epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

December 21, 2021

Consumer Financial Protection Bureau
1700 G St. NW, Washington D.C. 20552

Re: Notice and Request for Comment Regarding the CFPB's Inquiry Into Big Tech Payment Platforms [Docket No. CFPB 2021-0017]

Dear Director Chopra:

The Electronic Privacy Information Center (EPIC) welcomes the opportunity to comment on the Consumer Financial Protection Bureau's (the Bureau) inquiry and efforts to bolster consumer privacy through this investigation of the data collection practices of the online payments industry. Financial technology firms should not be profiling, analyzing, or monetizing private information about Americans' day-to-day transactions; private financial information should remain private, regardless of the platform used to process transactions. We are encouraged by this inquiry into an historically opaque industry, espaecially given the sensitive nature of consumer financial data and the far-reaching consequences implicated by surveillance of that data. In addition, we applaud Director Chopra's proactive approach to closely examining the current state of privacy and consumer protection in the financial services industry and to examining the current state of the industry world-wide, particularly in China.

The example order significantly advances the Bureau's privacy, consumer protection, and competition goals as they relate to the online payments industry. However, EPIC strongly believes that the order should be supplemented with inquiries regarding: (i) the company policies that govern how data is used internally, (ii) the security protocols that companies put in place to protect consumer data, (iii) the notification regime activated when those protocols fail, and (iv) the extent to which consumers have a meaningful choice of payment platforms. EPIC also encourages the Bureau to formally extend its inquiry beyond the online payment platforms and to continue to investigate other entities with access to consumer financial data (many of which are likely to be uncovered within the scope of this initial inquiry).

I. Introduction and Scope

In 2017, the CFPB published nine principles to guide the consumer-authorized access and use of consumer financial account data. The Bureau based its principles on improving products and services, increasing competition in financial markets, and empowering consumers to take greater control of their financial lives, noting that "such access and use must be designed and implemented to serve and protect consumers."[1]

Many of these nine principles are echoed in our commentary below. In Section II, our discussion of data minimization and data siloing aligns with the Bureau's principle of Data Scope and Usability. We address data mapping in Section III, which significantly overlaps with the Bureau's principle of Effective and Efficient Accountability Mechanisms. Data security and mandatory notifications, which we discuss in Section IV, relate to several Bureau principles including: Security, Access Transparency, and Ability to Dispute and Resolve Unauthorized Access. Finally, in Section V, we discuss the need for greater oversight where consumers have no meaningful choice, which corresponds with many of the principles already listed, as well as Control and Informed Consent.

The Bureau's inquiry[2] raises important questions that demand attention now. One reporter recently observed a more than 200% increase in complaints regarding mobile or digital wallets since

[1] Bureau of Consumer Fin. Prot. (CFPB), *Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation*, at 3 (Oct. 18, 2017), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf [Consumer Protection Principles].

[2] CFPB, Notice and Request for Comment, n.1 (Nov. 5, 2021), available at https://www.federalregister.gov/documents/2021/11/05/2021-24176/notice-and-request-for-comment-regarding-the-cfpbs-inquiry-into-big-tech-payment-platforms (linking to https://files.consumerfinance.gov/f/documents/cfpb_section-1022_generic-order_2021-10.pdf [Example Order]).

the pandemic began.[3] Looking at the Bureau's current docket, the majority of comments come from consumers who were defrauded via these payment applications.[4] While not all of these complaints specifically implicate data privacy or security issues, these consumer harms are inevitable in the absence of robust enforcement. When companies fail to adequately inform consumers about what data they are collecting, how that data is being used or disclosed to others, and what security measures the company has implemented, the companies are exacerbating the risk of fraud, exploitation, manipulation, lack of choice, and unfairness. We expect the Bureau's investigation will raise many of these questions; our commentary below identifies a few areas in which the Bureau's example order seems to leave important questions unanswered.

Additionally, one note about scope. EPIC agrees with the Independent Community Bankers of America (ICBA) that the Bureau's investigation of consumer financial privacy should not end with this inquiry of online payment platforms.[5] We urge the Bureau to follow up on its recent inquiries by investigating data aggregators and other entities which collect, use, store, disclose,

---

[3] *See* Gage Goulding, *Hackers Purchase Passwords to Access Apps Like Venmo, CashApp & Drain Accounts*, NBC-2 (Oct. 7, 2021), https://nbc-2.com/news/2021/10/06/hackers-purchase-passwords-to-access-apps-like-venmo-cashapp-drain-accounts/. *See also* CFPB, Consumer Complaint Database, Mobile or Digital Wallet Complaints by date received by the CFPB, March 1, 2020 through December 21, 2021, available at https://www.consumerfinance.gov/data-research/consumer-complaints/search/?chartType=line&dateInterval=Month&date_received_min=2020-03-01&lens=Overview&product=Money%20transfer%2C%20virtual%20currency%2C%20or%20money%20service%E2%80%A2Mobile%20or%20digital%20wallet&searchField=all&tab=Trends. At its peak, monthly complaints increased by more than 640%, from 130 complaints in March 2020 to 971 complaints in April 2021. The fewest complaints filed since March 2020 occurred in September of 2020; during that month, 201 complaints were filed with the CFPB, a 55% increase over March figures. The CFPB reported 312 complaints in November 2021, or a 147% increase over March 2020 (and a more than 35% increase YOY). *See id.*

[4] More than 40 of 60 comments came from defrauded consumers, with an additional two comments from individuals addressing the issue without having fallen victim to a scam, as of December 15. *See* All Comments, Notice and Request for Comments Regarding the CFPB's Inquiry into Big Tech Payment Platforms, https://www.regulations.gov/docket/CFPB-2021-0017/comments (last visited Dec. 15, 2021).

[5] *See* Comments of Independent Community Bankers of America (ICBA), CFPB-2021-0017, at 2, 3, 4, available at https://www.regulations.gov/comment/CFPB-2021-0017-0059 (e.g. "Do not limit examinations to big tech payment platforms but also consider data aggregators and other entities which handle, store, and use consumer financial data.").

and/or sell consumer financial data.[6] EPIC would welcome the opportunity to engage the Bureau about investigating aggregators of consumer financial data, however the scope of this comment is limited to the Bureau's inquiry of online payment platforms as represented by the example order provided.

II. Data Minimization and Data Siloing

We are encouraged by the Bureau's interest in ensuring that data is only used for approved purposes.[7] We agree with the multiple commenters who urge the Bureau to consider mandating data minimization standards.[8] In particular, we echo the recommendations of Texas Appleseed that the

[6] The Bureau has compiled and shared some information, *see, e.g.*, *Consumer-authorized financial data sharing and aggregation: Stakeholder insights that inform the Consumer Protection Principles* (Oct. 18, 2017), available at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf [Stakeholder Insights Report]; *Bureau Symposium: Consumer Access to Financial Records* (July 2020), available at https://files.consumerfinance.gov/f/documents/cfpb_bureau-symposium-consumer-access-financial-records_report.pdf [Symposium Report], but many questions still remain unanswered.

[7] *See* Example Order, *supra* note 2, at ¶ 9(e) and 11(b) as this relates to data purportedly collected to combat fraud; at ¶ 14 and 15 for data purportedly used to improve service delivery (including developing, selling, and/or marketing the product); at ¶ 22-27 regarding surveillance-based advertising and targeted offers. This aligns with stakeholder feedback from the 2016 RFI. *See* Stakeholder Insights Report at 5 ("To limit these risks, stakeholders suggest that the Bureau could limit access to and the use of consumer financial data to the express purpose for which the consumer has authorized that access."). Both banks and credit unions cautioned the Bureau about "secondary uses" of consumer data in response to the CFPB's 2020 ANPR. *See, e.g.*, Comments of PNC, CFPB-2020-0034, at 8, available at https://www.regulations.gov/comment/CFPB-2020-0034-0042, ("These 'secondary uses,' as defined in the ANPR, are not reasonably expected by consumers. Any rules promulgated by the Bureau should require that secondary uses are conspicuously disclosed to consumers."); Comments of Credit Union National Association (CUNA), CFPB-2020-0034, at 6, available at https://www.regulations.gov/comment/CFPB-2020-0034-0036 ("As discussed above, credit unions and banks have limited tools available to discipline third parties who steal or abscond with consumer financial data. ….Further, direct access theoretically increases the risk that data will be shared beyond the level required for the primary purpose").

[8] *See, e.g.*, Comments of ICBA at 3 (urging the CFPB to require data minimization standards); Comments of Lieff Cabraser Heimann & Bernstein [Lieff Cabraser], CFPB-2021-0017, at 2, available at https://www.regulations.gov/comment/CFPB-2021-0017-0046 (details of Plaid settlement including data minimization). The Bureau recently addressed data minimization as "the general notion that data users only request, and data holders only share, consumer data necessary to perform the service described to and authorized by the consumer." *Consumer Access to Financial Records*, Advanced Notice of Proposed Rulemaking, CFPB-2020-0034, at 16 n 21, available at https://files.consumerfinance.gov/f/documents/cfpb_section-1033-dodd-frank_advance-notice-proposed-rulemaking_2020-10.pdf.

Bureau require companies to adhere to Collection Limitation, Use Limitation, and Purpose Specification principles.[9]

Data minimization applies at multiple levels: the external data collection level and the internal level of structuring at which teams (or even employees) are granted access to consumer data. We believe the Bureau's example order questions are sufficient to develop a general understanding of what data is collected and how it is used and shared externally. However, answers to the proposed questions might not reveal which individuals and departments within each company are able to access consumer data, and for what purposes, and might not reveal what measures each company has undertaken to ensure that data use is limited solely to the siloed purposes for which data has been collected.[10] EPIC agrees that there should be an automatic expiration on consent to disclose personal financial data, requiring periodic reconfirmation from consumers (both consumer advocates and Capital One proposed an annual expiration).[11]

We also urge the Bureau to consider the data security benefits of data minimization.[12] Data that was never collected cannot be compromised and limiting the number of parties with access to

[9] *See* Comments of Texas Appleseed, CFPB-2021-0017, at 18-19, available at https://www.regulations.gov/comment/CFPB-2021-0017-0060 (using "data minimization" as shorthand to refer to Fair Information Practice Principles including Collection Limitation, Use Limitation, and Purpose Specification and quoting FTC Commissioner Slaughter in urging a shift to data minimization rather than a focus on opt-in vs. opt-out consent).
[10] Bank Policy Institute (BPI) provides an illustrative example in its comments, at 3, available at https://www.regulations.gov/comment/CFPB-2021-0017-0072. ("For example, unless explicitly permissible by applicable law or regulation, a non-financial affiliate providing an e-commerce platform linking customers and merchants should be prohibited from using data or insights obtained from customer payment activity to market or price any other product or service targeting such customer.")
[11] See Symposium Report at 8; Comments of National Consumer Law Center (NCLC), CFPB-2020-0034, at 5, 9, 13, available at https://www.regulations.gov/comment/CFPB-2020-0034-0049; Comments of Capital One, CFPB-2020-0034, at 3, 6, 7, 8, available at https://www.regulations.gov/comment/CFPB-2020-0034-0077.
[12] The Bureau is familiar with the relationship between data minimization and data security from its recent efforts in this area. *See* Symposium Report at 6. BPI addresses this relationship in its comments as well. *See* BPI, at 5. ("…data minimization is a fundamental security principle: limiting the collection or dissemination of sensitive data reduces the consumer's risk of exposure.")

data correspondingly limits the means by which that data could be exposed. Security is further discussed in Section IV, *infra*.

III. Data Mapping

Data siloing is best maintained by mapping data-related processes, activities, and flows (referred to herein as "data mapping"). The Bureau should require companies to fully map data related to their payment systems.[13] This would include sources of data, categories of data, purposes for collection and use, who has access both internally and externally, what data is shared with and/or sold to whom, what systems integrations are currently in use (or are on the product roadmap), where data sits (e.g. internal servers, third-party servers, physical copies, etc.), and in what form (encrypted, pseudonymized, etc.). Sections B and C of the example order address the data fields themselves, as well as data sharing and retention practices, but they might not be sufficient to identify all data sources, integrations, or storage systems. The Bureau must have a complete picture of relevant industry practices in order to effectively ensure the privacy and security of nonpublic personal information about consumers held by these providers.

Moreover, consumers cannot be said to make an informed choice about what provider they choose to do business with, and what uses of their data they consent to, absent these kinds of disclosures. We agree with Consumer Action that consumers should be in control of their data, and

[13] The Bureau noted a similar observation among participants in its 2020 Symposium. *See* Symposium Report at 5 ("Several participants asserted specifically that data flows should be traceable; i.e., consumers should be able to see not just what data are being shared or how frequently, but which entities are handling it at various points in its journey from holder to end user. No participants disagreed with this assertion.").

consumer control requires consumers being sufficiently informed about a company's data practices.[14] We discuss consumer choice issues further in Section V, *infra*.

IV. Data Security and Mandatory Notifications

We are dismayed to see so little attention to data security in this inquiry, especially as data security is an issue of perennial concern for the Bureau.[15] Paragraph 50[16] of the example order addresses fraud prevention and notification, how a consumer can contact a company about fraud concerns, and a consumer's ability to regain access after their account has been or seems to be compromised. However, we do not think that this inquiry will adequately identify information about data breaches and data security practices unrelated to fraud.

Inadequate data security practices and inadequate breach notifications are particularly concerning given the broad range of data collected and analyzed in these systems, as the inquiry rightly points out.[17] While consumers often do not feel the pain of inadequate data security until it

[14] Comments of Consumer Action, CFPB-2021-0017, at 2, available at https://www.regulations.gov/comment/CFPB-2021-0017-0058. Meaningful consumer choice, and the absence of choice that often confronts consumers, is discussed in Section V, *infra*.

[15] *See, e.g.*, CFPB, *Mobile financial services: Summary of comments from the public on opportunities, challenges, and risks for the underserved*, at 54 (Nov. 2015), available at https://files.consumerfinance.gov/f/201511_cfpb_mobile-financial-services.pdf (Section 4.1, Security); Symposium Report at 6; Stakeholder Insights Report at 7, 10.

[16] Example Order, *supra* note 2, at 15-16.

[17] *See id.* at 8-27, 43-47. Additionally, the inquiry asks companies to distinguish between direct product data and indirect product data, further suggesting an expectation that there will be data aggregation and/or analysis occurring. *See id* at Definition 11 "Indirect Product Data", ¶ 10. Additionally, Texas Appleseed has recognized the use of "alternative data" by financial companies to assess consumer financial strength. *See* Texas Appleseed at 12. This is further-supported by a 2014 Upturn report. *See* Robinson and Yu, *Knowing the Score: New Data, Underwriting, and Marketing in the Consumer Credit Marketplace*, Upturn (Oct. 2014), available at https://www.upturn.org/static/files/Knowing_the_Score_Oct_2014_v1_1.pdf. *See also* Mikella Hurley and Julius Adebayo, *Credit Scoring in the Era of Big Data*, 18 Yale J.L. & Tech. 148 (2016), available at https://digitalcommons.law.yale.edu/cgi/viewcontent.cgi?article=1122&context=yjolt *(*"The credit scoring industry has experienced a recent explosion of start-ups that take an 'all data is credit data' approach, combining conventional credit information with thousands of data points mined from consumers' offline and online activities").

reaches the point of a fraudulent transaction, the root of the problem arises much earlier at a data protection level.[18]

This industry is not unique in its struggles with credential theft or bypassing authentication—however, the last two years in particular do not inspire confidence.[19] We agree with multiple commenters who recommend that the Bureau subject tech companies, data aggregators, and others that handle financial data to comparable data security standards as financial institutions.[20] ICBA suggested that the Bureau incentivize providers to improve their security protocols by holding them

[18] National Association of Federally-Insured Credit Unions (NAFCU) addressed a similar concern. Comments of NAFCU, CFPB-2020-0034, at 4, available at https://www.regulations.gov/comment/CFPB-2020-0034-0056 ("From the consumer's vantage, a third party's lack of appropriate safeguards may not be fully known until after the fact if data seeking entities are not subject to regular examinations like traditional financial institutions and data holding financial institutions cannot employ guardrails through contractual provisions.")

[19] *See, e.g.*, Zak Doffman, *PayPal 'Critical' Login Hack: New Report Warns You Are Now at Risk from Thieves,* Forbes (Feb. 22, 2020), https://www.forbes.com/sites/zakdoffman/2020/02/22/paypal-critical-login-hack-new-report-warns-you-are-at-risk-from-thieves-heres-the-reality/?sh=7f450e6b445e; Goulding *supra* note 3; Alexis Keenan, *Square's Cash App Vulnerable to Hackers, Customers Claim: 'They're Completely Ghosting You,'* Yahoo Finance (March 20, 2021), https://www.yahoo.com/now/squares-cash-app-vulnerable-to-hackers-customers-claim-113556593.html; Charlie Osborne, *Researchers Discover Bypass 'Bug' in iPhone Apple Pay, Visa to Make Contactless Payments,* ZDNet (Sept. 29, 2021), https://www.zdnet.com/article/researchers-discover-bypass-bug-in-iphone-visa-apple-pay-to-make-contactless-payments/. Public Citizen's comments note the recent attraction of cryptocurrency to hackers and scammers. *See* Comments of Public Citizen, CFPB-2021-0017, at 4, available at https://www.regulations.gov/comment/CFPB-2021-0017-0071 ("In a five-month period ending March 2021, the Federal Trade Commission reported 7,000 cryptocurrency scams covering some $80 million in reported losses. That is 12 times the number of scams reported during the same period a year earlier, with a 1000 percent greater estimated loss."). FinCEN remarked on a similar trend as early as 2019. *See* Prepared Remarks of FinCEN Director Kenneth A. Blanco, delivered at the Federal Identity (FedID) Forum and Exposition (Sept. 24, 2019), available at https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-federal-identity-fedid ("In some cases, cybercriminals appear to be using fintech data aggregators and integrators to facilitate account takeovers and fraudulent wires. By using stolen data to create fraudulent accounts on fintech platforms, cybercriminals are able to exploit the platforms' integration with various financial services to initiate seemingly legitimate financial activity while creating a degree of separation from traditional fraud detection efforts.")

[20] *See, e.g.*, Lieff Cabraser at 2 (noting a recent order requiring Plaid to maintain a webpage describing its security practices); NAFCU at 2, 4 (urging the Bureau to require tech companies handling consumer financial data to manage privacy and security to the same standards that apply to credit unions and other regulated financial institutions). Several commenters offered similar recommendations in their comments in the Bureau's 2020 ANPR docket. *See, e.g.*, Comments of BPI, CFPB-2020-0034, at 2; MasterCard, at 5-6; American Financial Services Association, at 3; American Bankers Association, at 3; Capital One, at 4, 13, 20-23; Navy Federal Credit Union at 3 (urging the Bureau to require GLBA-style protections but only as relates to security events), and PNC at 4-5 (urging protections based on the Federal Financial Institutions Examinations Council examination guidance).

liable for making consumers whole.[21] We are agnostic to this approach as it relates to fraudulent transactions—however, because many other data-related harms are unlikely to result in quantifiable relief to consumers,[22] we would not expect such an incentive structure to motivate companies to adequately protect all types of consumer data.

We urge the Bureau to ensure that providers implement proper protocols to protect the data they have amassed about their consumers (e.g. using access controls, encryption, etc.).[23] We also encourage the Bureau to request examples from each provider of a hypothetical cyber incident that would trigger a notification to an impacted consumer, one that would trigger a notification to an enforcement entity but not to any consumer, and one that would trigger an internal investigation with no external notification whatsoever. This should help the Bureau and the public to better understand at what level of incident consumers are typically informed about the security of their data and enables the Bureau to set standards adjusting this level, if necessary.

V. Greater Oversight Where Consumers Have No Meaningful Choice

Although there is value in innovation, both competition and consumer protection demand that consumer choice—where choice is relevant—be based on clear, accurate, and transparent

[21] *See* ICBA at 5 ("While these incidents vary considerably in attack type and complexity, one constant remains true throughout – non-bank entities must have the same stringent protections in place as financial institutions.")
[22] *See, e.g.*, TransUnion LLC v. Ramirez, 141 S. Ct. 2190 (2021) (finding no concrete harm to extent that credit reporting agency did not disclose to third parties wrongful identification of thousands of consumers as being on Office of Foreign Assets Control list).
[23] EPIC made similar recommendations to the FTC regarding the Safeguards Rule for data privacy of financial institutions. Find a more robust list of examples of baseline security practices we would encourage the CFPB to engage these companies about in that commentary. *See EPIC Comments on FTC Safeguards Rule* (Aug. 1, 2019), available at: https://epic.org/epic-comments-on-ftc-safeguards-rule/. This commentary to the FTC also addresses data minimization, discussed in Section II, *supra*.

information. The Bureau recognized this in its nine consumer protection principles.[24] If a consumer is not aware of a company's data collection and usage practices, that consumer cannot be said to have made an informed choice about whether to do business with that company.[25] Similarly, a consumer's decision to terminate business with a company must be accompanied by an easy method to terminate use of that consumer's data by that company's third party partners.[26] The Bureau should also prohibit platforms from formalizing privacy as a paid service.[27]

While there is a value to consumer data, it cannot become a bargaining chip allowing companies to place a price on privacy. This would have obviously disparate consequences for consumers who can "afford" privacy as opposed to those who cannot, creating a privacy right that exists solely for the wealthy. To address this issue, we urge the Bureau to inquire about any fees or

[24] *See* Consumer Protection Principles at 1 ("The Principles express the Bureau's vision for realizing a robust, safe, and workable data aggregation market that gives consumers protection, usefulness, and value."). The Bureau also spoke to this in its Stakeholder Insights Report, at 6. Two solutions were proposed to address this potential problem: effective disclosures and easy opportunities to confirm, revoke, and/or modify access to their data. *See id.*

[25] Texas Appleseed has outlined five sets of questions that are a good start to what companies should be communicating to consumers in an easy-to-find and easy-to-understand manner. *See* Texas Appleseed, at 21; *see also* Lieff Cabraser at 2 (settlement requiring enhanced disclosures). NCLC has provided several troubling examples of how a consumer's data may be used without their knowledge. *See* Comments of NCLC, CFPB, 2020-0034-0049, at 16 ("…deposit accounts can include a host of sensitive information, including what neighborhoods and stores the consumer shops in.…Thus, use of account data could lead to racial or other disparities not based on the individual's credit risk."), at 21-22 (discussing the prevalence and problematic aspects of Experian's ConsumerView product, and recommending that a consumer's access rights include the ability to discover which covered persons have accessed that consumer's information through ConsumerView).

[26] *See* Comments of PNC, CFPB-2020-0034, at 8, available at https://www.regulations.gov/comment/CFPB-2020-0034-0042 (quoting Federal Reserve Board Governor Lael Brainard "[w]hen a consumer deletes a fintech app from his or her phone, it is not clear this would guarantee that a data aggregator would delete the consumer's bank login and password, nor discontinue accessing transaction information." And urging the CFPB to mandate "a readily accessible and transparent way [for consumers] to revoke their access authorizations" to data aggregators and data users with significant volumes of consumer data).

[27] For example, the "right of no retaliation" under the CCPA. *See* Müge Faziologlu, *Top-10 operational impacts of the CPRA: Part 8 – Rights to delete, no retaliation and children's privacy*, IAPP (Feb. 16, 2021), available at https://iapp.org/news/a/top-10-operational-impacts-of-the-cpra-part-8-rights-to-delete-no-retaliation-and-childrens-privacy/ (citing to CCPA/CPRA Section 1798.125, available at https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.125).

discounts that platforms offer in exchange for additional permissions from consumers regarding the collection, use, sharing, selling, and/or storing of their data.[28]

Even where a consumer is properly informed, barriers of price or inconvenience may make alternatives effectively inaccessible and therefore irrelevant to the consumer's choice.[29] In many instances payment platforms act as two-sided markets in which merchants get to make an informed choice about the platform(s) they will use, but consumer choice is limited to the merchant, not extending to the payment platform.[30] The Bureau's oversight is especially important where consumers are presented with this kind of take-it-or-leave-it at checkout.

Conclusion

Once again, we applaud the ongoing efforts of the Bureau and Director Chopra to advance consumer privacy and the thoughtful approach to this request for comment and the drafted order. We urge the Bureau to supplement its investigation of online payment platforms as outlined in the example order with inquiries regarding data siloing, data security, and data minimization, and to continue its important work regarding other entities with access to consumer data, such as data aggregators.

[28] Question 3b of the Bureau's Example Order asks about how companies encourage consumer usage of their products, but this question is not specific to data-related permissions. Capital One also addresses this issue from a "cost of data access" perspective. Comments of Capital One, CFPB-2020-0034, at 19. The Bureau's 2020 Symposium Report addressed a different form of coercive disclosure, at 6 ("One advocate said consumers need to have some rights against being required to provide data as a condition to achieve certain ends (such as employment, or to procure a loan where traditional data sources are sufficient to underwrite the applicant).")

[29] *See* Robert Gellman, *Privacy, Consumers, and Costs: How the Lack of Privacy Costs Consumers and Why Business Studies of Privacy Costs are Biased and Incomplete*, March 2002, Section III(A), available at https://archive.epic.org/reports/dmfprivacy.pdf.

[30] Consumer Action has also called attention to this issue in its comments. *See* Consumer Action at 2.

Respectfully submitted, this the 21st day of December 2021, by

Chris Frascella
Law Fellow

Calli Schroeder
Global Privacy Counsel

Tom McBrien
Law Fellow

Alan Butler
Executive Director and President

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036