Before the
Consumer Financial Protection Bureau
Washington, D.C.

In re Request for Information Regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information	Document Number: 2023-09353

COMMENTS OF
THE COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION (CCIA)

In response to the Request for Information ("RFI") published in the Federal Register at 88 Fed. Reg. 16951 (Mar. 21, 2023) and extended at 88 Fed. Reg. 38499 (June 13, 2023), the Computer & Communications Industry Association ("CCIA")[1] submits the following comments to the Consumer Financial Protection Bureau ("Bureau"):

I. Introduction

CCIA is pleased to provide comments to help inform the CFPB and stakeholders about data broker business practices and to help facilitate and promote the responsible collection and sale of consumer information. We provide comments herein on some of the topics raised in the RFI, including noting the privacy protections responsible organizations provide for consumers and the unique consumer risks created by the data broker industry.

CCIA and its members appreciate the Bureau's efforts in promoting transparency, fair practices, and consumer protection. By leveraging its authority, enforcement, research, and consumer complaint functions, the CFPB can play a crucial role in addressing potential harms associated with data brokers.

[1] CCIA is an international, not-for-profit trade association representing a broad cross-section of communications and technology firms. For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

II. Data Broker Business Practices and the Unique Risks to Consumers

Responsible organizations are committed to safely handling and safeguarding the personal information consumers provide to them. As noted in the RFI, people have expressed concerns about the lack of control over how data collected about them is used. That is why many leading technology companies have developed and implemented robust privacy policies and programs, along with adopting innovative privacy technologies.[2] These efforts, along with privacy controls, have helped empower consumers while ensuring they continue to receive the benefits from new products and services. Responsible data practices include adhering to important principles like data minimization but also ensuring an organization's privacy principles are sufficient to manage privacy risks to individuals. Good privacy practices include core tenets like transparency and meaningful consumer consent as it is important for consumers to know what information is being collected and how that information is used when they are online. Further, it provides clarity regarding how one's data is collected, used, and shared – empowering individuals to make informed choices about whether to share it at all.

Companies like Google and Amazon remain committed to responsible data practices and their investment into privacy-enhancing technologies (PETs) is just one of the latest efforts to preserve the trust and privacy of their consumers. PETs, most notably differential privacy, are a key tool to minimize data processing.[3] Moreover, PETs offer a variety of tools to enable data minimization. PETs have significantly lowered the baseline of risk associated with handing over one's data and made the incremental increases in risk much smaller. PETs have introduced machine learning into data privacy, which "has the power to reveal information that would not be obvious to a human evaluating a dataset unassisted."[4]

These technology companies have been able to earn and maintain consumer trust through investment and commitments to user privacy.[5] The data broker industry, however, adopts a different approach which, as commentators have noted, has resulted in "numerous consumer

---

[2] https://safety.google/privacy/data/

[3] *See*, Amazon, *Differential Privacy*, Science https://www.amazon.science/tag/differential-privacy

[4] Andrea Scripa Els, *Artificial Intelligence as a Digital Privacy Protector*, 31 HARV. J.L. & TECH. 217, 218 (2017).

[5] Amazon Staff, *Amazon is earning and maintaining customer trust through privacy*, Amazon (Jan. 28, 2022), https://www.aboutamazon.com/news/how-amazon-works/amazon-is-earning-and-maintaining-customer-trust-through-privacy; Corin Faife, *Google pitches for user trust with expanded privacy controls*, The Verge (May 11, 2022), https://www.theverge.com/2022/5/11/23066161/google-privacy-controls-protected-computing-io.

harms and abuses…including significant privacy and security risks, the facilitation of harassment and fraud, the lack of consumer knowledge and consent, and the spread of inaccurate information."[6] Data brokers – those that specialize in the collecting, aggregating, and selling of consumer data to other parties – engage in a wide range of activities with consumer information without providing consumers any meaningful privacy protections. Data brokerage business practices lack any transparency to provide consumers with sufficient information to make informed decisions, let alone the ability to meaningfully exercise control over their personal information.

There are no federal statutes specifically governing the data broker industry. Despite two states – California and Vermont – having data broker registry laws, the applicable controls imposed upon data brokers are overwhelmingly inadequate.[7] The lack of oversight over the data broker and the insufficient consumer control when it comes to interacting with data brokers has created severe risks to civil rights, liberties, competition, and national security.[8] Enforcement actions and investigative reports have revealed countless instances of data brokers knowingly selling consumer data to bad actors, putting countless individuals at risk of serious harm. The individuals put at risk due to these data brokerage business practices included vulnerable groups such as:

- current and past military personnel – by advertising and selling sensitive information that includes individual web searches, family members, and real-time GPS locations data to foreign adversaries like China and Russia.[9]
- the elderly and vulnerable Americans – by selling data to scammers, despite knowing that "their clients were engaged in criminal activity and exploiting the vulnerable" to "sustain revenue streams from their partnerships with scammers."[10]

---

[6] 88 Fed. Reg. 16951 (Mar. 21, 2023) https://www.federalregister.gov/documents/2023/03/21/2023-05670/request-for-information-regarding-data-brokers-and-other-business-practices-involving-the-collection.
[7] Justin Sherman, *Examining State Bills on Data Brokers*, Lawfare (May 31, 2022), https://www.lawfaremedia.org/article/examining-state-bills-data-brokers.
[8] Steven J. Arango, *Data Brokers Are a Threat to National Security*, U.S. Naval Institute (Dec. 2022),https://www.usni.org/magazines/proceedings/2022/december/data-brokers-are-threat-national-security.
[9] Suzanne Smalley, *Brokers' sales of U.S. military personnel data overseas stir national security fears*, Cyberscoop (April 20, 2022), https://cyberscoop.com/data-brokers-national-security-risk/.
[10] Alistair Simmons and Justin Sherman, *Data Brokers, Elder Fraud, and Justice Department Investigations*, Lawfare (July 25, 2022), https://www.lawfaremedia.org/article/data-brokers-elder-fraud-and-justice-department-investigations.

- medical patients – by selling consumers' precise geolocation data and marketing in a manner that would allow its client to "track consumers' movements to and from sensitive locations" such as at a health clinic, therapist's office, or an addiction treatment center. [11]

III. Conclusion

CCIA applauds the CFPB for conducting this opportunity to provide comment on the unique consumer risk created by data broker business practices. CCIA and its members appreciate the CFPB's commitments to consumer protection and addressing the potential harms associated with data brokers.

Respectfully submitted,

Alvaro Marañon
Policy Counsel
Computer & Communications Industry Association
25 Massachusetts Avenue NW, Suite 300C
Washington, DC 20001
amaranon@ccianet.org

July 15, 2023

[11] Lesley Fair, *FTC says data broker sold consumers' precise geolocation, including presence at sensitive healthcare facilities*, FTC Business Blog (Aug. 29, 2022), https://www.ftc.gov/business-guidance/blog/2022/08/ftc-says-data-broker-sold-consumers-precise-geolocation-including-presence-sensitive-healthcare.