MAXINE WATERS, CA
CHAIRWOMAN

United States House of Representatives
Committee on Financial Services
2129 Rayburn House Office Building
Washington, D.C. 20515

PATRICK MCHENRY, NC
RANKING MEMBER

November 18, 2019

Memorandum

To: Members of the Committee on Financial Services

From: FSC Majority Staff

Subject: November 21, 2019, "Banking on Your Data: The Role of Big Data in Financial Services"

The Task Force on Financial Technology will hold a hearing entitled, "Banking on Your Data: The Role of Big Data in Financial Services," on November 21, 2019 at 9:30 a.m. in Room 2128 of the Rayburn House Office Building. This single-panel hearing will have the following witnesses:

- **Ms. Lauren Saunders**, Associate Director, National Consumer Law Center
- **Dr. Seny Kamara, PhD.,** Associate Professor of Computer Science, Brown University and Chief Scientist, Aroki Systems
- **Dr. Christopher Gillard, PhD.,** Professor of English, Macomb Community College and Digital Pedagogy Lab Advisor
- **Mr. Don Cardinal**, Managing Director, Financial Data Exchange ("FDX")
- **Mr. Duane Pozza,** Partner, Wiley Rein

Overview

Today it is easy and inexpensive for companies to collect, store, process, and sell data, regardless of the data's size, type, or location. The vast amounts of consumer information and data collected and stored by financial institutions, data aggregators, and cloud providers, among others, is commonly referred to as "big data." The "big" in big data refers to the size, complexity, and newness of any given data set; big data is key for product development because it can be used to generate insights, support decision making, and enable automation.[1] Notably, big data and cloud computing are often used interchangeably, but that is technically inaccurate. As discussed in a recent hearing,[2] cloud computing is about *computer* resources (servers and applications), whereas "big data" refers to the *computing* resources used by datasets (primarily storage and automation).[3] Big data is not unique to any one industry because it is typically comprised of data sets from all industries. However, the four basic concepts to processing big data across all industries are: volume, velocity, variety, and variability.[4]

---

[1] Gartner, "Gartner Glossary," at https://www.gartner.com/en/information-technology/glossary/big-data (last accessed Nov. 11, 2019). For example, in the financial services industry, using big data to determine the likelihood that a loan applicant will make timely repayments (loan underwriting) is key because the process traditionally relied on an in-person process and a few data sources. Big data has increased the data sources in underwriting, arguably allowing more speed, accuracy and confidence in loan decisions. *See*, U.S. Government Accountability Office ("GAO"), "Data and Analytics Innovation: Emerging Opportunities and Challenges, GAO-16-659SP," Sept. 2016, at https://www.gao.gov/assets/680/679903.pdf.

[2] Task Force on Artificial Intelligence hearing, "AI and the Evolution of Cloud Computing: Evaluating How Financial Data is Stored, Protected, and Maintained by Cloud Providers," Oct. 18, 2019, at https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-20191018-sd002-u1.pdf.

[3] *See*, GAO, *supra* 1.

[4] National Institute of Standards and Technology ("NIST"), "NIST Big Data Interoperability Framework: Volume 1, Definitions, Special Publication 1500-1r1," Jun. 2018, at https://doi.org/10.6028/NIST.SP.1500-1r1.

1. *Volume* refers to the size of a data set (as large as terabytes and petabytes) and grows when users generate and submit points of data, an example is a Facebook data feed.
2. *Velocity* refers to the flow of data coming into and being processed by an algorithm or information technology ("IT") system. This stream can be delayed or happen in near or real time, including, for example, a large merchant's transaction data feed.
3. *Variety* refers to the different types of incoming data into a dataset and can take the form of text, audio, and video. It can also refer to the source of a data set like data scraped from a website and/or data from a partner database.
4. *Variability*, while not a common characteristic of big data, acknowledges that big data sets are often scalable and can rapidly change with respect to the first three characteristics. A data set at any time may grow or shrink in volume, flow at different velocities, and include different varieties of data.

The increased use of big data in financial services has led to the rapid development of new products and services.[5] Often at the forefront of the development of most new products and services in financial services are data aggregators;[6] partly because of their ability to rapidly capture huge swarths of data from multiple sources and compile the data into a standardized and summarized form for sell to investors and other entities.[7]As discussed in a recent hearing on alternative data,[8] this is often achieved through web scraping (extracting data from websites without a direct relationship with the website or financial firm maintaining the data)[9] or through application program interfaces ("APIs"), which provide data aggregators access through negotiated agreements and can provide consumers more control.[10] Big technology firms have increasingly explored and entered the financial marketplace, while being subjected to an unclear legal framework compared to financial institutions, and the platforms and consumer data they maintain have been utilized for credit underwriting, discriminatory housing advertisements, and other purposes.[11]

[5] U.S. Department of Treasury, "A Financial System That Creates Economic Opportunities: Nonbank Financials, Fintech, and Innovation," at 22-39, Jul. 2018, at https://home.treasury.gov/sites/default/files/2018-08/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financials-Fintech-and-Innovation_0.pdf.

[6] *See,* Consumer Financial Protection Bureau ("CFPB"), "Request for Information Regarding Consumer Access to Financial Records," 81 *Federal Register* 83808, Nov. 22, 2016. *See also,* CFPB, "Consumer-Authorized Financial Data Sharing and Aggregation: Stakeholder Insights That Inform The Consumer Protection Principles," Oct 18, 2017, at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation_stakeholder-insights.pdf.

[7] Steven Melendez and Alex Pasternack, "Here are the data brokers quietly buying and selling your personal information," Fast Company, Mar. 02, 2019, at https://www.fastcompany.com/90310803/here-are-the-data-brokers-quietly-buying-and-selling-your-personal-information. *See also,* Lauren Saunders, "Fintech and Consumer Protection: A Snapshot," NCLC, Mar. 2, 2019, at https://www.nclc.org/images/pdf/cons-protection/rpt-fintech-and-consumer-protection-a-snapshot-march2019.pdf

[8] Task Force on Financial Technology hearing, "Examining the Use of Alternative Data in Underwriting and Credit Scoring to Expand Access to Credit," Jul. 25, 2019, at https://financialservices.house.gov/uploadedfiles/hhrg-116-ba00-20190725-sd002_-_memo.pdf.

[9]*See generally*, Timothy B. Lee, "Web Scraping Doesn't Violate Anti-Hacking Law, Appeals Court Rules," Ars Technica, Sept. 9, 2019, at https://arstechnica.com/tech-policy/2019/09/web-scraping-doesnt-violate-anti-hacking-law-appeals-court-rules/.

[10] FINRA, "Know Before You Share: Be Mindful of Data Aggregation Risks," Mar. 29, 2018, at https://www.finra.org/investors/alerts/be-mindful-data-aggregation-risks, *see generally,* Penny Crosman "Is Finra's dire warning about data aggregators on target?" Apr. 9, 2018, at https://www.americanbanker.com/news/is-finras-dire-warning-about-data-aggregators-on-target.

[11] For example, *see,* Full Committee hearing, "Examining Facebook's Proposed Cryptocurrency and Its Impact on Consumers, Investors, and the American Financial System," Jul. 17, 2019; *see also*, Full Committee hearing, "An Examination of Facebook and Its Impact on the Financial Services and Housing Sectors," Oct. 23, 2019.

Regulating and Protecting Big Data

The primary laws regulating the use of data in financial services at the federal level are the Gramm-Leach-Bliley Act ("GLBA"),[12] which imposes data protection and notice requirements on financial institutions, and the Fair Credit Reporting Act ("FCRA"),[13] which covers the collection and use of data related to credit reporting. Another notable provision of federal law is Section 1033 of the Dodd-Frank Wall Street Reform and Consumer Protection Act ("Dodd-Frank"),[14] which requires the Consumer Financial Protection Bureau ("CFPB") to issue rules regarding how consumers access their information from financial institutions. The CFPB has not issued rules under this provision, but instead has provided nine Consumer Protection Principles to help safeguard consumer interests.[15] The discussion below focuses on big data in the financial marketplace and to what extent GLBA applies.

Title V, Subtitle A of GLBA, which was enacted into law two decades ago on November 12, 1999, provides a framework for regulating the privacy practices of "financial institutions" – which is broadly defined under GLBA to include ATM operators and tax preparers, as well banks and credit unions. The framework is built upon: (1) providing privacy notices to consumers; (2) limiting when a financial institution may disclose a customer's nonpublic personal information ("NPI")[16] with third parties; and (3) establishing standards for safeguarding records and information.[17]

First, unless an exception applies, GLBA and its implementing regulations prohibit financial institutions from sharing NPI with non-affiliated third parties unless they first provide consumers with notice and an opportunity to "opt-out."[18] Further, financial institutions are prohibited altogether from sharing account numbers or credit card numbers to third parties for use in direct marketing. Second, financial institutions must provide clear and conspicuous initial and annual notices to customers describing their privacy policies and practices.[19] These notices must include, among other things, the categories of NPI collected and disclosed, the categories of third parties with which the financial institution shares NPI, and the policies and practices with respect to protecting the confidentiality and security of NPI. Third, GLBA and its implementing regulations require financial institutions to maintain administrative, technical, and physical safeguards to ensure the security and confidentiality of customer NPI, and to protect against any anticipated threats, hazards or unauthorized access to such information.[20] Financial institutions regulated by federal banking agencies are further required to implement a program for responding to the unauthorized access of customer NPI.[21]

---

[12] 15 U.S.C. §§ 6801–6809. *See also,* Congressional Research Service ("CRS"), "Data Protection Law: An Overview," Mar. 25, 2019, at https://www.crs.gov/Reports/R45631. Another notable provision not in discussion today is the Bank Service Company Act, 12 USC 1861-1867(c).

[13] 15 U.S.C. §§ 1681–1681x.

[14] 12 U.S.C. § 5533.

[15] CFPB, "Consumer Protection Principles: Consumer-Authorized Financial Data Sharing and Aggregation," Oct. 17, 2018, at https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf. Notably, the CFPB stated, "The Principles are intended to be read together and are not intended to alter, interpret, or otherwise provide guidance on—although they may accord with—existing statutes and regulations that apply in this market."

[16] GBLA defines "nonpublic personal information" as "personally identifiable financial information" that is not "publicly available" and is either is "provided by a consumer to a financial institution," "resulting from any transaction with the consumer or any service performed for the consumer," or "otherwise obtained by the financial institution." *See,* 15 U.S.C. § 6809(4).

[17] *See,* CRS, *supra* 16.

[18] *Id.*

[19] *Id.*

[20] *Id.*

[21] *Id.*

This framework is generally implemented through two rules: the Privacy of Consumer Financial Information Rule (Regulation P)[22] and the Safeguards Rule.[23] This year, the FTC proposed a set of changes and sought comments to both Regulation P[24] and the Safeguards Rule.[25] Notably, the FTC is seeking to expand and align the definition of financial institutions under both Regulation P and the Safeguards Rule to include "finders" or entities that charge fees for connecting consumers who are looking for a loan to a lender.[26] Also, the FTC is seeking to establish more prescriptive information security standards for financial institutions.[27] The CFPB, FTC, and federal banking agencies share civil enforcement authority for GLBA's privacy provisions. However, the CFPB has no enforcement authority over GLBA's data security provisions. Under the data security provisions, federal banking regulators have exclusive enforcement authority for depository institutions, and the FTC has exclusive enforcement authority for all non-depository institutions.[28] GLBA does not specify any civil remedies for violations of the Act, but agencies can seek remedies based on the authorities provided in their enabling statutes.[29] GLBA also imposes criminal liability on those who "knowingly and intentionally" obtain or disclose "customer information" through false or fraudulent statements or representations. Criminal liability can result in fines and up to five years' imprisonment.[30] GLBA does not contain a private right of action to allow affected individuals to sue violators.

State and International Data Protection Law Developments

Various states and foreign jurisdictions have taken steps to enhance data privacy by implementing data protection laws and regulations. Below is a brief description of several notable developments.

The California Consumer Privacy Act ("CCPA"). Enacted in 2018, the CCPA, broadly provides rights to consumers relating to the access to, deletion of, and sharing of personal information that is collected by businesses. There is a GLBA carve out in the CCPA, that finds California's privacy law inapplicable to "personal information collected, processed, sold, or disclosed . . . if it is in conflict with [GLBA]".[31] Contrasted with the CCPA's definition of "personal information"[32] (any data that could be reasonably linked to an individual or household), it is not clear, for example, how some data of a consumer applying for a home loan through a bank and its affiliates, like data aggregators, would be treated.

The New York Cyber Security Regulation for Financial Institutions ("NYCRR"). Effective in 2017, the New York State Department of Financial Services ("DFS") promulgated the NYCRR to protect customer information and information technology of regulated entities.[33] Experts have noted that the NYCCR is broader and more prescriptive than GLBA in the institutions it covers and information security standards it sets forth.[34]

---

[22] CFPB, "12 CFR Part 1016 - Privacy of Consumer Financial Information (Regulation P)." *See also*, FTC, "How To Comply with the Privacy of Consumer Financial Information Rule of the Gramm-Leach-Bliley Act." (last accessed Nov. 9, 2019).
[23] FTC, "Safeguards Rule." (last accessed Nov. 9, 2019)
[24] FTC, "Privacy of Consumer Financial Information Rule Under the Gramm-Leach-Bliley Act." (last accessed Nov. 9, 2019)
[25] FTC, "Standards for Safeguarding Customer Information." (last accessed Nov. 9, 2019)
[26] Mike Nonaka, et al., "FTC Proposes to Add Detailed Cybersecurity Requirements to the GLBA Safeguards Rule," Mar. 7, 2019, at https://www.insideprivacy.com/financial-privacy/ftc-proposes-to-add-detailed-cybersecurity-requirements-to-the-glba-safeguards-rule/.
[27] *Id.*
[28] *See*, CFPB, *supra* 21.
[29] *See*, FTC, *supra* 21.
[30] *Id.*
[31] CCPA § 1798.145(e). (last accessed Nov. 9, 2019)
[32] CCPA § 1798.140(o). (last accessed Nov. 9, 2019)
[33] 23 NYCRR 500. (last accessed Nov. 9, 2019)
[34] Michael Krimminger, "New York Cybersecurity Regulations for Financial Institutions Enter Into Effect," Mar. 25, 2017, at https://corpgov.law.harvard.edu/2017/03/25/new-york-cybersecurity-regulations-for-financial-institutions-enter-into-effect/.

The European Union's General Data Protection Regulation ("GDPR"). The European Union ("EU") has a wide-ranging data protection regulatory scheme. Whereas U.S. data privacy statutes generally are sectorial, European privacy regulations have generally concerned any entity's accumulation of large amounts of data. EU treaties provide individuals with a general right to "protection of personal data" from all potential interferences.[35]. GDPR provides a series of general rights to individuals, some include the right to be informed and the right to be forgotten.[36]

Financial Surveillance and Marginalized Communities

Twenty years ago, when GLBA was enacted, it was more clear what financial data was to consumers and financial institutions. However, as technology has advanced, what GLBA protects is not as clear as it once was. Further, without clear protections or redress for misuses of consumers' financial data and information the bargain for exchange potentially disproportionally hurts consumers.[37] At the same time, this gap may leave low-income populations even more susceptible to mass data collection and aggregation of not only their financial data but also, their personal data. For example, if collected by data aggregators and ultimately sold to financial institutions, includes eye movements, it is unclear how that could help inform the loan-underwriting process.[38] However, the mass collection of data on low-income populations is a form of "financial surveillance," that allows companies to digitally stalk low-income populations' every move, behavior, and activity.[39] This potentially widens preexisting economic gaps by allowing faster and more targeted predatory tactics on low-income people and increases discrimination. To combat financial surveillance, researchers are using cryptographic technologies (ways to hide data from third-parties).[40] For example, secure multi-party computation can be applied to large datasets in credit ratings to conduct the computations (or equations) without having to decrypt the data.

Legislative Proposals

Safeguarding Non-bank Consumer Information Act. (Lynch). This discussion draft clarifies the Gramm-Leach-Bliley Act's consumer financial privacy and data security provisions and gives the Bureau of Consumer Financial Protection rulemaking and enforcement authority over the safeguards rule with respect to data aggregators and other financial institutions.

Financial Information Data Modernization Act ("FIDMA"). This is a discussion draft that sets forth minimum data security standards by clarifying "financial data" and "non-financial institutions" under the Gramm-Leach-Bliley Act to protect consumers and provide guidance that contemplates advances in technology for entities interacting with financial data.

H.R. 4008, the No Biometric Barriers to Housing Act of 2019. (Reps. Clarke, Pressley, and Tlaib). This bill prohibits the use of biometric recognition technology and biometric data analysis in housing units and buildings covered under the Public Housing, Section 8 Project-Based Rental Assistance, Section 811 Supportive Housing for Persons with Disabilities, and Section 202 Supportive Housing for the Elderly programs.

---

[35] *See*, CRS, *supra* 17.
[36] *Id*.
[37] Chris Gilliard, "Privacy's not an abstraction," Fast company, Mar. 25, 2019 at https://www.fastcompany.com/90323529/privacy-is-not-an-abstraction.
[38] Aaron Holmes, "Facebook users are noticing a bug that lets the app access their iPhone's camera while they're scrolling through their newsfeed," Business Insider, Nov. 12, 2019, at https://www.businessinsider.com/facebook-bug-accesses-camera-iphone-app-2019-11.
[39] Mary Madden, Michele Gilman, Karen Levy, and Alice Marwick "Privacy, Poverty, and Big Data: A Matrix of Vulnerabilities for Poor Americans," 95 Wash. U. L. Rev. 053 (2017), at https://openscholarship.wustl.edu/law_lawreview/vol95/iss1/6.
[40] *See*, Nigel P. Smart, "Future Directions in Computing on Encrypted Data" Nov. 2015 https://www.ecrypt.eu.org/csa/documents/D2.2-ComputingonEncryptedData.pdf.