CENTER FOR DEMOCRACY & TECHNOLOGY

December 20, 2021

To: Amy Zirkle, Program Manager for Payments & Deposits
Bureau of Consumer Financial Protection
1700 G Street NW
Washington, DC 20052

Re: Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms (Docket No. CFPB-2021-0017)

The Center for Democracy & Technology (CDT) respectfully submits these comments in response to the Bureau of Consumer Financial Protection's (CFPB) request for information regarding the CFPB's inquiry ("Inquiry") into the payment platforms operated by Google, Apple, Facebook, Amazon, Square, and PayPal ("Companies"). CDT is a nonpartisan, nonprofit 501(c)(3) organization that is dedicated to advancing civil rights and civil liberties in the digital world and challenging exploitative uses of technology.

Director Rohit Chopra has stated that the Inquiry is intended to "yield insights that may help the CFPB to implement other statutory responsibilities" and better understand large technology companies' practices.[1] The Inquiry is especially necessary because, while fair lending laws readily apply to financial institutions, the extent to which they cover the full range of technology companies providing payment services is less clear.[2] Yet, technology companies have arguably become as common a fixture of consumer finance as financial institutions. When reviewing and assessing each of the six Companies' responses to the Inquiry, CDT urges the CFPB to consider the following potential issues that may become evident in the information received.

[1] Bureau of Consumer Fin. Prot., Statement of the Director Regarding the CFPB's Inquiry Into Big Tech Payment Platforms (Oct. 21, 2021), https://files.consumerfinance.gov/f/documents/cfpb_section-1022_directors-statement_2021-10.pdf.

[2] *See e.g., Cyber Threats, Consumer Data, and the Financial System: Hearing before the H. Subcomm. on Consumer Prot. and Fin. Inst. of the H. Comm. on Fin. Serv.* (2021) (testimony of Samir Jain, Director of Policy, Center for Democracy & Technology), https://cdt.org/wp-content/uploads/2021/11/hhrg-117-ba15-wstate-CDT-Samir-Jain-20211103-House-Financial-Commitee-testimony.pdf [hereinafter "Testimony of Samir Jain"]. *But see* Complaint ¶ 35, PayPal, Inc., F.T.C. Docket No. C-4651 (May 23, 2018); Decision and Order, PayPal, Inc., F.T.C. Docket No. C-4651 (May 23, 2018).

Flawed approaches to user privacy

The Inquiry asks for information pertaining to whether each collected data field can be used to identify an individual user of the payment system.[3] Specifically, it asks for information from the Companies about their aggregation and anonymization methods. The CFPB should maintain a skeptical eye when examining how each Company interprets the terms "aggregated" and "anonymized" and executes these measures.

Sufficient anonymization is difficult to achieve because anonymized data can be combined with just a few other data points to re-identify the data relatively easily.[4] This is especially true for location data – one of several types of data the Companies collect – because an entity can re-identify location with publicly available information alone.[5] This risk continues to grow with the availability of greater volumes of data and improved methodologies to match data across multiple datasets.[6] This danger is particularly acute with respect to the Companies, several of which amass voluminous and detailed data about individuals. As a result, payment information that may appear appropriately anonymized in isolation may be subject to re-identification when combined with all the other data the Companies possess.

Data aggregation has the potential to be a more privacy-protective approach.[7] Still, data can be disaggregated, increasing privacy risks when the data is repurposed for secondary uses that the user may not fully understand, let alone agree to.[8]

---

[3] Bureau of Consumer Fin. Prot., Order to File Information on Payments Products, Section B: Data Harvesting, Questions 9(b), (c), and (d) (Oct. 21, 2021), https://files.consumerfinance.gov/f/documents/cfpb_section-1022_generic-order_2021-10.pdf [hereinafter "CFPB Inquiry"].

[4] MANA AZARMI AND ANDREW CRAWFORD, CTR. FOR DEMOCRACY & TECH., USE OF AGGREGATED LOCATION INFORMATION AND COVID-19: WHAT WE'VE LEARNED, CAUTIONS ABOUT DATA USE, AND GUIDANCE FOR COMPANIES 2-3 (May 29, 2020), https://cdt.org/wp-content/uploads/2020/05/2020-05-29-Use-of-Aggregated-Location-Information-and-Covid-19.pdf.

[5] Stuart A. Thompson and Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html.

[6] ELIZABETH LAIRD AND HANNAH QUAY-DE LA VALLEE, CTR. FOR DEMOCRACY & TECH., DATA ETHICS IN EDUCATION AND THE SOCIAL SECTOR: WHAT DOES IT MEAN AND WHY DOES IT MATTER? 17 (2021), https://cdt.org/wpcontent/uploads/2021/02/2021-02-19-Data-Ethics-and-Ed-and-Social-Sector-FINAL.pdf.

[7] AZARMI, *supra* note 4, at 3-5; Chris Calabrese, *Working with Airbnb to Use Data to Fight Discrimination*, CTR. FOR DEMOCRACY & TECH. (Jun. 17, 2020), https://cdt.org/insights/working-with-airbnb-to-use-data-to-fight-discrimination/; Emma Llansó, *Understanding Automation and the Coronavirus Infodemic: What Data Is Missing?*, CTR. FOR DEMOCRACY & TECH. (Apr. 22, 2020), https://cdt.org/insights/understanding-automation-and-the-coronavirus-infodemic-what-data-is-missing/

[8] LAIRD, *supra* note 6, at 15 (2021).

Misalignment with consumers' reasonable expectations

The Inquiry asks the Companies to describe how consumers are informed about the Companies' data collection, use, and retention, and how the Companies respond to consumers granting or denying consent.[9] When reviewing the procedures described in response to this item, the CFPB should compare consumers' expectations when they use one of the Companies' payment systems to the expectations consumers have with respect to financial institutions.

Consumers generally anticipate certain types of data collection and exchanges with traditional financial institutions. Consumers are generally aware that account and routing numbers are produced by financial institutions themselves, and that these institutions have consumers' addresses, contact information, Social Security numbers, and dates of birth. Consumers expect that these institutions will know the party to whom they send or from whom they receive payments, and they might also recognize that fraud alerts are triggered by their location and account activity data.[10] With appropriate disclosures, consumers may reasonably expect the Companies to have most of this data as well to the extent they use their payment processing services.

However, consumers might not foresee the extent to which the Companies combine this payment-related information with all the other information they collect and the insights and inferences such combinations yield. It does not help that more of the Companies are blurring the lines between social networking features and payment platforms, influencing the degree of risk consumers recognize in the sharing of payment data. For example:

- Facebook users socialize with family and friends, follow brands, share content and news, buy and sell items, donate, send payments to personal contacts, create events, pay to watch certain media, view advertisements related to purchase history, purchase subscriptions and intangible "stars" to send to creators, all within the same few spaces.[11]

[9] CFPB Inquiry, Section E, Question 43.

[10] *See Banks Focus on Location to Fight Fraud*, PYMNTS.COM (Jan. 19, 2021), https://www.pymnts.com/news/security-and-risk/2021/location-detection-building-the-bank-business-case-for-better-geolocation-data/.

[11] Facebook, *Facebook Pay*, https://pay.facebook.com/; Jia Jen Low, *Data From Facebook Pay Will Power Its Advertising*, TECHHQ (Nov. 14, 2019), https://techhq.com/2019/11/data-from-facebook-pay-will-power-its-advertising/.

- Integration across Google and Apple's wide range of applications and devices may feed far more consumer data – from purchase history, to navigation history and web browsing activity saved to user accounts, to viewing history on streaming services and apps like YouTube and iTunes, to physical fitness data through wearables – into these Companies' advertising ecosystem.[12]
- PayPal operates Venmo, which has turned consumers' transactions into social media feeds where users can share, comment on, and "react" to recent payments and see with whom other users are exchanging payments.[13] The FTC charged that Venmo misled consumers about the extent to which they could control the privacy of this information.[14]

The Companies have a wealth of data that, when combined with data collected in the course of processing payments, vastly expand how much the Companies can influence how consumers move through digital spaces beyond what consumers reasonably expect.

The Inquiry asks whether collected data fields are used only to "facilitate the delivery of product to consumers."[15] When reviewing the Companies' responses, the CFPB should scrutinize what delivery of the payment services truly entails, whether each data field is actually necessary to facilitate delivery of the payment services, and whether the Companies may be using each data field for other purposes, especially when combined with other data. Companies may assert that certain data does "facilitate the delivery" of services because it helps improve targeted advertising, but that does not help deliver the actual payment processing service to the consumer whose data is collected. Some of the Companies' policies state that they use and exchange data about purchases with third parties to develop, provide, and improve their products, and that they may retain data that is disassociated from users.[16] The CFPB should

[12] Google, *Products*, https://about.google/products/; ELIZABETH ANNE WATKINS, CTR. FOR DIGITAL JOURNALISM, GUIDE TO ADVERTISING TECHNOLOGY (Dec. 2018), https://www.cjr.org/tow_center_reports/the-guide-to-advertising-technology.php.

[13] Complaint ¶¶ 9, 17, PayPal, Inc, *supra* note 2; Jack Morse, *Payment Apps Collect and Share Your Data. Here's How to Lock Them Down*, Mashable (Jun. 9, 2021), https://mashable.com/article/venmo-cash-app-paypal-data-privacy.

[14] Press Release, Fed. Trade Comm'n, PayPal Settles FTC Charges That Venmo Failed to Disclose Information to Consumers About the Ability to Transfer Funds and Privacy Settings; Violated Gramm-Leach-Bliley Act (Feb. 27, 2018), https://www.ftc.gov/news-events/press-releases/2018/02/paypal-settles-ftc-charges-venmo-failed-disclose-information.

[15] CFPB Inquiry, Section B: Data Harvesting, Questions 9(e) and 11(b).

[16] *See e.g.*, Facebook, *Data Policy*, https://www.facebook.com/policy.php (last revised Jan. 11, 2021); Apple, *Apple Pay & Privacy*, https://www.apple.com/legal/privacy/data/en/apple-pay/; Amazon, *Amazon.com Privacy Notice*,

question whether the Companies in fact collect, retain, and share payment data for purposes related to the Companies' performance indicators[17] that do not necessarily translate to benefits for consumers.

Further, the CFPB should look closely at whether Companies' agreements and disclosures are adequate. The Inquiry asks for information about agreements to which consumers must consent in order to use the Companies' payment platforms. Reliance on terms of use or similar notice mechanisms does not ensure that consumers are adequately informed.[18] Even to consumers who do review notice mechanisms, the network of third parties (or "partners") with whom data is shared remains obscured. Navigating through Facebook, Amazon, and Google's numerous policy pages, consumers may not learn that MoPub, a mobile app advertising platform, lists these Companies among over a hundred advertising partners who have other partners of their own.[19] The CFPB should probe the Companies' response to analyze how, or even whether, the Companies ensure that consumers comprehend precisely what they are agreeing to when they accept these agreements. Based on the language and volume of the agreements, policies, and disclosures that the Companies provide, the CFPB should assess how clearly and thoroughly the companies explain who third parties are, the types of data shared with each identified third party, and the purposes for which each type of data sharing occurs.

Potential consequences for other consumer finance decisions

Expansion of the Companies' online payment platforms also raises questions about potential impacts down the road for credit and loan applicants. The Inquiry asks whether the Companies collect data related to race, sex, age, and other traits protected under the Equal Credit Opportunity Act.[20] But the agency should examine what other data the Companies use and collect that may be proxies for such characteristics or that can result in disparate impacts.

Compared to data that financial institutions use to process payments, consumers have far less visibility into the array of data that financial institutions use to approve or deny credit, modify interest rates or other borrower terms, and advertise or offer new products to current or

https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ (last updated Feb. 12, 2021).

[17] CFPB Inquiry, Section B: Data Harvesting, Question 4.

[18] Testimony of Samir Jain, *supra* note 2.

[19] MoPub, *Our History*, https://www.mopub.com/en/company/history; MoPub, *MoPub Partners*, https://www.mopub.com/en/legal/partners.

[20] CFPB Inquiry, Section B: Data Harvesting, Questions 46 and 47.

prospective customers.[21] This includes data that can become proxies for protected characteristics.[22] For example, one fintech company's use of education data subjected students at minority-serving higher education institutions to higher student loan interest rates.[23] Employment data is another basis for lending decisions, and people of color are more often denied loans based on the type of employment they have and on whether they work multiple jobs.[24] Decision-making based on data about a consumer's education and employment history can cause disabled consumers to be rejected at higher rates as well.[25]

Reports have documented how some of the Companies deliver social networking and advertising differently based on data related to marginalized identities and their intersections.[26] The merging of social media features, advertising features, and payment services enables the Companies to combine data derived from payment processing with multiple other streams of data they readily access as part of their business models. This is especially concerning as lenders and credit bureaus actively seek data about consumers' social media and web activity when determining creditworthiness, especially for young consumers who are just beginning to build credit.[27] The CFPB should examine closely whether and how the Companies' collection of data in connection with payment processing services may feed into discrimination and

[21] Ctr. for Democracy & Tech, Comments to Federal Financial Regulators on Financial Institutions' Use of AI, Jul. 1, 2021, https://cdt.org/wp-content/uploads/2021/07/2021-07-01-CDT-Request-for-Information-and-Comment-on-Financial-Institutions-Use-of-Artificial-Intelligence-including-Machine-Learning.pdf.

[22] Karen Hao, *The Coming War on The Hidden Algorithms That Trap People in Poverty*, MIT TECH. REV. (Dec. 4, 2020), https://www.technologyreview.com/2020/12/04/1013068/algorithms-create-a-poverty-trap-lawyers-fight-back/.

[23] STUDENT BORROWER PROT. CTR., INEQUITABLE STUDENT AID 16 (2021), https://protectborrowers.org/wp-content/uploads/2021/03/SBPC_Inequitable-Student-Aid.pdf; RELMAN COLFAX PLLC, FAIR LENDING MONITORSHIP OF UPSTART NETWORK'S LENDING MODEL 22-23 (2021), https://www.relmanlaw.com/media/cases/1088_Upstart%20Initial%20Report%20-%20Final.pdf.

[24] *See* Emmanuel Martinez and Lauren Kirchner, *The Secret Bias Hidden in Mortgage-Approval Algorithms*, THE MARKUP (Aug. 25, 2021), https://themarkup.org/denied/2021/08/25/the-secret-bias-hidden-in-mortgage-approval-algorithms.

[25] Obligations under the Fair Credit Reporting Act apply to entities that qualify as consumer reporting agencies and furnish information bearing on character, reputation, personal characteristics, or mode of living, as well as to medical information.

[26] *See* MUHAMMAD ALI ET AL., DISCRIMINATION THROUGH OPTIMIZATION: HOW FACEBOOK'S AD DELIVERY CAN LEAD TO SKEWED OUTCOMES 1-2, PROCEEDINGS OF THE ACM ON HUMAN-COMPUTER INTERACTION (2019) https://arxiv.org/pdf/1904.02095.pdf; Jeremy B. Merrill, *Google Has Been Allowing Advertisers to Exclude Nonbinary People from Seeing Job Ads*, THE MARKUP (Feb. 11, 2021, 8:00 AM). https://themarkup.org/google-the-giant/2021/02/11/google-has-been-allowing-advertisers-to-exclude-nonbinary-people-from-seeing-job-ads.

[27] *See e.g.*, Aime Williams, *How Facebook Can Affect Your Credit Score*, FIN. TIMES (Aug. 25, 2016), https://www.ft.com/content/e8ccd7b8-6459-11e6-a08a-c7ac04ef00aa.

disparate impacts in the financial system as a whole, as well as with respect to the Companies' own practices.

The Inquiry also asks how the Companies detect and respond to fraud or other illegal activity,[28] but the Companies may themselves contribute to this activity. Companies that turn transactions into a social media feed or incorporate them into communication tools can end up giving significant insight to bad actors about consumers' activities and social connections.[29] Thus, exposure and misuse of payment data and other online activity now might be setting consumers up for worsened credit discrimination in the future.

Conclusion

Safeguards under existing consumer financial protection laws, including Section 1031 of the Dodd-Frank Wall Street Reform and Consumer Protection Act, prohibit unfair, deceptive, and abusive practices.[30] However, the applicability of these safeguards, and consumers' ability to detect potential violations, is complicated because consumers have a very different relationship with the Companies' numerous data-driven products than with traditionally covered financial institutions. When reviewing the Companies' responses, the CFPB should determine whether the Companies' payment platforms might over-rely on ineffective methods to protect identifiable information, deviate from consumers' reasonable expectations regarding data use and sharing, and/or open the door to increased discrimination in consumer finance. As these risks grow, we urge the CFPB to clarify and update the agency's regulations and guidance so that entities that want to be part of the financial system are required to be accountable as such.

Respectfully submitted,

Ridhi Shetty
Policy Counsel, Privacy & Data Project
Center for Democracy & Technology
rshetty@cdt.org

[28] CFPB Inquiry, Section B: Data Harvesting, Question 50.
[29] *See* ED MIERZWINSKI ET AL., U.S. PIRG EDUC. FUND, VIRTUAL WALLETS, REAL COMPLAINTS: HOW DIGITAL PAYMENT APPS PUT CONSUMERS' CASH AT RISK 8 (June 2021), https://uspirg.org/sites/pirg/files/reports/VirtualWallets/Virtualwallets_USP_V3.pdf.
[30] 12 U.S.C.§ 5531; 15 U.S.C. § 6801 et seq.; 15 U.S.C. § 1683 et seq.