June 20, 2023

Rohit Chopra
Director
Consumer Financial Protection Bureau
1700 G Street NW
Washington, District of Columbia 20552

RE: Comments of ACT | The App Association regarding the Consumer Financial Protection Bureau's Request for Information regarding Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information

Dear Director Chopra:

ACT | The App Association (the App Association) appreciates the opportunity to provide input to the Consumer Financial Protection Bureau (CFPB or Bureau) in response to its request for information on Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information.[1]

I. Statement of Interest & General Comments on Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information

In general, the App Association supports the Bureau's efforts to better understand new business models that sell consumer data to exercise enforcement, supervision, regulatory, and other authorities. Consumer data essentially powers the internet, which has brought about both significant innovation as well as risks to those consumers. While the data that consumers generate about themselves through their online activities is valuable and should be accessible and portable to them, many harms consumers face also stem from the pervasive collection of data that they may unknowingly have generated. Many beneficial use cases of personalization and targeted advertising exist, but at the same time, they also give rise to abuse and privacy threats that can result in real-world damage.

The App Association is a global trade association for small and medium-sized technology companies. We work with and for our members to promote a policy environment that rewards and inspires innovation while providing resources that help them raise capital, create jobs, and continue to build incredible technology. Today, the value of the ecosystem the App Association represents—which we call the app economy—is approximately $1.8 trillion and is responsible for 6.1 million American jobs.[2] As the world has quickly embraced mobile technology, our member companies have been creating innovative solutions that power the growth of the internet of things (IoT) across modalities and segments of the economy.

The App Association's members include many innovators who develop mobile technology products in both established and emerging markets, and they work to handle personal data with the appropriate care.

[1] Request for Information: Data Brokers and Other Business Practices Involving the Collection and Sale of Consumer Information (March 21, 2023), Federal Register Number 2023-05670
[2] https://actonline.org/2022/09/30/act-the-app-association-report-reveals-apps-contributed-e210-billion-to-the-eu-economy-in-2021/.

Our members take privacy and consumer complaints seriously, and they care about how data is used and shared because it affects how their products function and how consumers engage with those products and services. Our members handle and work with data daily, so they are directly affected by consumer trust issues that abuse by data brokers may cause. Consumer trust is fundamental for competitors in the app economy, especially for smaller firms that may not have substantial name recognition. Strong data privacy protections that meet evolving consumer expectations are a key component of developing consumer trust in tech-driven products and services. The App Association helps shape and promote privacy best practices in a variety of contexts, including for apps directed to children and digital health tools, making us well-positioned to respond to this CFPB request for information.

We believe the current lack of understanding and transparency of data broker practices makes users only more vulnerable to risks and makes it harder for policymakers to address the issue. Additionally, the lack of federal privacy legislation has allowed the data broker industry to profile millions of Americans in a legal grey zone. We, therefore, welcome the Bureau gathering information on data brokers and their business practices.

II. General Views of the App Association on the Need for a Comprehensive Cross-Sectoral Privacy Framework

The protection of consumers' data and trust is of the utmost importance to the small business community. Now more than ever, the small businesses and startup innovators we represent rely on a competitive, trustworthy, and secure ecosystem to reach millions of potential users across consumer and enterprise opportunities so they can grow their businesses and create new jobs. Today, the "tech sector" no longer exists as a separate, unique vertical. Rather, it has expanded and taken root as part of other industries, and in the process, it has been democratized into a startup economy that thrives across the nation, mostly outside of Silicon Valley. As cars begin to drive themselves and physicians adopt clinical decision tools that utilize artificial intelligence (AI), the United States is fast evolving into a "tech economy." Moreover, companies thought of as tech heavyweights often have more in common with traditional economy players from a business model standpoint; the former just happen to use newer technologies and find ways to make them useful for people.

As regulators from across key markets abroad continue to rush to utilize approaches to regulation of the digital economy which are often heavy-handed, the United States has remained the greatest market in the world for building a startup due to its evidence-based and light-touch approach to regulating new industries. Across the world, other governments struggle to incent and sustain the digital economy growth seen only in this country because companies elsewhere often face great barriers to bringing novel products and services to market, slowing technological innovations to the pace of government approval.

The American approach to privacy remains a work in progress, and the App Association agrees that the time for changes to the U.S. approach to privacy regulation has arrived. Federal sector-specific regulation of privacy, along with a patchwork of state-level laws and regulations, presents a challenging scenario for a small business innovator. The App Association is supportive of a new federal privacy framework that will clarify the obligations of our members and pre-empts the fractured state-by-state privacy compliance environment, and generally urges that the U.S. approach to privacy provide robust privacy protections that correspond to Americans' expectations, as well as leverage competition and innovation. We believe comprehensive federal privacy legislation can address some of the issues raised by the Bureau in this request for information (RFI). A federal law more intentionally focused on curbing privacy harms should empower consumers to exert more control over their sensitive personal information, including the rights to access, correction, and deletion of such information. Sensitive personal information should also be subject

to some flexible limits on processing activities that pose too great a risk to consumers, especially in the context of data brokers selling personal data to discriminate or deceive.

As the RFI points out, business models have emerged that sell consumer data and have grown alongside the internet and advanced technologies which may not be covered by existing legislation like the Fair Credit Reporting Act (FCRA). Data brokers collect and aggregate various categories of personal information, including a consumer's name, physical and e-mail addresses, phone numbers, age, gender, education, family information, professional information (job and/or salary), political leanings, ownership of homes or cars, and, increasingly, sensitive location data and health information via wearables and smartphones. The practice of building profiles of individuals who lack understanding of the scope and breadth of data brokers' business practices and their impacts exposes those individuals to significant privacy and security risks, including, as the RFI notes, the facilitation of harassment and fraud, discrimination, and the spread of false information. We agree with the Bureau that consumers should be able to expect companies to safeguard their personal information and should be able to know and control how companies obtain and use their data. If a company is selling and/or sharing user data, that company should clearly explain why and how that data is being shared (in plain language, as opposed to unnecessarily long and complicated end-user license agreements), and how it will be used so that the consumer can make an informed decision and provide affirmative consent mechanisms for certain uses.

All consumers must be able to trust and safely access digital services to realize their full potential and increase the adoption of beneficial digital services. Enabling all Americans to enjoy robust privacy protections via federal privacy legislation will help to accomplish that goal and increase trust in the digital economy. Trust is the linchpin of App Association members' economic viability. Even as more and more of our member companies take advantage of opportunities in the enterprise space, trust is just as—if not more—important as it is for companies that serve consumers directly.

III. Extent to Which Sales or Transfers of Consumer Data by Data Brokers Raises Privacy Concerns

App Association members include leading consumer financial app developers who build transparency and privacy concepts into their innovations "by design" as a matter of principle and ethics. Our members condemn the unethical or illegal sharing of sensitive financial information with third parties, particularly when it is done without the knowledge and consent of an individual. If consumers access their and their family's financial data—some of which are likely sensitive—through a smartphone, users should have a clear understanding of the potential uses of that data by developers. Otherwise, most users will not be aware of who has access to their information, how and why they received it, and how it is being used. The downstream consequences of using data in this way may ultimately erode a user's privacy and willingness to disclose information to his or her financial services provider. The App Association believes that it is in the best interest of the consumer/user to understand how their data is being used.

At the same time, the small business developer community the App Association represents already practices responsible and efficient data usage to solve problems identified across consumer and enterprise use cases. Since the inception of the General Data Protection Regulation (GDPR) in Europe, the California Consumer Privacy Act (CCPA), and the subsequent adoption of similar measures around the country and the world, our members have responded to evolving consumer expectations and enhanced market competition by meeting and, in many cases, exceeding relevant legal requirements. These efforts include the utilization of cutting-edge privacy-by-design approaches from the earliest phases of product development and the most advanced tools and methodologies available, such as differential privacy

techniques.[3] We welcome such regulation, as complying with GDPR and CCPA has given some of our members a competitive advantage over competitors who are not compliant and typically creates new opportunities through a thorough review of organizational processes.

The App Association appreciates and shares the Bureau's interest in protecting user privacy. Consumers around the world rely on our members' products and services, with the expectation that our members will keep their valuable data safe and secure. Despite the protestations of traditional financial institutions attempting to retain their ironclad grip over consumer financial data, our members' commitment to privacy and security is robust, as evidenced above.

Like the Office of the National Coordinator for Health Information Technology (ONC)[4] and Centers for Medicare & Medicaid Services (CMS)[5] have, the Bureau should establish a framework outlining high-level data privacy and security guardrails that addresses individual access, data collection, uses and disclosures, consent and authorization, breach mitigation procedures and consumer notice, and security practices. Such requirements should be based on demonstrated risks to consumers, with technology-neutral measures, scaled to the levels of risk presented, as means for compliance. Such guardrails should ensure that consumers are oriented to the risks of sharing their financial data with third parties that are not financial institutions and better equip the Federal Trade Commission to hold third parties to sound privacy and security practices.

IV. How Federal Privacy Legislation Could Regulate Data Brokers

The American Data Privacy and Protection Act (ADPPA) was introduced in the 117th Congress in June 2022 and remains the closest the United States has come to passing federal privacy legislation. ADPPA is a comprehensive federal privacy law that would introduce requirements for businesses that store, process, and share personal data. It also includes two sections that are relevant to the Bureau's request for information on data brokers. Section 206 defines "third-party collecting entities" as companies that collect personal data about an individual but do not directly collect it from that individual and "whose principal source of revenue is derived from processing or transferring covered data that the covered entity did not collect directly from the individuals linked or linkable to the covered data." While this definition is not an exact synonym for data brokers, this language would likely cover most third-party actors in the data broker industry, excluding first-party collectors and those that have a "principal source of revenue" other than processing or transferring personal data.

Section 206 would require third-party collecting entities to:

1. Place a conspicuous notice on their website that includes FTC-approved language and link to an FTC-created registry of third-party collecting entities;
2. Register with the FTC if the third-party collecting entities processed covered data of more than 5,000 people or devices in the previous year;
3. Pay fines for failing to register or provide notices on their websites.

---

[3] Differential Privacy, HARVARD UNIVERSITY PRIVACY TOOLS PROJECT. https://privacytools.seas.harvard.edu/differential-privacy (last visited 17 February 2023).

[4] Office of the National Coordinator for Health Information Technology, Information Blocking and the ONC Health IT Certification Program: Extension of Compliance Dates and Timeframes in Response to the COVID-19 Public Health Emergency. October 2020. https://www.federalregister.gov/documents/2020/11/04/2020-24376/information-blocking-and-the-onc-health-it-certification-program-extension-of-compliance-dates-and

[5] Centers for Medicare & Medicaid Services, "Patient Privacy and Security Resources – Supporting Payers Educating their Patients." December 2020. https://www.cms.gov/files/document/patient-privacy-and-security-resources.pdf

Per ADPPA, the FTC would create and maintain a public, searchable, and central registry of third-party collecting entities and the information they have submitted to the registry. Within the registry, consumers would be able to submit a "do not collect" request to all entities the registry includes. This mechanism would provide consumers with a one-stop-shop to opt out of third-party collection and request entities to delete all covered data held about them.

Section 203 of ADPPA does not explicitly target data brokers or third-party collecting entities, but it gives consumers some data rights, including correction and deletion of covered data. When an individual requests correction or deletion, the covered entity has to make a reasonable attempt to notify third parties and service providers to which the individual's data may have been transferred of this request. We note, however, that this notification requirement does not require third parties to correct or delete the individual's data. A deletion request would still need to be submitted to the FTC. Nonetheless, ADPPA or a similar bill that takes a comprehensive approach to consumer privacy would take crucial steps to decrease the threats and harms consumers face in the current data broker environment.

V. Conclusion

As stated above in more detail, the App Association prefers and supports strong federal privacy legislation that requires covered companies to take certain steps to detect, prevent, and remediate unauthorized access to personal information. We support the inclusion of data security requirements that preempt most state laws that would otherwise impose conflicting or substantially different data security obligations. Strong federal data security provisions would raise the average readiness of American companies to defend against cyber threats of all kinds, from state-sponsored ransomware campaigns to social engineering and phishing attacks. Additionally, last year's ADPPA proposed creating a national, public registry of companies that could be engaged in data brokerage and established a central opt-out mechanism for consumers from third-party data brokers' processing practices. Both provisions would help remedy some of the issues present in the currently mostly unregulated data broker ecosystem.

We thank the CFPB in advance for its consideration of our views. We are committed to helping the Bureau actualize the benefits that will flow from consumers enjoying strong access rights and choice regarding their personal data, including financial data. We look forward to engaging further in the future.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Anna Bosch
Privacy Policy Associate

Leanna Wade
Regulatory Policy Associate