CENTER FOR DEMOCRACY & TECHNOLOGY

Via submissions@banking.senate.gov

March 15, 2019

Chairman Mike Crapo & Ranking Member Sherrod Brown
Members of the United States Senate Committee on Banking, Housing and Urban Affairs
534 Dirksen Senate Office Building
Washington, D.C. 20510

RE: Improving Data Privacy, Protection and Collection Practices in Financial Data

Dear Chairman Crapo and Ranking Member Brown:

The Center for Democracy & Technology (CDT) is a non-profit, non-partisan technology advocacy organization based in Washington, D.C., that works to promote democratic values by shaping technology policy and architecture, with a focus on the rights of the individual. CDT supports laws, corporate policies, and technological tools that protect privacy and security online. We write today to offer several ideas for where the Committee might explore how current legal and regulatory tools are advancing financial data privacy and access.

The Committee has asked several questions as to what should be done through legislation, regulation, or implementation of best practices that would improve disclosures made to consumers (Question 2) and their subsequent control over the use of financial data (Question 3). Separately, it asks what should be done about data brokers (Question 5). Our comments address these three key issues.

> *(2) What could be done through legislation, regulation, or by implementing best practices to ensure that financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) provide adequate disclosure to citizens and consumers about the information that is being collected about them and for what purposes?*

Disclosures are one of the primary mechanisms by which the Gramm-Leach-Bliley Act (GLBA) attempts to govern the privacy practices of financial institutions, but the end result is that the regulation of financial data privacy operates under an untenable framework of "notice and choice."

It is often stated that financial services are highly regulated. This is accurate in certain respects, but it is an overstatement with respect to the privacy interests of individuals in their financial data. The Gramm-Leach-Bliley Act (GLBA) was enacted to modernize financial services, specifically by permitting the mergers of banks, stock brokers, and insurers. Removing these regulations raised concerns that new financial institutions would have increased access to

otherwise nonpublic financial information, which Congress recognized required security safeguards and additional transparency to consumers.[1]

This eventually manifested itself in GLBA's Safeguards Rule and Financial Privacy Rule.[2] While the Safeguards Rule may meaningfully regulate the data security of financial information, the Financial Privacy Rule is a "privacy" rule in name only. Among other provisions, it directs financial institutions to (1) provide a written, annual disclosure of their privacy practices and (2) inform customers of their ability to opt-out from a limited amount of sharing of nonpublic personal information. Congress's justification, at the time, was that such disclosures would empower consumers because "if you do not like the bank's policy, you can take your business somewhere else."[3]

Unfortunately, this sort of "notice and choice" framework does not work, as CDT has most recently explained to the Senate Judiciary Committee this week.[4] Banks can easily share information if -- and when -- consumers fail to opt out or if the purpose of sharing falls under one of GLBA's many statutory exceptions, including joint marketing ventures and affiliate sharing. Even where consumers take the time to read their bank's privacy policies, they have little practical control over how their financial information is shared with third parties, and the GLBA arguably incentivizes sharing among affiliates.[5]

Bank privacy policies have become more of a burden than any educational benefit. Congress itself acknowledged this when it amended GLBA to require financial regulators to propose a model disclosure form that would allow consumers to easily compare privacy practices across different financial institutions.[6] This ubiquitous model notice, while well-intentioned, has not improved the situation. The model notice permits financial services to pick from a menu of different options to describe their practices, and the generalities are such that even privacy-conscious consumers are left confused as to (1) how their data is used, (2) what data is shared and (3) with whom.[7]

---

[1] For an overview of the law's history, *see* Jolina C. Cuaresma, *The Gramm-Leach-Bliley Act*, 17 Berkeley Tech. L.J. 497 (2002).
[2] 15 U.S.C. §§ 6801–6809.
[3] 145 CONG. REC. S 13,883, 13,913 (1999) (statement of Sen. Gramm).
[4] Statement of Michelle Richardson, Director, Privacy & Data, Center for Democracy & Technology before the United States Senate Committee on the Judiciary (Mar. 12, 2019), *available at* https://www.judiciary.senate.gov/meetings/gdpr-and-ccpa-opt-ins-consumer-control-and-the-impact-on-competition-and-innovation. *See also Notice and Choice Are No Longer a Choice*, Center for Democracy & Tech. (Mar. 1, 2019), https://cdt.org/blog/notice-and-choice-are-no-longer-a-choice/.
[5] *See* Cuaresma, *supra* note 1, at 512-13.
[6] Press Release, Federal Regulators Issue Final Model Privacy Notice Form (Nov. 17, 2009), https://www.ftc.gov/news-events/press-releases/2009/11/federal-regulators-issue-final-model-privacy-notice-form.
[7] Kashmir Hill, *Amazon and Chase Are Still Confusingly Opaque About What They Do With Your Credit Card Data*, Gizmodo (Feb. 25, 2019), https://gizmodo.com/amazon-and-chase-are-still-confusingly-opaque-about-wha-1832351497.

Rapid innovation in mobile banking has amplified this challenge. Many financial institutions are now required to have multiple privacy notices: mobile app stores require them, state laws have mandated that websites have privacy policies, and these are above and beyond what is already required of financial institutions under GLBA (or, in some situations, the Fair Credit Reporting Act).[8] Consumers cannot meaningfully understand what practices apply to which policies, which is why CDT has called on Congress to put in place meaningful limits on the secondary uses of information through legislation. Our federal privacy legislative proposal does not directly address financial information, but we also recognize the need to reassess our existing sectoral privacy requirements, including GLBA.[9]

(3) *What could be done through legislation, regulation, or by implementing best practices to give citizens and consumers control over how financial regulators and private financial companies (including third-parties that share information with financial regulators and private financial companies) use consumer data?*

Again, we would reiterate that individual control over financial data will not result in systemic change to how financial institutions collect, use and share our data. However, at the same time, consumers should be given more meaningful controls over their financial information *and* how to utilize this data for themselves.

While everyone generally agrees that individuals should be able to access and port, or move, their financial data, stakeholders have different views on implementation and ease of use. For instance, Section 1033 of the Dodd-Frank Act codifies the right of consumers' to access their financial data, but it is unclear the extent to what extent this right extends to third-party apps.[10] As financial technology firms and other intermediaries work on technical and policy solutions,[11] Congress could weigh in.

Congress' view is particularly important in light of recent regulatory inquiries launched at the Consumer Financial Protection Bureau and the Department of the Treasury. The CFPB's inquiry, for instance, focused on access rights to both accounts and account-related data and how these rights impact individual choice and control. However, aside from the CFPB's development of

[8] The American Express Privacy Center, for example, highlights an online privacy statement and presents a link to additional privacy notices, as required by law. Every large financial institution is required to offer myriad policies like this. American Express Privacy Center, https://www.americanexpress.com/us/legal-disclosures/privacy-center.html (last visited Mar. 13, 2019).

[9] CDT Federal Baseline Privacy Legislation Discussion Draft, Section 10(3), *available at* https://cdt.org/insight/cdts-federal-baseline-privacy-legislation-discussion-draft.

[10] For instance, it is unclear whether Section 1033 should be expanded beyond direct consumer-bank relationships; this access right may also be in tension with data security requirements that limit access. For an overview, *see* Mary Wisniewski, *The data access debate is about to get a lot more interesting*, American Banker (Jan. 27, 2017), https://www.americanbanker.com/news/the-data-access-debate-is-about-to-get-a-lot-more-interesting.

[11] Penny Crosman, *Big banks, aggregators launch group to hash out data-sharing issues*, American Banker (Oct. 18, 2018), https://www.americanbanker.com/news/big-banks-aggregators-launch-group-to-hash-out-data-sharing-issues. The Financial Data Exchange is largely focused on technical challenges rather than policy matters, however.

"Consumer-Authorized Financial Data Sharing and Aggregation Principles" in 2017, there has not been clear instruction from financial regulators.[12]

There is tremendous potential for innovation in financial services to deliver better customer experiences and greater control their financial planning.[13] One idea would be encourage banks to display which services and applications have access to account data in a centralized location. This could also promote granular controls. For example, combined with the use of authorization protocols, users could pick and choose what permissions to grant (for example, permissioning access to financial transactions but not bank balances) and easily revoke access at any time. This functionality could also be augmented by improving information flows during user onboarding when accounts are linked together, offering displays about what types of data permissioned parties are accessing, for what purpose, and for what duration in the dashboard itself.

This future requires confronting both policy and technical challenges. Financial institutions, fintech providers, and other third parties not only have to work together, but resolve liability considerations and reconcile data security imperatives. While there have been some early partnerships, these one-off agreements and bank-specific APIs may actually splinter the market and confuse consumers.

If industry collaboration cannot catalyze better experiences around financial data sharing,[14] legislative and regulatory action could provide needed guidance. Efforts such as the UK's Open Banking Standard, for example, have promoted standardized open APIs — with a dedicated eye to protecting user privacy and security.[15] An API-approach requires protections against oversharing and other data use concerns and will also require strong authentication protocols like OAuth, which might also include a permissions system to facilitate transparency and control over user's data. Lessons may also be learned from the EU's revised Payment Services Directive (PSD2),[16] which may promote innovation and facilitate both "Account Information Service Providers" (like the Mint financial aggregator and planning app) and the use of account access via API.

---

[12] Press Release, CFPB Outlines Principles For Consumer-Authorized Financial Data Sharing and Aggregation (Oct 18, 2017), https://www.consumerfinance.gov/about-us/newsroom/cfpb-outlines-principles-consumer-authorized-financial-data-sharing-and-aggregation/.

[13] *Financial Dashboards: Enhancing User Control Outside a Traditional "Privacy Dashboard"*, Center for Democracy & Technology (Sept. 27, 2017), https://cdt.org/blog/financial-dashboards-enhancing-user-control-outside-a-traditional-privacy-dashboard/.

[14] Financial Data Exchange, https://financialdataexchange.org/; *see also* CFSI's Consumer Data Sharing Principles: A Framework for Industry-Wide Collaboration (Oct. 2016), https://s3.amazonaws.com/cfsi-innovation-files/wp-content/uploads/2017/01/19192549/2016-Consumer-Data-Sharing-CDAWG-white-paper-Final.pdf.

[15] *E.g.*, Open Banking Standard, https://www.openbanking.org.uk/providers/standards/.

[16] Payment Services Directive 2, Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (Text with EEA relevance), *available at* https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32015L2366.

(5) What could be done through legislation, regulation, or by implementing best practices so a consumer can easily identify and exercise control of data that is being (a) collected and shared by data brokers and other firms and (b) used as a factor in establishing a consumer's eligibility for credit, insurance, employment, or other purposes.

Data brokers, including the three credit reporting agencies, continue to be a mystery to average Americans.[17] Congress should act on recommendations made by the Federal Trade Commission in 2014 and build upon protections and transparency requirements placed on data brokers by Vermont.

Unchecked data collection has costs, which are too often borne by the most vulnerable communities in our society. In 2013, the Senate Commerce Committee issued a detailed report highlighting how data brokers identified financially vulnerable populations in categories like "Rural and Barely Making It" or "Ethnic Second-City Strugglers."[18] The committee warned that data brokers "operate behind a veil of secrecy," a situation that a follow-up report from the World Privacy Forum cautioned "hides racism, denies due process, [and] undermines privacy rights."[19]

In 2014, the Federal Trade Commission (FTC) investigated nine data brokers that provide marketing products, risk mitigation products, and people search products, and concluded that these companies collect increasingly diverse pools of data from numerous sources, largely without consumers knowledge and that intra-broker trading was common.[20] The FTC offered a number of potential legislative recommendations to Congress, including suggesting the creation of a centralized mechanism, like an online portal, where data brokers could "identify themselves, describe their information collection and use practices, and provide links to access tools and opt outs."[21] However, despite efforts such as Senator Markey's "Data Broker Accountability and Transparency Act,"[22] Congress has not further considered the FTC's recommendations, leaving states to attempt to police data brokers by themselves.

---

[17] In the aftermath of the 2017 Equifax breach, more than one consumer confused Equifax with Experian.

[18] Senate Commerce Committee, Oversight of Oversight and Investigations, Majority Staff, 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/public/_cache/files/0d2b3642-6221-4888-a631-08f2f255b577/AE5D72CBE7F44F5BFC846BECE22C875B.12.18.13-senate-commerce-committee-report-on-data-broker-industry.pdf.

[19] Pam Dixon & Robert Gellman, The Scoring of America: How Secret Consumer Scores Threaten Your Privacy and Your Future, World Privacy Forum (Apr. 2, 2014), https://www.worldprivacyforum.org/2014/04/wpf-report-the-scoring-of-america-how-secret-consumer-scores-threaten-your-privacy-and-your-future/.

[20] Data Brokers: A Call For Transparency and Accountability: A Report of the Federal Trade Commission (May 2014), https://www.ftc.gov/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014.

[21] *Id.*

[22] *E.g.*, AkinGump, *Markey, Democrats Introduce Data Broker Bill* (Mar. 6, 2015), https://www.akingump.com/en/experience/practices/corporate/ag-deal-diary/markey-democrats-introduce-data-broker-bill.html.

CENTER FOR DEMOCRACY & TECHNOLOGY

In May 2018, Vermont enacted H 764, which requires data brokers to provide more information about what they collect; put in place reasonable security procedures; avoid using data for stalking, committing fraud, or engaging in illegal discrimination; and, importantly, register with the Vermont secretary of state in order to create a centralized database for the public to see broker-contact information, purchaser credentialing, recent security breaches, and any options to opt out of data collection. Importantly, these were all recommendations made by the FTC five years ago.

CDT supported these legislative recommendations.[23] While we believe a comprehensive privacy proposal is ideal, data brokers present a particular challenge. As the FTC report acknowledges, defining the different categories of and business models that make up data brokers is challenging. Our federal legislative privacy proposal defines data brokers as commercial entities primarily engaged in the licensing or selling of personal data of individuals with whom they have no direct relationship; it also includes several provisions directly related to data brokers, including the creation of a federal registry and restrictions on unlawful discrimination.[24] Congress must acknowledge the basic fact, as Vermont does, that few Americans are "aware that data brokers exist, who the companies are, or what information they collect, and may not be aware of available recourse."[25]

--

Thank you for the opportunity to comment as this Committee explores how to improve the privacy of Americans' financial information. We hope these comments can help shape activities in Congress, and CDT looks forward to engaging further on these issues. Please do not hesitate to reach out with any questions to 202.407.8812 or via email at jjerome@cdt.org.

Sincerely,
Joseph Jerome
Policy Counsel, Privacy & Data Project
Center for Democracy & Technology

[23] *FTC Data Broker Report Highlights Need for Oversight*, Center for Democracy & Technology (May 28, 2014), https://cdt.org/blog/ftc-data-broker-report-highlights-need-for-oversight/.
[24] Center for Democracy & Technology, Federal Privacy Legislation, https://cdt.org/campaign/federal-privacy-legislation/ (last visited Mar. 13, 2019).
[25] Vermont H. 764, An Act Relating to Data Brokers and Consumer Protection, Findings and Intent, Section 1(E)(2), *available at* https://legislature.vermont.gov/Documents/2018/Docs/ACTS/ACT171/ACT171%20As%20Enacted.pdf.