November 20, 2019

Congressman Stephen F. Lynch
Task Force on Financial Technology
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC 20515

Congressman Tom Emmer
Task Force on Financial Technology
House Committee on Financial Services
2129 Rayburn House Office Building
Washington, DC, 20515

Congressman Lynch and Congressman Emmer,

We applaud the Task Force on Financial Technology ("Task Force") for holding this timely hearing on the role of technology and data practices at scale in financial services.

Digital technology, and the data that drives it, has provided numerous innovative products and services that have benefited the American public. Internet-related tech innovation has been so successful that consumers and users now rely heavily on internet services and platforms in nearly every facet of their daily lives. Despite the clear benefits, the pervasiveness of these services and platforms means there is the potential for significant harms that negatively affect users at scale.

When the personal data that fuels the online ecosystem is misused or abused, it can lead to a host of harms, ranging from physical and financial injury to lost opportunity to digital redlining. As Federal Trade Commission ("FTC") Commissioner Rebecca Kelly Slaughter has noted, these harms disproportionately affect vulnerable and marginalized communities.[1] While such harms are well documented,[2] any advances in federal law to provide increased consumer protections have failed to keep pace. With no comprehensive federal privacy law in existence, there is no oversight, safeguards, or accountability for how companies collect, use, or protect the often-sensitive personal data they collect from internet users.

Further, a handful of platforms have established a level of dominance in various online services that raise serious competition concerns. These platforms appear poised to leverage existing dominance online to allow them to enter other markets, including financial services. In fact, some dominant platforms have already entered (or announced plans to enter) the space. The

---

[1] *See* Remarks of Commissioner Rebecca Kelly Slaughter, *The Near Future of U.S. Privacy Law*, Silicon Flatirons (Sept. 6, 2019), https://www.ftc.gov/system/files/documents/public_statements/1543396/slaughter_silicon_flatirons_remarks_9-6-19.pdf.

[2] *See, e.g.*, Public Knowledge Comments to the National Telecommunications and Information Administration, Docket No.: 180821780-8780-01 (Nov. 9, 2018), https://www.publicknowledge.org/documents/public-knowledge-ntia-consumer-privacy-comments/; Lawyers' Committee for Civil Rights Under Law et al., *Letter to Congress on Civil Rights and Privacy* (April 19, 2019), https://lawyerscommittee.org/wp-content/uploads/2019/04/Letter-to-Congress-on-Civil-Rights-and-Privacy-4-19-19.pdf.

FTC, Department of Justice, and numerous Congressional committees are currently investigating potential competitive harms caused by dominant platforms and whether existing antitrust laws are sufficient to address dominance and market power in the digital economy. Several of these companies have also demonstrated carelessness or disregard for how they treat sensitive consumer data.[3]

Public Knowledge has long advocated for the importance of sector-specific regulation to protect consumers, promote competition, and further the public interest, including most recently in the context of dominant digital platforms.[4] The Committee should be commended for its formation of the Task Force and for holding important hearings on financial technology data practices to build the public record and to identify ways to strengthen consumer protections in the financial sector. In this letter, we raise certain policy concerns that we identify in the digital platform space, particularly as it relates to financial services.

Privacy Concerns

Thousands of data brokering companies exist that collect thousands of data points on each individual in their data set, including highly sensitive information about health status and economic stability.[5] For years, data brokers have operated in the shadows, free of meaningful government oversight, while they profit off of vast troves of consumer data. Because these brokers do not have a direct business relationship with consumers, they are often trafficking in personal data without consumer knowledge or consent. While some brokers offer consumer choices around how the broker may use personal data, the FTC has found a "fundamental lack of transparency about data broker industry practices." The Senate Commerce Committee has reported that data brokers classify consumers in categories like "Ethnic Second-City Strugglers" and "Tough Start: Young Single Parents."[6] They can use these profiles to engage in harmful marketing practices like predatory lending and other digital redlining activities that disproportionately impact marginalized communities. Many data brokers are quite small, but some of these small entities are the most egregious privacy violaters. For example, last year, Exactis, a data broker with only 10 employees was reported to have exposed the data of 230 million consumers.[7] Government oversight of the data broker ecosystem is sorely needed to establish transparency and accountability and to protect user rights.

---

[3] *See*, *e.g.*, Federal Trade Commission, *FTC Approves $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook*, ftc.gov (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/08/ftc-approves-final-consent-order-settling-charges-background; Federal Trade Commission, *Privacy and Data Security Update: 2018*, https://www.ftc.gov/system/files/documents/reports/privacy-data-security-update-2018/2018-privacy-data-security-report-508.pdf.

[4] *See generally*, Harold Feld, *The Case for the Digital Platform Act: Market Structure and Regulation of Digital Platforms*, Roosevelt Institute (May 2019), https://www.digitalplatformact.com/.

[5] *See* Aliya Ram and Madhumita Murgia, *Data Brokers: Regulators try to rein in the "privacy deathstars"*, Financial Times (Jan. 7, 2019), https://www.ft.com/content/f1590694-fe68-11e8-aebf-99e208d3e521. (Paywall).

[6] *See* Committee on Commerce, Science, and Transportation, *A Review of the Data Broker Industry: Collection, Use, and Sale of Consumer Data for Marketing Purposes* (Dec. 18, 2013), https://www.commerce.senate.gov/services/files/0d2b3642-6221-4888-a631-08f2f255b577.

[7] *See* Keri Paul, *What is Exactis—and how could it have leaked the data of nearly every American?*, MarketWatch (June 29, 2018), https://www.marketwatch.com/story/what-is-exactisand-how-could-it-have-the-data-of-nearly-every-american-2018-06-28.

As large tech companies like Apple and Facebook enter into the financial services market, more transparency and scrutiny is essential regarding the data that drives decisions by financial services providers. Companies are now using artificial intelligence technology based on deep machine learning to generate important decisions on creditworthiness. As was highlighted in an article earlier this year on Motherboard, companies like, "ZestFinance, Lenddo, SAS, Equifax, and Kreditech are selling their AI-powered systems to banks and other companies, to use for their own creditworthiness decisions."[8] These decisions, however, are not transparent, nor is it clear what data these companies are using in their deep learning AI to make credit decisions. Unlike other credit scores, there is no way to appeal these decisions, nor is it possible to learn the constituent parts that make up this new, secretive creditworthiness score.

Decisions on creditworthiness have been historically discriminatory against people of color, women, and members of the LGBTQ community. A recent paper highlighted the fact that as recently as 2018, face-to-face and fintech lenders charge, "otherwise-equivalent Latinx/African-American borrowers 7.9 (3.6) bps higher rates."[9] This recent data raises numerous concerns that are worthy of the Committee's attention, including:

- What data is being used by these companies and how did they get it?
- How has the underlying data been tested, and have the requisite procedures been put into place to make sure that this data is not replicating historical inequities in the financial sector?
- What protections or means of appeal will be given to consumers to find out about secret credit scores and correct inaccuracies?
- Are the results that the machine learning AI is reaching explainable to the average consumer?

We urge the Task Force and the Committee to investigate whether the financial industry has thought of and instituted these necessary consumer protections.

Any privacy regime that Congress adopts to further protect user rights should not be based on data ownership. To the extent that data ownership even addresses the privacy problem—a tenuous connection—data ownership should not be grounded in copyright law, and new (sui generis) data ownership rights are likely to create practical and legal confusion that will not meaningfully protect consumer privacy. Privacy is a basic consumer protection issue best resolved through comprehensive federal privacy legislation. As discussed below, to achieve the worthy goal of data sharing to promote competition or scientific research, lawmakers should instead look at imposing data portability and interoperability mandates on certain online platforms to give users true choice and control over what to do with their data.

The asymmetric information and power imbalances that plague the current data ecosystem would persist under a data ownership regime. Individuals would not have the information to understand what they are selling, or the bargaining power to get a fair price. Aside from the

---

[8] Rose Eveleth, *Credit Scores Could Soon Get Even Creepier and More Biased*, Motherboard (June 13, 2019), https://www.vice.com/en_us/article/zmpgp9/credit-scores-could-soon-get-even-creepier-and-more-biased.

[9] Robert Bartlett et al., *Consumer-Lending Discrimination in the FinTech Era, National Bureau of Economic Research*, Working Paper No. 25943 (June 2019) https://www.nber.org/papers/w25943.

means of compensation, it's hard to see how this is any different from the current failed "notice and choice" privacy regime. Consumers already face the impossible task of reading and understanding[10] countless opaque and lengthy privacy policies (read: contracts, often filled with legalese) that outline the scope of how their information is used by the companies that profit off of data, many of which we don't have any direct contact with. Note that individuals have zero leverage to negotiate these privacy policies and terms of use. This would not change under a data ownership regime.

In general, Congress should not create incentives for individuals to accept payment in exchange for signing over their personal data, which could include incredibly privacy-invasive information (such as biometric, health, and precise geolocation data) as well as seemingly non-sensitive information that could be used by trained algorithms to infer intimate information. Such arrangements could lead to disparate impacts affecting members of low-income and other marginalized communities who might not be so privileged to sell or lease their data sparingly. Pay-for-surveillance will surely be popular among data-hungry businesses. Companies have been willing to pay users, including teens, to collect user data,[11] and these companies have the leverage to change the terms of the contracts to the detriment of users at their whim. Congress should take steps to address this imbalance, not facilitate it.

Competition Concerns

Incumbent online platforms benefit from natural economic characteristics that protect their market dominance, causing a slew of competition policy concerns. Companies like Amazon and Facebook benefit from "network effects," meaning that as the number of users goes up, so do the benefits to users of being on the platform. In other words, all else equal, you benefit more from joining the social media platform your friends are on than you do by joining a newer or smaller social network without your friends. Many digital platforms benefit from economies of scale because their software has almost no marginal cost for adding users. Many digital platforms also benefit from economies of scope because data is much more valuable when aggregated and analyzed as a group instead of viewed as single pieces of information. If Google provides an individual's e-mail and maps, including traffic data, then Google can tell that individual when to leave for their flight so they arrive on time. By contrast, a competitor's mapping application that doesn't have access to the user's e-mail isn't even aware there is a flight to catch. Incumbent online platforms also benefit from behavioral ticks like "bounded rationality," where consumers use shortcuts rather than carefully choosing the best option each time. Most consumers don't check multiple online stores every time they buy oven mitts—they simply go to the same store each time. Similarly, users don't use Bing every few months to see how it matches up with Google's search engine—they just keep returning to Google Search.

The combination of these characteristics makes it incredibly difficult for small companies to grow and new companies to compete against incumbent dominant platforms. Without dynamic

[10] *See* Kevin Littman Navarro, *We Read 150 Privacy Policies. They Were An Incomprehensible Disaster*, New York Times Opinion, (Accessed November 20, 2019), https://www.nytimes.com/interactive/2019/06/12/opinion/facebook-google-privacy-policies.html.
[11] *See* Rachel Lerman, *Facebook launching app that pays users for data on app usage*, APNews (June 11, 2019), https://apnews.com/289df88fb145472198e54024b5c2f6a8.

competition, where new competitors actually pose a threat to the market position of incumbents, economists expect less innovation, higher prices, and lower product quality. Some harms are more obvious: less consumer choice and limited opportunity for entrepreneurship. The potential for these harms exists in the financial sector where incumbent platforms like Facebook and others have sought to expand their business into financial services. To the extent that dominant platforms have or plan to enter into the financial services market, we believe that the Task Force and the Committee should closely scrutinize the ways in which such arrangements can have anti-competitive effects.

An important tool that can be applied to promote competition in the digital platform space is interoperability. In simple terms, interoperability means enabling different systems and organizations to communicate with each other and work together. Interoperability achieves several interrelated benefits for consumers and the economy. First, interoperability gives consumers practical control over their personal data. Consumers should not feel stuck with a bad service because it has all of their data and their friends' data. Second, interoperability encourages innovation in both incumbents, who have to improve their services to keep users in the original platform, and challengers, who have a fighting chance to develop successful new products and services. Network effects can "lock-in" users—even when users are frustrated by a platform and would like to leave; users may be prevented from leaving due to the difficulties of switching to another platform and/or the network benefits of transacting with other users on the dominant service. To the extent that dominant platforms are operating in or are soon to enter the financial sector, the way in which they interoperate with competing services, like for example by disallowing competing forms of payment on a platform or network, should be closely scrutinized.

Conclusion

We urge the Task Force to investigate the privacy and competition concerns outlined above as you consider policies to address problems in the digital marketplace. Thank you again for your attention to these important issues.

Sincerely,

/s/ Dylan Gilbert
Dylan Gilbert
Policy Counsel
Public Knowledge

CC: Chairwoman Maxine Waters and Ranking Member Patrick McHenry