data is not neutral and when decisions are made without addressing the discrimination embedded in the data, the results are inevitably also discriminatory. Many studies and other data collection methods throughout history exclude Asian American, Native Hawaiian, and Pacific Islander communities entirely from the data collection, limit data collection populations to only those who speak English, or fail to disaggregate any of the data. Unfortunately, this continues to be a common practice, at even institutions like Pew Research.[8] Up to 50% of AAPIs have Limited English Proficiency (LEP),[9] and these populations are often in greatest need of protections and services. Any data collection methods that fail to reach and accurately represent the metrics of these communities entirely excludes AAPIs as an entire demographic group[10] and/or skews the data significantly by only sampling the most convenient groups (those that speak English proficiently). Moreover, even though the AAPI community is one of the most diverse and complex[11]data sets rarely ever disaggregate the data. Data that is used to make important automated decisions for many AAPIs fails to accurately represent them, acknowledge, or include them at all. Automated decision making for Asian Americans, Native Hawaiians, and Pacific Islanders is rarely based on representative data. Inaccurate and incomplete data poses serious negative repercussions, as automated decisions rely on existing data to make important decisions that deeply impact the lives of individuals and communities.

The CFPB should examine the ways that data is used to inform commercial data practices to ensure that all data is accurate, thorough, contextualized and actually representative of the lived realities of individuals. Without contextualizing, fixing, and augmenting data with more accurate metrics, the data that is used to make decisions for the AAPI community will continue to be inaccurate, biased, and ultimately harmful. Data sets must be audited for fairness, inclusivity, and accuracy before they are used to make significant decisions for individuals.

---

7 https://www.brookings.edu/blog/techtank/2022/07/18/examining-the-intersection-of-data-privacy-and-civil-rights/

8 https://www.pewresearch.org/internet/2013/03/29/why-pew-internet-does-not-regularly-report-statistics-for-asian-americans-and-their-technology-use/

9 https://aapidata.com/infographic-limited-english-2-2/.

10 https://www.urban.org/urban-wire/asian-americans-are-falling-through-cracks-data-representation-and-social-services

11 https://www.pewresearch.org/fact-tank/2021/04/29/key-facts-about-asian-origin-groups-in-the-u-s/

Sensitive personal data for sale endangers not only the privacy of individuals but also the civil rights of already surveilled marginalized communities. It's imperative that the CFPB use its regulatory power to investigate the deceptive practices of data brokers and how their practices harm historically marginalized communities.

****

Advancing Justice | AAJC thanks you for the opportunity to provide comments related to this rulemaking. For more information, please contact Emily Chi, Senior Director for Telecommunications, Technology and Media at Asian Americans Advancing Justice | AAJC at echi@advancingjustice-aajc.org.

Sincerely,
Asian Americans Advancing Justice | AAJC