XVII. To Screen Scrape, or Not to Screen Scrape: That Is the Question the Consumer Financial Protection Bureau Does Not Answer

A. Introduction

Financial data comprises specialized personal data relating to finance, such as transactions, balances, fees, and interest charges.[1] Financial data aggregation refers to a third party's collecting financial data, usually to perform a further service on behalf of the consumer.[2] Currently, the United States does not have any overarching regulation regarding financial data aggregation.[3] Section 1033 of the Dodd-Frank Act (Dodd-Frank) states broadly that covered persons must make consumer data available and usable.[4] This broad provision has sparked debate on whether covered persons must make the data available in any way a consumer permits or if the covered person is only required to provide the data through its own chosen method.[5] In essence, do

---

[1] *Fintech: Examining Digitization, Data, and Technology: Hearing Before the S. Comm. on Banking, Housing and Urban Affairs*, 115th Cong. 31 (2018), https://www.govinfo.gov/content/pkg/CHRG-115shrg27749/pdf/CHRG-115shrg27749.pdf [hereinafter *Hearing*] ("Financial data, including, for example, balances, fees, transactions, and interest charges[.]").

[2] *Id.* at 32 (stating that financial aggregators gather consumer data to provide to application service providers).

[3] *Id.* ("[T]here are no overarching statutory, regulatory or market standards in the United States with regard to consumer or small business authentication, or with regard to the data consumption protocol used by aggregators to transmit the end user's data, with their permission, to their application of choice[.]"); While the Gramm-Leach-Bliley Act does specify financial institutions and some nonbank financial institution must comply with provisions to protect nonpublic consumer data, it does not address data aggregation methods. Pub. L. No. 106-102 (1999).

[4] Dodd-Frank Wall Street Reform and Consumer Protection Act, Pub. L. No. 111-203, 124 Stat. 1376 (2010). (Stating "Covered persons shall make available to a consumer, upon request, information in the control or possession of the cover person concerning the consumer financial product or service that the consumer obtained from such covered person, including information relating to any transaction, series of transactions, or to the account including costs, charges and usage data. The information shall be made available in an electronic form usable by consumers.").

[5] Beam et al., *Whose Data Is It? CFPB Releases Consumer Protection Principles for Consumer-Authorized Financial Data Sharing and Aggregation*,

financial institutions need to facilitate consumers' requests to use financial data in third party services?[6] Congress has authorized the Consumer Financial Protection Bureau (CFPB) to implement and enforce consumer financial law to help navigate situations like those presented in the above question.[7] In fact, the CFPB issued a set of non-binding Consumer Protection Principles pointed at this very issue, but these principles failed to spell out the state of play required between financial institutions, third party service providers (TSPs), data aggregators, and consumers.[8]

For the interest of this article, TSPs refer to financial technology (FinTech) companies that deliver value-added financial services to consumers.[9] In the United States, TSPs provide these services by using a data aggregation firm as an intermediary to extract financial data from a financial institution's online platform, which then enables the TSP to use the data to support its services.[10] For example, when a consumer is signing up for an account on Mint.com,[11] the TSP must provide his login credentials to his formal banking institution in order

---

MAYER BROWN (Nov. 2, 2017), https://www.mayerbrown.com/-/media/files/perspectives-events/publications/2017/11/whose-data-is-it-cfpb-releases-consumer-protection/files/updatecfpbprinciplesforfinancialdatasharingandaggr/fileattachment/updatecfpbprinciplesforfinancialdatasharingandaggr.pdf.

[6] *Id.* at 2 (stating that Section 1033 of Dodd-Frank prohibits financial institutions from withholding financial data from its corresponding consumer, but unclear whether financial institutions must facilitate all forms of sharing).

[7] 12 U.S.C. 5511(a); 12 U.S.C. 5511(b)(5) (stating the purpose and objectives of the Bureau).

[8] CONSUMER FINANCIAL PROTECTION BUREAU, CONSUMER PROTECTION PRINCIPLES: CONSUMER-AUTHORIZED FINANCIAL DATA SHARING AND AGGREGATION (Oct. 17, 2018), https://files.consumerfinance.gov/f/documents/cfpb_consumer-protection-principles_data-aggregation.pdf; *see* Erin Fonte & Brenna McGee, *EU Law Brings Data Sharing Pointers for US Financial Cos.*, LAW360 (June 29, 2018), https://www.law360.com/articles/1056977/eu-law-brings-data-sharing-pointers-for-us-financial-cos ("[T]he principles do little to illuminate how FIs must share that data with consumers and third parties in the U.S.").

[9] *See e.g.*, INTUIT MINT, https://www.mint.com/how-mint-works [https://perma.cc/57SC-XZGU] (last visited Oct. 6, 2019).

[10] Fonte, *supra* note 8 ("Screen scraping remains the norm and FIs allow it due to market pressures and consumer demand.").

[11] Mint.com is an online platform that provides its users a comprehensive snapshot of their financial health and includes budgeting tools and payment reminders. *See* INTUIT MINT, *supra* note 9.

to enable Mint's financial services.[12] From the bank's consumer-facing interface, Intuit,[13] the data aggregator, uses its proprietary software to gather the consumer's transaction information that Mint.com packages into a user-friendly, financial product.[14] The data aggregator's methodology of using the consumer's login credentials to access consumer financial data is called screen scraping.[15] While use of FinTech tools like Mint.com is wide spread, screen scraping has raised concern over its security risks.[16] Some financial institutions have mitigated these concerns by providing other methods for data aggregators and/or TSPs to access consumer financial data, such as the use of Application Programming Interfaces (APIs).[17] APIs provide a direct feed to the

---

[12] *Id.* (stating that a TSP requires customer data to complement a financial service.)

[13] Mint.com formerly used data aggregator Yodlee before partnering with Intuit. *See* Blake Ellis, *WTF?! Where did my Mint.com data go?,* CNN (Dec. 2, 2010), https://money.cnn.com/2010/12/02/pf/mint_leaves_yodlee/index.htm [https://perma.cc/YNW6-R293]; In 2016, Intuit stopped providing financial data aggregation services to third parties, focusing solely on its own financial products. Jarred Keneally, *Intuit Financial Data APIs (CAD) Update*, INTUIT DEVELOPER (Mar. 15, 2016), https://blogs.intuit.com/blog/2016/03/15/intuit-financial-data-apis-cad-update/ [https://perma.cc/4VNY-WFZN] (stating that providing third party aggregation no longer fits the core business strategy and Intuit will only aggregate for its own products).

[14] INTUIT MINT https://www.mint.com/how-mint-works/security (last visited Oct. 6, 2019) (stating how data aggregators and financial service providers cooperate to tailor products to users).

[15] U.S. DEP'T OF TREAS., A FINANCIAL SYSTEM THAT CREATES ECONOMIC OPPORTUNITIES NONBANK FINANCIALS, FINTECH, AND INNOVATION REPORT TO PRESIDENT DONALD J. TRUMP EXECUTIVE ORDER 13772 ON CORE PRINCIPLES FOR REGULATING THE UNITED STATES FINANCIAL SYSTEM (July 2018) at 25, https://home.treasury.gov/sites/default/files/2018-07/A-Financial-System-that-Creates-Economic-Opportunities---Nonbank-Financi....pdf [hereinafter, *Treasury Report*] ("In screen-scraping, consumers provide their account login credentials—usernames and passwords—in order to use the fintech application.").

[16] *Hearing*, *supra* note 1, at 32 ("Usage of third-party, FinTech tools in the U.S. is widespread[.]"); *id.* at 37–38 (stating that screen scraping opens consumers and financial institutions to cybersecurity threats, identity theft, and access to personal data outside the scope of services from third parties).

[17] *Id.* at 32 ("Some financial institutions have created direct feeds, such as Application Programming Interfaces (APIs), specifically for aggregators and third parties to utilize for the purpose of providing products or services to their customers[.]").

suite of data for data aggregators/TSPs[18] so that a TSP can power its financial tools.[19] APIs eliminate the need for TSPs to have access to consumer login credentials and may limit the scope of data shared with TSPs and data aggregators.[20] Some firms do not apply a single approach to data aggregation. For example, Intuit signed a data-sharing agreement and uses JPMorgan's API instead of the customary screen scraping method for the customers of JPMorgan Chase bank.[21] Yet, consumers within the United States are still more likely to encounter TSPs whose data is collected via screen scraping due to the lack of financial institutions utilizing APIs.[22]

Part B of this article provides a deeper look into screen scraping, APIs, and the ownership of financial data. Next, Part C summarizes how the European Union (EU) has tackled data aggregation with its revised Payment Services Directive (PSD2). Finally, this article concludes with a discussion of the complications surrounding a pro-consumer data aggregation model in the United States.

---

[18] TSPs generally use data aggregation firms to collect their customers' data at financial institutions. Meir Leff, *WTF is Data Aggregation?*, TEARSHEET (Feb. 11, 2019), https://tearsheet.co/wtf/wtf-is-data-aggregation/ [https://perma.cc/Y4AB-CQAT]; however, some TSPs and data aggregators had combined to provide a full service. *See* Ellis, *supra* note 13 (stating that Intuit acquired Mint.com for $170 million and it will power its financial services).

[19] *Id.* (stating the purpose of the API).

[20] *Id.* at 39. (stating that APIs can operate without some of the privacy worries seen in TSPs and data aggregators.)

[21] While Intuit may seek similar agreements with other financial institutions, it still employs screen scraping techniques at other institutions. Patricia Wexler, *Chase, Intuit to Give Customers Greater Control of Their Information*, CHASE MEDIA CENTER (Jan. 25, 2017), https://media.chase.com/news/chase-intuit-to-give-customers-greater-control-of-their-information [https://perma.cc/JE5C-MSGR].

[22] *Hearing*, *supra* note 1, at 32 ("[T]he vast majority of U.S. financial institutions have not [created APIs].").

B. Data Aggregation in the United States

1. Screen Scraping: Is It All That Bad?

There has been great debate over the security risks of screen scraping.[23] The main concern over screen scraping is the access to and storage of consumers' login credentials by data aggregators, who often are not identified to the consumer using a TSP's financial service.[24] This fact begs the question: if a data breach were to occur, would consumers even know if they were affected? The Gramm-Leach-Bliley Act (GLBA) only applies to financial institutions, which data aggregators are not.[25] At the state level, only thirteen states have data breach notification standards for the protection of consumer financial

---

[23] *See generally* Daniel Döderlein, *Fintechs' Defense of Screen Scraping Is Shortsighted*, AMERICAN BANKER (Sept. 7, 2017), https://www.americanbanker.com/opinion/fintechs-defense-of-screen-scraping-is-shortsighted); Liz Weston, *Why Banks Want You to Drop Mint, Other 'Aggregators'*, REUTERS (Nov. 9, 2015), https://www.reuters.com/article/us-column-weston-banks/why-banks-want-you-to-drop-mint-other-aggregators-idUSKCN0SY2GC20151109 [https://perma.cc/6XCH-BT27]; *but see generally* Future of European Fintech, *Manifesto for the impact of PSD2 on the future of European Fintech* (2017), https://www.futureofeuropeanfintech.com/assets/Manifesto-for-theimpact-of-PSD2-on-the-future-of-European-Fintech.pdf (available at https://www.paymentscardsandmobile.com/wp-content/uploads/2017/05/Manifesto-for-the-impact-of-PSD2-on-the-future-of-European-Fintech.pdf) (arguing that screen scraping is secure and PSD2 compliant and should not be banned in the EU).

[24] *See Hearing*, *supra* note 1, at 37 ("[Sharing login credentials] creates cybersecurity, identity theft, and data security risks for the consumer and financial institutions . . . D]ue to years of this practice, financial institution log-in credentials are now held by a myriad of companies."); *see also Treasury Report*, *supra* note 15, at 32 "[F]or FinTech applications that rely on a data aggregator to obtain or process the consumer's financial account and transaction data, the role of the data aggregator may be opaque to the consumer[.]").

[25] FEDERAL TRADE COMMISSION, GRAMM-LEACH-BLILEY ACT, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/gramm-leach-bliley-act [https://perma.cc/ME6L-T7RU] ("The Gramm-Leach-Bliley Act requires financial institutions—companies that offer consumers financial products or services like loans, financial or investment advice, or insurance—to explain their information-sharing practices to their customers and to safeguard sensitive data.").

data.[26] Outside of those thirteen states, it is unclear if consumers would be notified of a financial data breach. While the looming risk of a data breach exists in theory, there has not been a case of personal financial data being compromised due to screen scraping.[27]

Opponents of screen scraping still suggest it has other severe pitfalls.[28] First, screen scraping is inefficient because it requires a different approach for each native environment due to the diversity of financial institutions' online banking interfaces and must be updated each time the login credentials change.[29] Second, screen scraping enables TSPs to have unfettered access to the entire range of consumer data.[30] For instance, TSPs and/or data aggregators using screen scraping know personal information irrelevant to the value-added service, like your date of birth or names of your children.[31] Screen scraping is also traffic intensive, which results in reduced or slower access to online banking platforms.[32] Lastly, screen scraping affects the financial institution's ability to identify suspicious logins, which paired with the traffic volume, may confuse the bank's online system of being under an automated attack.[33] As a result, some proponents of screen scraping realize these limitations and they have suggested that

---

[26] *Treasury Report*, *supra* note 15, at 39 ("To date, only 13 states have imposed data security standards for protection of consumer financial data, which have different requirements.").

[27] *See* Döderlein, *supra* note 23 ("While there are no known hacks related to screen scraping, the risks for fraud are mounting.").

[28] *Id.*

[29] *Id*. ("There is no uniform way to carry out a screen scrape since every bank website is different."); *Hearing*, *supra* note 1, at 39 (stating screen scraping requires reconfiguration each time the login credentials are changed).

[30] *Hearing, supra* note 1, at 38 ("[S]creen scraping may result in access to data fields far beyond the scope of the service a third party offers the consumer—including personally identifiable information (PII) about consumers and in some cases their dependents.").

[31] *Id.* (stating that financial institutions often use dates of birth and names of dependents to confirm the identify of its consumers, which would be available if screen scraping is performed).

[32] *See* Penny Crosman, *The Truth Behind the Hubbub over Screen Scraping*, AMERICAN BANKER (Nov. 12, 2015), https://www.americanbanker.com/news/the-truth-behind-the-hubbub-over-screen-scraping. ("Second, it's a fact that the data aggregators' screen scraping activity drives spikes in volume to banks' online banking websites.").

[33] *Id.* ("To a bank server, the data aggregators' traffic looks and feels like an automated attack.").

screen scraping not be the preferred method of data aggregation but rather a failsafe.[34]

Given these abovementioned concerns, screen scraping has still remained the norm in the United States.[35] Summarily, screen scraping is a simpler, cost-effective solution[36] than an API channel.[37] Inertia also plays a significant role in opposing the adoption of APIs because screen scraping has been around since at least 2001.[38] Practical concerns, like competition, have also hindered the transition to APIs as financial institutions have flat out resisted third party financial tools.[39] In fact, a 2017 PwC survey found that 88% of financial institutions believed they had lost revenue due to FinTech competition.[40] TSPs are equally concerned with the competition aspect as some have reported financial institutions have blocked them from consumer data

---

[34] Nick Wallace, *Commission Right to Reject Screen-scraping Ban*, EUOBSERVER (Aug. 30, 2017), https://euobserver.com/digital/138824 ("None of this is to suggest that screen-scraping is preferable to APIs. On the contrary: screen-scraping is only a failsafe.").

[35] Fonte, *supra* note 8 ("Screen scraping remains the norm and FIs allow it due to market pressures and consumer demand.").

[36] *Treasury Report*, *supra* note 15, at 26 (stating that APIs are costly and may be an obstacle preventing smaller financial institutions the ability to partner with TSPs).

[37] *Hearing*, *supra* note 1, at 40 ("One of the unfortunate truths about screen scraping is that it is cheap and effective.").

[38] OFF. COMPTROLLER OF CURRENCY, BANK-PROVIDED ACCOUNT AGGREGATION SERVICES: GUIDANCE TO BANKS (Feb. 28, 2001), https://www.occ.gov/news-issuances/bulletins/2001/bulletin-2001-12.html [https://perma.cc/2WX2-VV2U] (summarizing the risks of account aggregation practices in 2001); *See Hearing*, *supra* note 1, at 40 ("One force working against adoption of safer data sharing technologies is simple inertia. Existing [screen scraping] practices have been the norm for close to two decades.").

[39] Center for Data Innovation, *Blocked: Why Some Companies Restrict Data Access to Reduce Competition and How Open APIs Can Help*, at 10 (Nov. 6, 2017), http://www2.datainnovation.org/2017-open-apis.pdf (explaining that TSPs' services compete with financial institution services or often lower financial institutions' margins).

[40] Kashyap et al., *Redrawing the Lines: FinTech's Growing Influence on Financial Services*, PRICEWATERHOUSECOOPERS (2017), https://www.pwc.com/gx/en/industries/financial-services/assets/pwc-fintech-exec-summary-2017.pdf ("Financial Institutions are increasingly likely to lose revenue to innovators, with 88% believing this already is occurring.").

despite having consumer consent.[41] To promote a more cooperative, non-regulatory solution, some banks have bilateral agreements with data aggregators to ease the burden for online platforms and assure access to consumer data.[42] But those aggregators, without bilateral agreements, may find themselves blocked from the consumer-permissioned collection of financial data.[43]

2. APIs: Are They Superior?

An API is a channel that allows two or more systems to communicate and exchange data to perform specialized tasks.[44] For example, in Uber's initial public offering (IPO) filing, the ride-sharing company partnered with Google to utilize Google's mapping functions on its application.[45] The two applications communicated through an API which allowed drivers to find their customers, the destination, and the route using Google Maps through the Uber application.[46] Financial institutions can use APIs to allow data aggregators access to financial data without the need of logging into a consumer's online banking

---

[41] Robin Sidel*, Big Banks Lock Horns With Personal-Finance Web Portals*, WSJ (Nov. 4, 2015), https://www.wsj.com/articles/big-banks-lock-horns-with-personal-finance-web-portals-1446683450 ("[T]he decision to cut off Mint was more of a technical matter than a shot across the bow to warn aggregators that they could turn them off at any time. At Wells Fargo, [. . .] an additional level of security to its accounts last month prevented aggregators from being able to automatically retrieve customer data[.]").

[42] Crosman, *supra* note 31 ("[L]arger aggregators like Intuit have agreements with banks under which the aggregators access the banks' systems at certain times of the day."); *E.g.,* Wexler, *supra* note 21.

[43] *JPMorgan's Clampdown on Data Puts Silicon Valley Apps on Alert*, AMERICAN BANKER (Mar. 26, 2019), https://www.americanbanker.com/articles/jpmorgans-clampdown-on-data-puts-silicon-valley-apps-on-alert (stating that JPMorgan entered into an agreement with Plaid and JPMorgan would start blacklisting traffic from other aggregators).

[44] *Treasury Report*, *supra* note 15, at 26.

[45] Jordan Novet, *Uber Paid Google $58 million over Three Years for Map Services*, CNBC (Apr. 11, 2019), https://www.cnbc.com/2019/04/11/uber-paid-google-58-million-over-three-years-for-map-services.html [https://perma.cc/ZY6E-GN3P] ("Google is noted as a key supplier of mapping technology to Uber in the ride-sharing company's IPO filing. . .").

[46] *Id.* ("[T]he technology shows the current place, the destination and a route, along with estimates of arrival times."). In 2015, Uber acquired deCarta for its navigation services.

interface.[47] APIs also allow financial institutions to know whether data sharing is occurring as opposed to large volume "suspicious attacks" on their platforms.[48] APIs provide financial institutions the ability to apply more security features, such as controlling the data aggregator's connection with the data through encrypted tokens that are provisioned for a specific task.[49] These security features place the control over financial data back into the hands of consumers and appear to combat many of the security risks that screen scraping present.[50]

However, some of these features may be a double-edged sword.[51] Smaller financial institutions, like community banks, are disadvantaged by the cost of developing an API, which may lower their attractiveness to consumers seeking TSP financial services.[52] Some commentators have gone so far as to say that APIs do not necessarily increase security, but instead reduce competition.[53] Data aggregators have reported that APIs have been used to restrict or block data collection on some financial institutions' platforms even though the aggregators had consumer consent.[54] The Equifax hack of 2017 further

---

[47] *Treasury Report*, *supra* note 15, at 26 ("API method of access is generally enabled through consumer consent provided to the financial services company or at the API access point rather than through giving consumer login credentials to third-parties.").

[48] *Id.* ("Unlike in the case of screen-scraping, data aggregation through an API generally means that financial services companies are knowingly participating in the sharing of data.").

[49] *Hearing*, *supra* note 1, at 38–39 ("Consumers who want their data aggregated sign into their accounts at the financial institution's website and provide authorization for third party aggregators to access their financial data. The financial institution and the data aggregator then manage that connection through secure, encrypted tokens that are provisioned for the specific connection.").

[50] *Id.* at 39.

[51] *See generally* Chris Wood, *Why Do FinTechs Want To Save Screen Scraping?*, NORDICAPIS (June 22, 2017), https://nordicapis.com/fintechs-want-save-screen-scraping/ [https://perma.cc/USU8-4X32].

[52] *Hearing*, *supra* note 1, at 40 (stating that the cost of APIs serve as an obstacle for smaller financial institutions).

[53] Center for Data Innovation, *supra* note 38 (stating that blocking TSP tools did not increase security but reduced competition).

[54] *Treasury Report*, *supra* note 15, at 27–28 ("APIs [were] frequently and unilaterally restricted, interrupted, or terminated by financial services companies.").

illustrates that even APIs may experience data vulnerabilities.[55] Nonetheless, some international jurisdictions, including: Australia, Hong Kong, India, and most notably, the EU, have shifted towards providing access to financial data through APIs.[56]

3. Who Owns the Data Anyways?

Stepping away from the "screen scraping or APIs" debate, a more fundamental policy issue exists: do you *own* your financial data? Scholars who have researched this question have found that neither U.S. nor EU data protection or privacy law identifies exactly who owns the data.[57] Ownership of financial data may best be described by drawing upon property law's differing conceptions of ownership, but specifically, a Benthamite bundle of sticks theory.[58] Dodd-Frank creates a consumer's right to access and use their financial information, but does touch upon other rights.[59] It does not discuss the right of transferability of financial data, i.e., selling financial data to third parties for profit.[60] In fact, selling consumers' transactional financial data is a lucrative industry.[61] While many consumers remain unaware

---

[55] Dep't of Media Relations, *Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes*, EQUIFAX (Sept. 15, 2017), https://investor.equifax.com/news-and-events/news/2017/09-15-2017-224018832 [https://perma.cc/LXY2-QUXT] (identifying the vulnerability in the Apache Struts web application [an API] that results in the leak of personal information).

[56] *Treasury Report*, *supra* note 15, at 177-78.

[57] Jeffrey Ritter & Anna Mayer, *Regulating Data as Property: A New Construct for Moving Forward*, 16 DUKE L. & TECH. REV. 220, 227 (2018) ("As a general proposition, no privacy or data protection laws expressly define which entity *owns* personal information.").

[58] As opposed to a Blackstonian total control theory of ownership. THOMAS W. MERILL & HENRY E. SMITH, PROPERTY: PRINCIPLES AND POLICIES, 17 (Robert C. Clark et al. eds., 3d ed. 2017) (describing the common metaphor of a bundle of sticks as the collection of all rights of ownership such as use, transfer, and exclude).

[59] Dodd-Frank, *supra* note 4.

[60] Although, Dodd-Frank does clarify that proprietary data, such as algorithms, is owned by the covered person. *Id.*

[61] Typically, consumers have consented to these types of sales through the user agreement and companies claim that there are no personally identifying indicators on sold data. *See* Peter Cohen, *Mastercard, AmEx And Envestnet Profit From $400M Business Of Selling Transaction Data*, FORBES (July 22,

of where their data goes and how it is used, even those consumers who remain concerned do not have a clear picture of what is allowed and what is not.[62] When this theory of data ownership is compared to what the Federal Education Rights and Privacy Act (FERPA)[63] and the Health Insurance Portability and Accountability Act (HIPPA)[64] have done for their respective sectors, we see similarly blurred results.

Covered persons under these federal laws act as stewards of the information and consumers have a right to access, use, and disclose their data.[65] In the HIPAA context, doctors cannot outright sell patient medical data, but the line is blurred when the doctor uses a patient's data to create a medical product which is sold for profit.[66] The medical research business is booming and patients do not see any of the proceeds.[67] Similarly, under FERPA, covered persons are restricted from sharing information about a student's educational record without consent.[68] However, private data brokers are not covered persons

---

2018), https://www.forbes.com/sites/petercohan/2018/07/22/mastercard-amex-and-envestnet-profit-from-400m-business-of-selling-transaction-data/#6eff1f377722 [https://perma.cc/B4MY-ZDVR]; *see also* Penny Crosman, *Should Banks be in the Business of Surveillance Capitalism?*, AMERICAN BANKER (June 8, 2017), https://www.americanbanker.com/news/should-banks-be-in-the-business-of-surveillance-capitalism (stating that anonymized data can be de-anonymized and consumers are not properly informed of data selling policy).

[62] Crosman, *supra* note 60 (stating that consumers don't know how their data is being used).

[63] Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (2012).

[64] Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104–191, 110 Stat. 1936 (1996).

[65] Chelsea Allison, *Who Owns Personal Data*, PLAID (Mar. 1, 2019), https://fin.plaid.com/articles/who-owns-personal-data/ (comparing financial data to data protected under HIPAA and describing health providers as stewards with clients having access rights).

[66] Richard Harris, *If Your Medical Information Becomes a Moneymaker, Could You Get a Cut?*, NPR (Oct. 15, 2018), https://www.npr.org/sections/health-shots/2018/10/15/657493767/if-your-medical-information-becomes-a-moneymaker-could-you-could-get-a-cut [https://perma.cc/8XF9-D4PV] (stating that the use of data to create a medical product can be interpreted as being a "health care operation," which allows use of patient data).

[67] Yet, some for-profit businesses are emerging that compensate patients for authorized use of their medical data. *Id.*

[68] Collins et al., *New Study on the Marketplace for Student Data*, FERPA SHERPA (June 7, 2018), https://ferpasherpa.org/fordhamclip1/ [https://perma.cc/4SMU-SQ6K] ("Under FERPA, schools and teachers are prohibited from

under FERPA and other federal laws[69] and have made a business of selling lists of student information based on stereotypes.[70] These lists are populated from public records, commercial sources, and sometimes surveys taken at school.[71] Some states have taken action to fill in the gaps by covering data brokers, but overall, there is a lack of transparency surrounding these student lists.[72]

As former CFPB Director Richard Cordray put it, "[like] your student records or medical records, your financial records tell an important story about you."[73] Consumers ought to control the story that is told, and one way is through a pro-consumer data aggregation method. Defining what financial data ownership means will help bring to the fore pro-consumer data collection methods as the attendant rights of data ownership will be delineated.[74] The remaining sections of this article will provide more context to what is entailed in a pro-consumer data collection method.

---

sharing information from a student's educational record . . . unless there is parental consent. . .").

[69] Children's Online Privacy Protection Act (COPPA), 15 U.S.C. §§ 6501–6506 (2012); Protection of Pupil Rights Amendment (PPRA), 20 U.S.C. § 1232(h) (2012).

[70] *See generally* Russell et al., *Transparency and the Marketplace for Student Data*, VA. J. L. & TECH. (forthcoming).

[71] Collins et al., *supra* note 67 ("For example, some schools are likely giving out surveys from the National Research Center for College and University Admissions (NRCCUA), an organization listed in the study as a 'Student Data Broker.'").

[72] *Id.* ("For example, Vermont recently passed legislation requiring "data brokers" to post information about their data practices and opt-outs with the Vermont Secretary of State.").

[73] Richard Cordray, Prepared Remarks of CFPB Director Richard Cordray at the Field Hearing on Consumer Access to Financial Records (Nov. 17, 2016) (transcript available at https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-cfpb-director-richard-cordray-field-hearing-consumer-access-financial-records/).

[74] *See* Ritter, *supra* note 56, at 222 ("Once ownership is well-defined, then the attendant rights can be more precisely expressed—rights to access, license, transfer, modify, combine, edit, and delete data naturally flow from the control that ownership vests.").

C. Data Aggregation in the European Union: PSD2

In January 2018, the PSD2 came into effect in the EU.[75] PSD2 divides TSPs into two categories: payment initiation service providers (PISPs) and account information service providers (AISPs).[76] PISPs are TSPs who initiate a transaction on behalf of the consumer, while AISPs are TSPs who consolidate financial information from multiple sources into a single product for consumers to view.[77] PayPal.com is an example of a PISP when the consumer pays for a product through his PayPal account that is linked to his banking institution.[78] AISPs perform services similar to that of Mint.com mentioned earlier.[79] PSD2 includes data aggregators within the AISP category, thus providing expressed regulation to data aggregators.[80] PSD2 authorized the European commission to adopt the Regulatory Technical Standards (RTS) drafted by the European Banking Authority (EBA).[81] Two main objectives of the RTS are to enhance security through mandatory use of strong customer authentication (SCA) and to improve competition by requiring banks to share consumer-permissioned financial data with registered TSPs.[82] SCA involves consumers proving their identities

---

[75] EUROPEAN COMMISSION, PAYMENT SERVICES DIRECTIVE (PSD2): REGULATORY TECHNICAL STANDARDS (RTS) ENABLING CONSUMERS TO BENEFIT FROM SAFER AND MORE INNOVATIVE ELECTRONIC PAYMENTS (Nov. 27, 2017), https://europa.eu/rapid/press-release_MEMO-17-4961_en.htm [https://perma.cc/Z6E5-A869].

[76] *Id.* (stating that third party payment service providers include: Payment initiation services and aggregators and account information service providers).

[77] *Id.* (defining PISPs and TISPs).

[78] Paypal offers many methods of payment, such as adding a credit card, but acts as PISP when linked to the consumer's bank account. For example, at checkout of an online merchant, the customer is prompted with payment options and if Paypal is chosen, then the page is redirected to a Paypal login screen. *See* Paypal, *PSD2 Compliance*, PAYPAL, https://developer.paypal.com/docs/psd2-compliance/ [https://perma.cc/8JLM-QXG7].

[79] EUROPEAN COMMISSION, *supra* note 75; although, Mint.com is only available in the US and Canada. INTUIT MINT https://help.mint.com/General/992017171/Is-Mint-available-outside-the-US.htm [https://perma.cc/5VER-3GMQ] (last visited Oct. 6, 2019).

[80] EUROPEAN COMMISSION, *supra* note 75.

[81] *Id.* ("To this end, PSD2 empowers the Commission to adopt regulatory technical standards (RTS) on the basis of the draft submitted by the European Banking Authority (EBA).").

[82] *Id.* (stating the two main objectives of the RTS).

through two of three methods, also referred to as two-factor authentication: pins and passwords, something they own (e.g., a bank card or mobile device), and biometrics (e.g., iris or fingerprint scan).[83] SCA is aimed at preventing the unauthorized access concern associated with TSP services through proof of consumer consent.[84] The RTS aimed to increase competition by standardizing a secure data communication interface, which allows entry of more market participants, like TSPs.[85] PSD2 does not explicitly require the use of APIs for data aggregation, but it does ban the use of screen scraping.[86] The ban of screen scraping[87] eliminates the problem of inefficiency discussed in the above sections of this article.

D. Conclusion

While the recent regulatory changes in the EU[88] have not had much time to show results, one thing to be sure of is that consumers

---

[83] *Id.* (describing the three such elements that users can use to prove their identity).

[84] Brian Gaynor, *Are You Ready for Strong Customer Authentication (SCA)*, JPMORGAN (2017), https://www.jpmorgan.com/europe/merchant-services/insights/psd2-are-you-ready-for-strong-customer-authentication-sca [https://perma.cc/PCJ3-YWNF] (providing an example of SCA is two factor authentication).

[85] EUROPEAN CENTRAL BANK, THE REVISED PAYMENT SERVICES DIRECTIVE (PSD2) AND THE TRANSITION TO STRONGER PAYMENTS SECURITY (Mar. 2018), https://www.ecb.europa.eu/paym/intro/mip-online/2018/html/1803_revisedpsd.en.html [https://perma.cc/H5SE-RHNS] ("The aim is to reach a market agreement on one technical specification so that all systems across Europe could ultimately be based on one or a few technical API standards.").

[86] Council Decision 2018/385, 2018 O.J. (L 69) 20 (EU) (available at https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2018:069:FULL&from=EN) (stating that financial institutions must provide an access interface to TSPs to communicate with and receive information from the financial institution); *See* EUROPEAN CENTRAL BANK, *supra* note 84 (providing an example of such an interface as an API channel).

[87] Exceptions may apply and some screen scraping could be allowed via the Fallback Provision, if authorized by the EBA. EUROPEAN CENTRAL BANK, *supra* note 84 ("National authorities will grant the exemption to individual banks by national authorities, after having consulted the EBA.").

[88] EUROPEAN COMMISSION, *supra* note 75 ("[T]he RTS is due to become applicable around September [14,] 2019.").

will continue to adopt TSP financial services.[89] But if the United States is to adopt the most pro-consumer data aggregation model, effectively stating that consumers own their financial data is at least a mandatory first step.[90] Consumer consent should also be at the forefront of any decision to share or transmit financial data. The scope of data shared ought to be considered immediately thereafter. At first glance, these factors read as if APIs are the solution to a pro-consumer data aggregation model, but this judgment is hasty. The jury is still out in deciding the case of screen scraping versus APIs as the better data aggregation method. Both methods have their own advantages. Screen scraping is cheap, creates more competition in the TSP space, and consumers have become accustomed to sharing login credentials with TSPs.[91] APIs do not appear to be as clear of a choice as they are on paper, with both limiting competition due to its cost and being less secure than once thought.[92] Yet, APIs allow financial institutions to define the scope of personal data shared and allow consumers to revoke data aggregator's permission to collect their data at the touch of a button on the financial institution's online platform.[93]

The way forward, as of this instant in time, is through discussion amongst all of the interested parties: consumers, data aggregators, TSPs, and financial institutions. Some of the leading data aggregators have already joined together to make their own data aggregation framework.[94] Despite the Consumer Protection Principles, the CFPB

---

[89] Gulamhuseinwala et al., *EY FinTech Adoption Index 2017*, EY (2017), https://www.ey.com/Publication/vwLUAssets/ey-fintech-adoption-index-2017/$FILE/ey-fintech-adoption-index-2017.pdf (finding 87 percent of consumers prefer a FinTech application over a similar application provided by a traditional financial service provider).

[90] CONSUMER FINANCIAL PROTECTION BUREAU, *supra* note 8. (stating that although the CFPB published 9 non-binding standards pointing to user ownership of their data, these principles do little to show how FI's must share data with consumers).

[91] *Treasury Report*, *supra* note 15, at 33 ("[C]onsumers have to some extent become conditioned to opt for convenience over security[.]").

[92] *See* Dep't of Media Relations, *supra* note 54; *see also Treasury Report*, *supra* note 15, at 26.

[93] *Hearing*, *supra* note 1, at 39. ("consumers should be able to monitor those account access rights and direct their financial institution to revoke that if they so desire.").

[94] Ron Barasch, *Statement of Joint Principles for Ensuring Consumer Access to Financial Data*, YODLEE (May 11, 2018), https://www.yodlee.com/blog/envestnet-yodlee-quovo-and-morningstar-byallaccounts-statement-of-joint-

has chosen to remain on the sidelines by not actively implementing any regulation on the matter. While some financial institutions argue that the CFPB did not stay sidelined and implicitly denounced screen scraping in its issued Consumer Protection Principles, there still has been no rulemaking from the CFPB.[95] Allowing the industry to self-regulate is a true *laissez-faire* approach and it seems to be the correct stance as the security concerns about screen scraping only remain as *concerns* and have not come to fruition. Without being able to point to an example of a breach, the debate about screen scraping is better characterized as a debate about the question presented earlier: whether financial institutions are required to facilitate all means of data sharing for TSPs.[96] On this point, self-regulation may not help those TSPs who are blocked from accessing financial data through screen scraping.[97] Although, the bottom line established is that financial institutions are not in the clear to withhold financial data from its consumers.[98] The CFPB's hands-off approach will work for now, but if financial data is truly less secure than we previously thought, then the focal point of the

---

principles-for-ensuring-consumer-access-to-financial-data/ [https://perma.cc/Q3RH-796P].

[95] CONSUMER FINANCIAL PROTECTION BUREAU, CONSUMER ACCESS TO FINANCIAL RECORDS (Spring 2019), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=201904&RIN=3170-AA78 [https://perma.cc/WT6E-65K5] (designating the proposed rule as "priority: substantive, nonsignificant" and agenda stage of rulemaking as "Long-Term Actions"); CONSUMER FINANCIAL PROTECTION BUREAU, *supra* note 8, at 3 ("Access does not require consumers to share their account credentials with third parties."); Fonte, *supra* note 8 ("But it is unclear if this means that [financial institution]s can prohibit consumers from sharing their account credentials and require third parties to access consumer data through an API, or if prohibiting credential sharing would deter consumers from access since such a ban on the practice would make many fintech products and services currently offered unavailable.").

[96] Penny Crosman, *A CFPB Policy Everybody Seems to Like (Really)*, AMERICAN BANKER (Oct. 20, 2017), https://www.americanbanker.com/news/a-cfpb-policy-everybody-seems-to-like-really ("The whole debate over credentials is really a debate over whether or not financial institutions are really, honestly sharing consumer data with their permission with third parties.").

[97] Such as those companies blocked by JP Morgan. *See* JPMorgan, *supra* note 42.

[98] Beam et al., *supra* note 5, at 2. ("[The CFPB believes that] consumers should be able to access this information and give their permission for third-party companies to access this information as well").

issue will switch from market competition back to data aggregation security concerns. If push comes to shove, the CFPB may implement some PSD2-esque rulemaking, which could have some drastic consequences to TSPs relying on screen scraping.[99]

Zachary Zehner[100]

[99] Fonte, *supra* note 8. (stating that the CFPB has yet to make binding rules on this subject matter).
[100] Student, Boston University School of Law (J.D. 2021).