VOLUME 3 FEBRUARY 2022 ISSUE 1

JOURNAL ON EMERGING TECHNOLOGIES

© 2022 by the Notre Dame Journal on Emerging Technologies

NOTE

TRUST IN THE DIGITAL MARKETPLACE: AMAZON, THIRD-PARTY SELLERS, AND INFORMATION FIDUCIARIES

Jesse-Paul Crane

TRUST IN THE DIGITAL MARKETPLACE: AMAZON, THIRD-PARTY SELLERS, AND INFORMATION FIDUCIARIES

*Jesse-Paul Crane**

The rise of e-commerce has created a number of online marketplaces where digital platforms connect buyers and sellers. Consumers use platforms like Amazon, Etsy, Instacart, Uber, Lyft, and Airbnb to purchase goods and services from third parties while the platform itself takes a fee for operating the marketplace. Online platforms are not the only businesses that use such a "two-sided" marketplace model. The Supreme Court recently addressed antitrust concerns in this type of marketplace in Ohio v. Am. Express Co.[1] *Two-sided markets invoke a number of novel legal issues that impact both those who buy and sell over them, most prominently in the field of antitrust and consumer protection.*

Among these online marketplaces, Amazon has recently come under intense scrutiny from regulators in the European Union and the United States. Amazon is part of a quartet of American tech companies, joined by Facebook, Google, and Apple, that have raised alarm bells over their seemingly ever-increasing market power. Critics of these companies' business practices have urged aggressive antitrust and consumer protection enforcement actions.

Using its significant resource advantage, Amazon has allegedly developed cheaper versions of successful products that undercut sales for the product of the original third-party seller who developed it. While antitrust remains perhaps the most obvious means of addressing such competition concerns, existing antitrust jurisprudence in the United States presents considerable hurdles because Amazon's allegedly anticompetitive behavior, while perhaps unfair to merchants, likely benefits consumers by providing lower prices.

Rather than view this behavior exclusively through the lens of antitrust or consumer protection law, this Note will advance the position that Amazon, and other operators of online marketplaces' use of third-party commercial data, should be regulated under a fiduciary-like standard. This approach adopts the spirit of Jack Balkin's information fiduciary concept, but after analyzing its application in the e-commerce concept, argues in favor of a more concrete regulatory approach. By drawing

* Juris Doctor Candidate, Notre Dame Law School, 2022; Bachelor of Arts in Economics, Boston University, 2014. Many thanks to Professor Patrick Corrigan for his enthusiastic guidance as my advisor for this Note. I also want to express my gratitude to my friends and family, especially my fiancée, for their unending love and support in my journey through law school.

[1] 138 S. Ct. 2274 (2018).

from existing data protection regulations in the healthcare and securities sectors, Congress or a regulatory agency could impose a standard of data use that would instill greater trust in online marketplaces between merchants and platforms.

The consolidation of significant market power in the hands of one or only a few private companies has long been a cause of major concern for policymakers in the United States. Fear of corporate "trusts" during the late nineteenth and early twentieth centuries led to the development of antitrust law in the United States.[2] Throughout the course of the twentieth century, and especially after the end of the Cold War, the idea that governments should set and enforce competition policy spread outside the United States, most notably in the European Union.[3] The timing of the expansion of antitrust law roughly coincided with the development of the internet, and so it is fitting that the internet poses some of the biggest questions for the future of this area of the law. The proliferation of online platforms has been a cause of anxiety for policymakers, as many of these online companies have embraced Facebook's formerly unofficial motto to "move fast and break things."[4]

While antitrust law spread globally at the end of the twentieth century, it has remained a creature of the nineteenth century in many ways. In the United States, antitrust law prohibits monopolistic tactic.

---

[2] TIM WU, THE CURSE OF BIGNESS: ANTITRUST IN THE NEW GILDED AGE, 17 (2018).

[3] Consolidated Version of the Treaty on the Functioning of the European Union art. 101, May 9, 2008, 2008 O.J. (C115) 88–89 (prohibiting "all agreements between undertakings, decisions by associations of undertakings and concerted practices which may affect trade between Member States and which have as their object or effect the prevention, restriction or distortion of competition within the internal market"); Lei Nº 12.529, de 30 de Novembro de 2011, Diário Oficial da União D.O.U. de 1.12.2011 (Braz.), available at http://en.cade.gov.br/topics/legislation/laws/law-no-12529-2011-english-version-from-18-05-2012.pdf/view (establishing a Brazilian competition law authority and setting "forth preventive measures and sanctions for violations against the economic order, guided by the constitutional principles of free competition, freedom of initiative, social role of property, consumer protection and prevention of the abuse of economic power"); Competition Act 89 of 1998 § 2 (S. Afr.), available at https://www.gov.za/sites/default/files/gcis_document/201409/a89-98.pdf, (with the purpose to "promote and maintain competition").

[4] *See* Drake Baer, *Mark Zuckerberg Explains Why Facebook Doesn't 'Move Fast And Break Things' Anymore*, BUSINESS INSIDER (May 2, 2014), https://www.businessinsider.com/mark-zuckerberg-on-facebooks-new-motto-2014-5 (explaining why Facebook no longer uses the motto "Move Fast and Break Things").

that restrain trade to the detriment of consumer welfare.[5] The proliferation of online platforms has disrupted consensus among antitrust practitioners as to whether antitrust should remain focused only on market power that harms consumers, or whether antitrust should expand its purview to protect "competitive structures" in order to mitigate consolidation of the type currently seen in markets in which online platforms operate.[6]

This brings us to Amazon. One of the world's largest online retailers, Amazon controls about thirty-eight percent of the United States' e-commerce market.[7] But Amazon is more than just an online retailer; it also provides cloud computing services and hosts an online marketplace, Amazon Marketplace, where third-party sellers sell goods to buyers.[8] Amazon also manufactures and sells its own goods under the Amazon Basics label.[9] Moreover, Amazon is a highly vertically integrated firm that owns its shipping and fulfillment services.[10] This integration has made possible free, two-day shipping to "Amazon Prime" members, customers who pay an annual subscription fee in exchange for speedy delivery, among other perks.[11] Amazon's size, diverse business line, and integrated services provide consumers with a cheap and efficient online retail experience. Despite a lack of serious competition in the online retail space, Amazon's prices remain reasonable, and purchasers continue to buy more and more through Amazon.

The picture for third-party sellers is, at least anecdotally, not as rosy. Amazon's network effect provides major benefits to third-party sellers: access to a large customer base, reduced advertising costs, and a robust shipping network. But Amazon's size means selling on its marketplace brings some major drawbacks. Sellers feel that they must operate on Amazon Marketplace or else lose out on a significant chunk

---

[5] The Sherman Act, 15 U.S.C § 1 (2018). The federal courts have consistently interpreted the Sherman Act and subsequent antitrust legislation to require a showing of consumer harm to prove a violation. Nat'l Collegiate Athletic Ass'n v. Bd. of Regents of Univ. of Oklahoma, 468 U.S. 85, 107 (1984); *see* A.A. Poultry Farms, Inc. v. Rose Acre Farms, Inc., 881 F.2d 1396, 1401 (7th Cir. 1989) (interpreting § 2 of the Clayton Act).

[6] Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 737 (2017). Marshall Steinbaum & Maurice E. Stucke, *The Effective Competition Standard: A New Standard for Antitrust*, 87 UNIV. OF CHI. L. REV. 595, 601-02 (2020).

[7] STATISTA, E-COMMERCE IN THE UNITED STATES, 14 (2020), available at https://www.statista.com/study/28028/e-commerce-in-the-united-states-statista-dossier/.

[8] *What We Do*, AMAZON, https://www.aboutamazon.com/what-we-do.

[9] *Amazon Basics*, AMAZON, https://www.amazon.com/Amazon_Basics.

[10] Nick Statt, *Amazon is delivering half its own packages as it becomes a serious rival to FedEx and UPS*, THE VERGE (Dec. 13, 2019), https://www.theverge.com/2019/12/13/21020938/amazon-logistics-prime-air-fedex-ups-package-delivery-more-than-50-percent.

[11] *Amazon Prime*, AMAZON, https://www.amazon.com/amazonprime.

of potential revenue.[12] While other online platforms like Walmart.com and eBay host marketplaces similar to Amazon's, their customer bases are dwarfed by Amazon's. As a result, according to one third-party merchant, Walmart.com and eBay marketplaces account for a miniscule portion of sales.[13] Lack of competition for sellers means that they cannot vote with their feet and move to a different platform if they feel the charges that they pay are unfair or if they feel that Amazon's practices toward them are abusive. There is great potential for abuse by a marketplace operator who also sells its own goods.

Unlike a normal marketplace, where competitors operate on roughly an equal informational footing, Amazon competes with a significant advantage: it knows what its competitors are doing. Amazon tracks a significant amount of data from third-party sellers, including sales numbers, prices, and how frequently buyers are viewing a particular product.[14] According to allegations from third-party sellers, Amazon has used this data to drive the development of its own products, which it then promotes above the goods of third-party sellers in customer search results, siphoning away their sales.[15]

---

[12] Dana Mattioli, *Amazon Scooped Up Data From Its Own Sellers to Launch Competing Products*, WALL ST. J., (April 23, 2020), https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015.

[13] Molson Hart, *How Amazon's Business Practices Harm American Consumers: Why Amazon Needs a Competitor and Why Walmart Ain't It*, MEDIUM, (Jul. 18, 2019), https://medium.com/swlh/amazon-needs-a-competitor-and-walmart-aint-it-5997977b77b2. While the self-reported data of a single third-party merchant should never be held up as definitive proof of this phenomenon, Hart's claims comport with the consequences of the network effect. The platform effect holds that in online spaces, the more users gather on a particular platform, the more other users will adopt that platform. Evgeny Morozov, *Where Uber and Amazon rule: welcome to the world of the platform*, THE GUARDIAN (Jun. 6, 2015), https://www.theguardian.com/technology/2015/jun/07/facebook-uber-amazon-platform-economy. Because Amazon has the most third-party sellers and consequently the widest variety of goods, buyers will tend to congregate, or at least look first at Amazon. Justus Haucap & Ulrich Heimeshoff, *Google, Facebook, Amazon, eBay: Is the Internet Driving Competition or Market Monopolization?*, 11 INT'L ECON. & ECON. POLICY 49, 50–51 (2014). Third-party sellers recognize this dynamic and consequently even more will participate in Amazon Marketplace. *Id.* at 51.

[14] Mattioli, *supra* note 12.

[15] Annie Palmer, *Amazon Uses Data From Third-party Sellers to Develop Its Own Products, WSJ Investigation Finds*, CNBC (Apr. 23, 2020, 3:25 PM), https://www.cnbc.com/2020/04/23/wsj-amazon-uses-data-from-third-party-sellers-to-develop-its-own-products.html (last visited Dec. 18, 2020); *see also* Spencer Soper & Ben Brody, *Amazon Probed by U.S. Antitrust Officials Over Marketplace*, BLOOMBERG LAW (Sept. 11, 2019, 5:00 AM), https://www.bloomberglaw.com/product/blaw/document/X9PATQOC000000?criteria_id=9d6d12c6a18c8ad6d7d29c1d2b180ed2&searchGuid=ac14a7c7-440c-4295-86fc-a3c499e508d1&search32=MP9EnbamJZMkZljgQgvTaQ%3D%3DEiGvOz2-

B. Do We Need Intervention? Why not Antitrust Alone?

Is this simply the cost of doing business online? Does this require structural changes?[16] There is certainly a risk, at least from a consumer welfare perspective, of over-intervention. Amazon provides consumer goods at affordable prices with prompt delivery right to purchasers' doorsteps. Evidence suggests that these consumer benefits are only possible due to the interplay between Amazon's retail business, Amazon Marketplace, and Amazon's cloud computing arm, Amazon Web Services.[17] Disrupting the present structure of the corporation, through, for example, breaking up the firm into distinct parts might leave one or more of the pieces of a split-up Amazon as non-viable.[18]

Amazon has fallen squarely in the sights of a number of antitrust reformers who argue that it and other large tech companies represent a breakdown of the American antitrust tradition. A number of critics of the existing antitrust regime, Tim Wu and Lina Kahn among them, have argued that American antitrust has drifted too far away from its origins.[19] These "neo-Brandesians," so named because they trace their intellectual

---

K1s8TlH3COyeyT52qeatj6mx5OTuzmKgmPCccZseGjy6kbY6Bj959yQmMiLgyD8-nRVmDYHM880I_Ih8ZmR96X8BXcz9PXXsZ7QnQCTxETiD5_SQrNLdaQVJMZZfGjzbttEpdmgkWvOM9n88yLQySWZ5ZjqpeVvtyjiAKLVOHsP9g943vNosINb2pzoQHbzrCocMIWy4ZlSPrSnuqaeperU8Fw2Bk-sxCsuZz306iQ3L6xfWSBe8_Z_r (last visited Dec. 18, 2020).

[16] An individual third-party seller harmed by this alleged practice might have an individual cause of action for, say, patent infringement or unfair competition, depending on the nature of how their data was used. Depending on how widespread the alleged practice of the use of sales data to drive platform retail sales is among Amazon and other online platforms, addressing this phenomenon through one-off litigation may be a sufficient deterrent to prevent abuse. However, if this is a widespread phenomenon, not only would such abuse entrench Amazon's position in the market, but it could also potentially flood courts with litigation.

[17] John D. Stoll, *Amazon is a Giant. But Bigness isn't a Crime.*, WALL ST. J. (Sept. 21, 2018), https://www.wsj.com/articles/amazon-is-a-giant-but-bigness-isnt-a-crime-1537534900.

[18] Annual reports show that Amazon's cloud computing business is actually the source of much of its profits, so splitting AWS apart from the other two business segments could leave the consumer goods components in a situation where they would have to raise prices to remain profitable (or perhaps even viable). *See* Felix Richter, *Cloud Business Drives Amazon's Profits*, STATISTA (Apr. 26, 2019), http://www.statista.com/chart/9174/amazon-operating-profit/ (last visited Feb. 11, 2021). Cross-subsidization across a firm's business units is common and might be a way for Amazon to continue to grow its retail business's market share without raising prices. *See* Khan, *supra* note 6, at 747. A full analysis of whether Amazon's retail arm could survive without Amazon Web Services is well beyond the scope of this note or this author's ability. I raise this point only to say that if courts arrive at the point where they are considering structural antitrust remedies, they should be cognizant of cross-subsidization within a firm as internal financial ecosystems may be fragile. It seems possible that an overly aggressive approach could lead to a competitor exiting a market rather than more robust competition.

[19] *See generally* Wu, *supra* note 2; Khan, *supra* note 6.

lineage back to United States Supreme Court Justice Louis D. Brandeis, argue that contemporary antitrust law is overly focused on consumer welfare, a term never used in the Sherman Act, and ignores other drivers for the creation of the American antitrust regime, like ensuring that markets are not consumed by one or only a few competitors.[20] These commentators point to online platforms as examples of entities that monopolize markets but cannot be reined in by conventional antitrust law since they do not cause *financial* harm to *consumers*, but cause (non-monetary) damage to consumers and (financial) harm to competitors through the misuse of both groups' data, among other issues.[21]

The case for intervention ultimately leans on the normative value judgments at the heart of the current debate within American antitrust law. Do we return to a vision of antitrust based on the populist energy that drove the passage of the Sherman Act in 1899? Such a turn could decrease market efficiency in the short term, at least in terms of the prices that consumers pay for goods. But, in return, consumers could also benefit from having greater competition for their business and, perhaps, lower prices and better service in the long run. Small-scale capitalists, like Amazon's third-party sellers, could also benefit since they would be competing on a (slightly) less-tilted playing field.

Or should we strive for market efficiency? According to this viewpoint, Amazon has gained a dominant position in online commerce by offering a superior product and its success is self-promulgating through the network effect, not anticompetitive tactics.[22] If there are one-off instances of abusive behavior toward third-party sellers on Amazon Marketplace, those should be handled through litigation. Overly vigorous enforcement of antitrust will simply harm Amazon, consumers, and ultimately third-party sellers.[23]

While the harm surrounding Amazon's use of third-party seller's data has largely been anecdotal thus far, the Federal Trade Commission and the European Commission have both recently opened investigations into Amazon's practices surrounding seller's data collection.[24] The European Commission is further along in its investigation and has alleged that "Amazon systematically rel[ies] on non-public business data of independent sellers who sell on its marketplace, to the benefit of

---

[20] Wu, *supra* note 2, at 17-19.
[21] Khan, *supra* note 6, at 720-21.

[22] Stoll, *supra* note 17.
[23] *Id.*
[24] Soper & Brody, *supra* note 15; Press Release, European Commission, Antitrust: Commission Sends Statement of Objections to Amazon for the Use of Non-Public Independent Seller Data and Opens Second Investigation into its E-Commerce Business Practices (Nov. 10, 2020) (on file with author) [hereinafter European Commission].

Amazon's own retail business, which directly competes with those third party sellers."[25]

While hefty fines could undermine the rationale for misusing third-party sellers' data, without knowing how widespread the issue is, enforcement agencies run the risk of either under or over deterring this behavior. On a more basic level though, American antitrust authorities face an uphill battle of actually succeeding in these actions.[26] Given the lack of an essential facility doctrine in US antitrust law and the durability of the consumer welfare standard, Amazon may not have committed a cognizable offense by using its controlling position to examine competitors' data.

Antitrust alone, even if there was a consensus to break up Amazon, for example, might not be enough to mitigate future abuses of similar data. Even if there were many e-commerce platforms, none of which competed with third-party sellers, the value of sales data might drive them to monetize it differently than Amazon, but in a no less harmful way. Antitrust remedies may be only one of a constellation of necessary reforms to enable small-scale capitalists to succeed on the internet.[27] Third-party sellers need assurances that their commercial data will be safe online.

C. Sellers Face Significant Challenges in Online Marketplaces

The antitrust dilemma means that, although there is a growing consensus in favor of bringing enforcement actions against Amazon for the misuse of third-party seller data, such enforcement efforts face an uphill battle. Even if these efforts were to succeed, so long as third-party sellers have to operate on an e-commerce platform, their data could be at risk for misuse by the platform operator. While competition between platforms could be beneficial to third-party sellers, in that they have the option to switch to a competing platform if one platform abuses data, for

---

[25] European Commission, *supra* note 24.

[26] European antitrust law has made a number of different normative choices from American law, which enables greater regulatory intervention. One of the most prominent diversions is that European law acknowledges the existence of certain "essential facilit[ies]." Commission Decision 94/119 of 21 December, 1993, concerning a refusal to grant access to the facilities of the port of Rødby, 1993 O.J. (L 55) 12. This doctrine holds that private actors cannot refuse to deal with other market participants if, for some reason, competitors cannot operate in a given market without dealing with that private actor. *Id.* US antitrust law does not recognize this doctrine, see Verizon Commc'ns v. Trinko, 540 U.S. 398 (2004), and holds that antitrust law protects competition, not competitors. Brunswick Corp. v. Pueblo Bowl-O-Mat, Inc., 429 U.S. 477, 488 (1977) (quoting Brown Shoe Co. v. United States, 370 U.S. 294, 320 (1962)).

[27] Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F. 11, 20-22 (2020) [hereinafter *The Fiduciary Model of Privacy*].

a number of reasons, sellers face a number of costs when switching platforms.

First are the reputational costs. Buyers rank the quality of third-party sellers' goods, which is then visible to other prospective buyers. Changing platforms means a seller loses its reputation and must start cultivating a reputation through ratings on the new platform.[28] Second is the risk of different customers on different platforms. If your business is focused on selling novelty train sets, and the novelty train set community is very active on Platform A, but not Platform B, a train set seller may have difficulty transferring its business to Platform B since it might need to invest in advertising to its prospective customers that it has moved to a different e-commerce platform.[29] Given the network effects that attract and keep customers on a single platform, like Amazon Prime memberships, customers may be unwilling to change platforms along with a business. While neither of these factors is insurmountable for a third-party seller, both highlight that greater competition may not be a perfect panacea for the problems small-scale capitalists confront online.

One of the core risks that third-party sellers face is the abuse of data.[30] Sellers on Amazon Marketplace necessarily hand over reams of data about their business to one of their competitors.[31] Given that sensitive data may be abused in many more ways than just to compete unfairly, it might be appropriate to subject online marketplace operators to a duty to safeguard market participants' data.

---

[28]Haucap and Heimeshoff, *supra* note 13, at 54. One potential way to mitigate this cost for third-party sellers is with concept of data portability, i.e. a user of an online service would be able to move his or her user data from one platform to another. This was one of the innovations of the General Data Protection Regulation (GDPR) of the European Union. While many US-based users benefit from the GDPR's data portability scheme since online platforms cannot (or choose to not) segregate US-based users and EU-based users and extend many of its features to all users, there is currently no requirement in US Federal law requiring data portability. The California Consumer Privacy Act establishes a right for users to transfer data across platforms "to the extent technically feasible." Cal. Civ. Code § 1798.100(d).

[29] Haucap and Heimeshoff*, supra* note 13, at 57–58.

[30] "53% [of Amazon sellers] say Amazon sells its own products that directly compete with the seller's [and] 46% of sellers are concerned about Amazon protecting their privacy and security." *State of the Amazon Seller Survey*, JUNGLE SCOUT (2020), https://www.junglescout.com/wp-content/uploads/2020/02/State-of-the-Seller-Survey.pdf (last visited Dec 14, 2020).

[31] According to the Wall Street Journal, Amazon employees are able to generate reports on Amazon's third-party sellers that include average selling price, revenue, advertising per unit, and shipping costs. Mattioli, *supra* note 12.

II. APPLYING THE INFORMATION FIDUCIARY DUTY TO THE THIRD-PARTY SELLER-PLATFORM RELATIONSHIP

A. The Duties of an Information Fiduciary

One solution for commercial data abuses that stands as an alternative to antitrust would be making online marketplace operators "information fiduciaries" with the third-party sellers as beneficiaries. The information fiduciary concept has been articulated by Jack Balkin and it posits that online platforms owe a fiduciary duty to users where they not only must protect users' data, but also must only use consumer data in good faith.[32] The aim of Balkin's proposal is to impose the duty of care, loyalty, and confidentiality on digital platforms that gather personal information—akin to the duties that existing fiduciaries, like lawyers and doctors, owe to their clients and patients.[33]

While the information fiduciary concept is far from generally accepted, it has gained traction in proposed federal and state legislation.[34] Although, this concept is mainly geared toward the abusive use of personal consumer data in social media, its extension to protect commercial data is a natural outcropping. Importing fiduciary law into the context of seemingly arm's-length transactions between a platform and merchants might be counterintuitive at first, because fiduciary duties often imply a relationship of trust and confidence, and arm's-length commercial relationships rarely rise to such a level.[35]

---

[32] *See generally*, Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016) [hereinafter *Information Fiduciaries and the First Amendment*]; Jack M. Balkin, *Information Fiduciaries in the Digital Age*, BALKINIZATION (2014), https://balkin.blogspot.com/2014/03/information-fiduciaries-in-digital-age.html (last visited Dec 11, 2020) [hereinafter *Information Fiduciaries in the Digital Age*]; *The Fiduciary Model of Privacy*, *supra* note 27; Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, THE ATLANTIC (Oct. 3, 2016), https://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346/ (last visited Dec 7, 2020) [hereinafter *A Grand Bargain*].

[33] *A Grand Bargain*, *supra* note 32; *Information Fiduciaries and the First Amendment*, *supra* note 32, at 1207–09.

[34] Data Care Act of 2018, 115th Cong. § 3(4) (2018) (imposing a duty of loyalty on any entity that "(A) is engaged in interstate commerce over the internet or any other digital network; and (B) in the course of business, collects individual identifying data about end users, including in a manner that is incidental to the business conducted"); New York Privacy Act, S. 5642, 2020 Leg., 203d Sess. §1102(1) (N.Y. 2020) (requiring " every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer, without regard to the interests of the entity, controller or data broker").

[35] Murphy v. Kuhn, 682 N.E.2d 972, 974-75 (N.Y. 1997) (finding that an insurance agent-insured relationship is a commercial relationship that does not impose any

Under proposed legislation that draws on Balkin's data fiduciary framework, Amazon would likely be considered an information fiduciary to consumers (but not third-party sellers) since users hand over personal data.[36] Broadly speaking, data aggregators would owe a duty of confidentiality so as to not reveal sensitive user information.[37] They would also owe users a duty of care. A platform may breach its duty of care by inadequately protecting data from third-party hackers, or it may breach its duty by attempting to cover up data breaches and then failing to inform users that their data was compromised.[38] Finally, they would owe users a duty of loyalty so as to not place themselves in a conflicted position vis-à-vis the data beneficiary.[39]

But the contours of these duties in the digital context, especially the duty of loyalty, are not yet well-defined. For instance, is *any* type of targeted advertising a breach of the duty of loyalty? The Data Care Act of 2018 identifies the use of individual-identifying data that will "benefit the online service provider to the detriment of an end user and will result in reasonably foreseeable and material physical or financial harm to an end user" as a breach of the duty of loyalty.[40] This seems to target advertising that, for example, might induce a recovering gambler to relapse. But is the duty narrow enough to exclude situations where someone simply overspends due to a well-placed ad? Does it matter if one data fiduciary, say Facebook, uses data gathered by another data fiduciary, like Amazon, for targeting advertising? While the data fiduciary model has the benefit

---

special duties); Protocol Techs., Inc. v. J.B. Grand Canyon Dairy, L.P., 406 S.W.3d 609, 616 (Tex. App. 2013) (no agency relationship—and thus no fiduciary duties—between a buyer and a seller of a dairy farm because the contract specifically identified the relationship as commercial and the requirement for establishing a joint venture were not met).

[36] Under the New York Privacy Act, *supra* note 34, Amazon would be considered a controller because it "determines the purposes and means of the processing of personal data." §1100(4). Personal data is defined as, among other things, name, postal address, credit card number, purchasing or consuming history, search history, or password and username. § 1100(10)(a)(i)-(x). Likewise, Amazon would likely be considered an information fiduciary under the Data Care Act of 2018 because it "is engaged in interstate commerce over the internet or any other digital network; and in the course of business, collects individual identifying data about end users, including in a manner that is incidental to the business conducted." *Supra* note 534, at § 2(4). The Data Care Act of 2018 takes an even broader view of what type of data triggers fiduciary responsibilities, defining individual identifying data as "any data that is collected over the internet or any other digital network; and linked, or reasonably linkable, to a specific end user; or a computing device that is associated with or routinely used by an end user." The Data Care Act of 2018, *supra* note 34, at § 2(3).

[37] The Data Care Act of 2018, *supra* note 34, at § 3(b)(3); New York Privacy Act, *supra* note 34.

[38] The Data Care Act of 2018, *supra* note 34, at § 3(b)(1); New York Privacy Act, *supra* note 34.

[39] The Data Care Act of 2018, *supra* note 34, at § 3(b)(2); New York Privacy Act, *supra* note 34.

[40] The Data Care Act of 2018, *supra* note 34, at § 3(b)(2).

of elegance, its broad mandates may leave digital platforms in a position where there is a fundamental mismatch between a platform's targeted advertising business and its fiduciary duties.[41] More fundamentally, the public may be left uncertain as to which data collection practices are acceptable and which constitute a violation of their privacy rights due to the indeterminacy of the duties. Additionally, it is also not clear in all contexts how data beneficiaries would become independently aware of breaches of the duty of loyalty beyond voluntary disclosures or independent investigations into data platforms.[42]

As Lina Khan and David Pozen have pointed out, the imposition of fiduciary duties upon online platforms introduces the potential for inescapable conflicts of interest due to dual loyalties.[43] First and foremost, corporations owe fiduciary duties to their shareholders—and that duty often boils down to maximizing shareholder value.[44] In the context of Amazon Marketplace, Amazon could potentially breach its duty toward shareholders by *not* frontrunning third-party merchants since it would abdicate a potential source of revenue.

Amazon could argue that its strategy of protecting merchants' information and not frontrunning them by introducing competing products is ultimately profit-maximizing because it would attract more merchants or encourage existing merchants to devote more effort toward selling over Amazon Marketplace, ultimately netting greater fees and sales for Amazon. While Khan and Pozen's critique of conflicts between shareholders and companies trying to adhere to the information fiduciary duty was in the context of harvesting of *consumer* data that would consequently be used for targeted advertising, the core source of revenue for a company like Facebook, it is not clear that their critique is valid in every situation of platforms' use of data and that this necessarily results in a divided loyalty.

---

[41] Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497, 515 (2019).

[42] *Id.* Amazon Marketplace, however, presents a potentially manageable context in which the information fiduciary duty could be enforced with more limited monitoring costs than social media platforms. Because vendors can independently track (1) their sales, (2) their position in Amazon's results, and (3) the presence of competition from Amazon, they would be able to identify if and when Amazon is potentially behaving in an abusive manner.

[43] *Id.* at 508-10. Khan and Pozen's main critique of the information fiduciary concept is that it would ultimately undermine building the political will to challenge online platforms' structural powers. *Id.* at 536-37. By legally enshrining a relationship of trust and confidence between users and platforms, platforms would simply gain another advantage in maintaining their dominant market position. *Id.* at 536-537. Given the difficulties of detecting breaches of the information fiduciary duty and the ambiguous avenues for enforcing it, platforms ultimately may not have to change their behavior even though they are theoretically subjected to a heightened duty. *Id.* at 524-25.

[44] *Id.* at 508.

There is also a potential conflict of interest between a theoretical duty toward third-party sellers and a theoretical duty toward *consumers*, a classic reason sometimes cited as to why the imposition of fiduciary duties on market makers in securities markets is inappropriate.[45] If Amazon were to be an information fiduciary for merchants, is there an equally compelling rationale to say that it should be an information fiduciary for buyers as well? To be sure, Amazon collects some data from consumers. Much of it is fairly expected and linked to use of Amazon services, like order history and payment methods.[46] But there is a potential for conflict because Amazon also uses data for targeted advertising and shares deidentified data with third parties.[47]

If Amazon and a merchant were to sell the same good in the marketplace, and the Amazon product was a better fit for a consumer and was consequently promoted to that consumer, would this constitute a breach of the information fiduciary duty to the seller? Is there a conflict in this case, where Amazon would necessarily breach its duty of loyalty to one or both participants? It is not possible to reconcile this conflict in the Amazon Marketplace context.

B. Proposed Information Fiduciary Legislation Only Protects Personal Data

Balkin's paradigmatic information fiduciary is a social media platform that gathers sensitive data about individual users.[48] Examples of such information include name, location, internet protocol (IP) address, physical characteristics, or details about a user's social circle. This information is sensitive because it provides avenues for companies to pry into the private lives of users in a way well beyond what they intended to provide a social media platform. Above all though, the

---

[45] "'Markets would not work, if market makers were a fiduciary. What would a market maker do if he had a buyer and seller simultaneously approach him? . . . He can't be a fiduciary to one and not the other. He can't be a fiduciary to both.'" Stanislav Dolgopolov, *A Two-Sided Loyalty: Exploring the Boundaries of Fiduciary Duties of Market Makers*, 12 U.C. DAVIS BUS. L.J. 31, 33 (2011) (quoting Tom Braithwaite & Francesco Guerrera, *Goldman Lobbies Against Fiduciary Reform*, FIN. TIMES, May 12, 2010, at 4).

[46] *Amazon.com Privacy Notice*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=GX7NJQ4ZB8MHFRNJ#GUID-8966E75F-9B92-4A2B-BFD5-967D57513A40__SECTION_467C686A137847768F44B619694D3F7C (last visited Feb. 14, 2021).

[47] *Interest-Based Ads*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=202075050 (last visited Feb. 14, 2021).

[48] Information Fiduciaries and the First Amendment, *supra* note 32, at 1188-89.

platform owes the duties of loyalty, care, and secrecy to a *natural* person to protect *personal data*.[49]

The examples that Balkin points to as the original information fiduciaries—doctors and lawyers—owe fiduciary duties to natural persons so as to facilitate their clients and patients to be open and honest with them.[50] While doctors can only have a natural person as a patient, lawyers owe fiduciary duties to non-natural persons like a corporation when they serve as corporate counsel.[51] Is there a rationale for including or excluding non-natural persons from serving as beneficiaries of information fiduciaries?

Thus far, reformers like Balkin have not spoken directly one way or the other. However, there is a raft of proposed state and federal legislation inspired by Balkin that has adopted the information fiduciary model but limited potential beneficiaries to natural persons. The proposed Data Care Act of 2018 imposes a duty of loyalty upon online service providers where online service providers cannot "use individual identifying data, or data derived from individual identifying data, in any way that . . . will benefit the online service provider to the detriment of an end user; and . . . will result in reasonably foreseeable and material physical or financial harm to an end user; or . . . would be unexpected and highly offensive to a reasonable end user."[52] The Act defines end user as an "individual who engages with an online service provider or logs into or uses services provided by the online service provider over the internet or any other digital network."[53] Because an end user is defined as an individual, a non-natural person would not benefit from the duties imposed upon online service providers.

Legislation proposed in New York that has adopted the information fiduciary approach similarly restricts the beneficiaries of these fiduciary duties to natural persons. New York Senate Bill 5642 states that "every controller and data broker, which collects, sells or licenses personal information of consumers, shall exercise the duty of care, loyalty and confidentiality expected of a fiduciary with respect to securing the personal data of a consumer against a privacy risk; and shall act in the best interests of the consumer."[54] A consumer is defined as "a natural person who is a New York resident. It does not include an

---

[49] *Id.* at 1221.
[50] *Id.* at 1226-27.
[51] *See* Schaeffer v. Cohen, Rosenthal, Price, Mirkin, Jennings & Berg, P.C., 541 N.E.2d 997, 1002 (Mass. 1989).
[52] Data Care Act of 2018, *supra* note 34, at § 3(b)(2).
[53] *Id.* at § 2.
[54] New York Privacy Act, *supra* note 34, at § 1102(1).

employee or contractor of a business acting in their role as an employee or contractor."[55]

The nature of data collected about individuals is likely qualitatively different from what would be collected about commercial entities. Data surrounding a natural person's health, financial wellbeing, political or religious beliefs, sexual orientation, gender identity, or employment status (among a myriad of other data points) could impact that person's access to housing, healthcare, or employment. The stakes are much higher when securing a natural person's sensitive data than a commercial entity's sensitive data.

The mistreatment of commercial information could also have an adverse impact on a business, however. As the allegations surrounding Amazon's treatment of data gathered from sellers who participate in Amazon Marketplace demonstrate, the misappropriation of data surrounding sales figures could make a corporation ripe for abuse by an online service provider. While the harm a non-natural person faces is qualitatively different from the harm posed to a natural person, this distinction alone is an insufficient basis upon which to rule out extending the benefits of a fiduciary relationship to a non-natural person.[56]

Under Balkin's formulation, "[f]iduciary obligations arise from social relations of unequal power and vulnerability."[57] Since the risk posed to non-natural persons is of the same nature as the risk posed to natural persons and a seller in an online marketplace is in a relation of unequal power and vulnerability vis-à-vis the market operator, it makes sense to extend the duties of the information fiduciary to an online service provider even when the consumer of the service is a non-natural person, like a corporation.

With Balkin's information fiduciary approach gaining some traction through legislation, policymakers will need to grapple with whether and to what extent non-natural persons should be the beneficiaries of information fiduciaries. Part of establishing these boundaries will entail understanding when non-natural persons have alternate avenues for redress for abuses of their data available through

---

[55] *Id.* at § 1100(3).

[56] It is also worth noting that there is no requirement that only a corporation sell on Amazon Marketplace; all that's required to begin selling is a "[b]ank account number and bank routing number, [c]hargeable credit card, [g]overnment issued national ID, [t]ax information, [and p]hone number." *The Beginner's Guide to Selling on Amazon*, AMAZON, https://sell.amazon.com/beginners-guide.html (last visited Feb. 14, 2021). Individuals can sell through the marketplace as well. While proposed legislation that adopts the information fiduciary model would still leave a gap in addressing issue of commercial data that this note addresses, it would seem anomalous to protect some data that would be considered personal because an Amazon seller is a natural person, while declining to extend protection to similar data for corporate persons.

[57] *The Fiduciary Model of Privacy*, *supra* note 27, at 25-26.

other areas of law, such as contract law, antitrust remedies, or unfair competition claims.

Legislators might alternatively choose to construct a more complex statutory scheme outlining obligations, akin to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or the Family Educational Rights and Privacy Act (FERPA). This Note will advance the view that legislatures should pursue a more targeted statutory solution that imposes well-defined responsibilities on the handlers of commercial data rather than imposing simple, yet vaguely defined fiduciary duties.

C. Is Extending the Information Fiduciary Relationship to Commercial Data Consistent with Existing Fiduciary Law?

Balkin proposes that online service providers be subject to fiduciary duties, but he does not suggest that there is a common law basis for imposing them. While the rationale that a social media provider has access to "sensitive data," like a doctor might possess, implies a relationship of trust and confidence, Balkin never outright states that the common law doctrine surrounding fiduciary duties is now applicable to online service providers. These duties would need to be imposed through the legislative process.[58] But, this does not mean that the contours of the duties information fiduciaries owe to their beneficiaries will not develop through common law making.

What exactly constitutes a benefit to an online service provider would need to be fleshed out. Does a marginal increase in, say, algorithmic accuracy constitute a benefit? Or does the benefit need to be more substantial? This, among many other issues, will need to be established so that online service providers can understand which practices violate their duties and which are acceptable. Simply importing existing precedents surrounding fiduciary duties in other contexts through analogies may not make sense in the context of Balkin's information fiduciaries. Congress, state legislatures, and administrative agencies might decide to provide more stability and predictability by providing bright line rules in a robust statutory scheme.

More fundamentally, is Balkin right to say that the relationship between an online service provider and a user is one of such trust and confidence that there must be a fiduciary duty? Different methods of identifying fiduciary relationships point in different directions. Under Paul B. Miller's Fiduciary Powers Theory, online platforms would likely not be considered fiduciaries because they do not receive "discretionary legal powers to be exercised" for the benefit of another merely by

---

[58] *See The Fiduciary Model of Privacy*, *supra* note 27, at 22.

gathering data.[59] The marketplace-merchant relationship is still arm's length in that regard.

Under Gordon Smith's Critical Resource Theory, however, online service providers may be fiduciaries depending on whether personal data is viewed as a "critical resource."[60] Personal data has been referred to as the oil of the twenty-first century, and online service providers are the only economic actors who are able to gather and utilize personal data to generate economic value.[61] Given that the value of data as a resource cannot exist without individuals entrusting it to online service providers, a fiduciary duty might make sense for platforms that generate wealth from data where there was none before.[62]

Ultimately though, these standards do not provide a strong basis for imposing a common law fiduciary duty on an online marketplace operator. While Amazon certainly has greater power and expertise than third-party sellers, many commercial transactions feature imbalances in bargaining power, and that disparity alone is likely insufficient to establish a fiduciary relationship in an otherwise arm's length transaction.[63] A legislatively created information fiduciary duty may sit uneasily with common law fiduciary jurisprudence.

III. ESTABLISHING CONCRETE DATA PROTECTION STANDARDS FOR SENSITIVE COMMERCIAL DATA BY STATUTE OR REGULATION

Although an approach that blankets a commercial relationship with fiduciary duties is not appropriate in the online marketplace context, a more targeted and structured approach to data protection is possible. Congress or another federal agency could impose a fiduciary-like duty on online marketplaces that would require them to safeguard

---

[59] Paul B. Miller, *The Identification of Fiduciary Relationships*, *in* THE OXFORD HANDBOOK OF FIDUCIARY LAW 365, 379 (Evan J. Criddle, Paul B. Miller, & Robert H. Sitkoff eds., 2019).

[60] *Id.*

[61] *See* Shannon Tellis, *Data is the 21st Century's Oil, Says Siemens CEO Joe Kaeser*, THE ECON. TIMES (May 24, 2018), https://economictimes.indiatimes.com/magazines/panache/data-is-the-21st-centurys-oil-says-siemens-ceo-joe-kaeser/articleshow/64298125.cms (last visited Jan 19, 2021).

[62] Evan Criddle has proposed a broader approach to the identification of fiduciary relationships where a duty is owed "when one person is entrusted with legal or factual power over another's legal or practical interests." Miller, *supra* note 59, at 379. Online platforms could be viewed as information fiduciaries if one considers the management of personal data as part of an individual's "practical interests."

[63] Consol. Bearing & Supply Co., Inc. v. First Nat'l. Bank at Lubbock, 720 S.W.2d 647, 650 (Tex. App. 1986) (finding that "(1) a 'kind of trust relationship' between the parties, (2) the disclosing of information about their business not shared with the public, and (3) the sharing of information that may be detrimental to either party" between a bank and its client were insufficient to establish a fiduciary relationship).

third-party sellers' data and only access it for limited purposes. While this approach does not have the elegance or expansiveness of treating online platforms as information fiduciaries, it strikes a better balance between maintaining the coherence of fiduciary law and protecting small online sellers.

A. HIPAA and FERPA: Statutory Protections for Sensitive Data

Congress and federal administrative agencies have some experience in developing statutory and regulatory schemes surrounding the management of sensitive data. Access to, and the use of, sensitive health data is regulated by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health Act (HITECH).[64] HIPAA and HITECH provide standards for data protections to which healthcare providers and insurers must conform. Congress has also taken an even simpler approach in the Family Education Rights and Privacy Act of 1974 (FERPA), which contains simple mandates to educational institutions surrounding access to educational records. Both approaches demonstrate potential avenues Congress could take in establishing a regulatory scheme for how online data providers could use the data they gather.

Broadly speaking, entities covered under HIPAA and HITECH must develop policies and procedures for applying the minimum necessary standards to secure protected health information (PHI). PHI is defined to include any "individually identifiable information, whether it is in electronic, paper or oral form, that is created or received by or on behalf of a covered entity or its health care component."[65] Minimum standards require, "(1) obtaining individual authorization for PHI uses and disclosures not otherwise permitted, issuing a notice of its privacy practices, (2) safeguarding PHI against prohibited uses and disclosures, (3) setting restrictions on legal, public health and related PHI disclosures, (4) establishing provisions regarding individuals' rights to access and change their PHI, (5) developing administrative requirements involving the designation of privacy officials, (6) training and documentation, and (7) notifying individuals of certain privacy or security 'breaches' involving their PHI."[66]

---

[64] While HIPAA is well known, at least among the medical community, HITECH was passed in 2008 to address some of the perceived weaknesses of HIPAA's privacy protections. *Privacy Standards*, *in* EMPLOYER'S GUIDE TO THE HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT ¶ 821 (David Slaughter ed. 2020).

[65] *Id.*

[66] *Id.*

HIPAA and HITECH also allow for the use and disclosure of PHI in certain contexts, so long as the information has been de-identified.[67] Health insurance providers can use de-identified PHI to build data sets for health care operations, research, and public health purposes.[68] Covered entities can share PHI with "business associates," third-party entities that perform health plan functions.[69] Business associates must however also comply with the data protection mandates laid out in HIPAA and HITECH.[70] Both covered entities and business associates are explicitly banned from directly or indirectly selling PHI without receiving the explicit consent of the individual.[71]

Similarly, the Family Education Rights and Privacy Act of 1974 (FERPA), provides a statutory mandate for the data protection practices of educational institutions. Although Congress enacted FERPA in a pre-internet era, many data privacy themes that appear in discourse surrounding digital information appear in FERPA as well.

First and foremost, individuals are given control over their data. Under FERPA the relevant data is educational records. Educational institutions cannot deny students or their parents access to educational records.[72] Educational institutions also must affirmatively receive consent from a student or a student's parents prior to releasing educational records.[73]

---

[67] *Id.* at ¶ 822. HIPAA and HITECH allow for two modes of de-identifying information: (1) the expert method and (2) the safe harbor method. Under the expert method, a professional with scientific or statistical training must attest information is no longer identifiable. The safe harbor method draws a bright line by saying that information is no longer identifiable if geographic information, date elements (like date of birth), telephone number, fax number, email address, Social Security number, medical records number, health plan beneficiary number, account number, certificate/license number, vehicle identifiers, web universal resource locators, Internet protocol address numbers, biometric identifier, and any other unique identifying numbers have been removed. *Id.*

[68] *Id.*

[69] *Id.* at ¶ 823. "Business associates fall into two major categories: (1) [p]eople or entities that perform a function or activity on the covered entity's behalf involving PHI use or disclosure, such as third-party administrators; and (2) [t]hose that need PHI to perform specified services for the covered entity (such as attorneys and accountants)." *Id.*

[70] *Id.*

[71] *Id.* at ¶ 822. There are a number of exempt circumstances, however, and PHI may be sold when it is "made for public health activities, research purposes, to treat the individual, related to the sale, transfer, merger or consolidation of a covered entity, to pay a business associate for activities it undertakes on behalf of the covered entity under its business associate contract, made to provide an individual with a copy of his or her own PHI under the HIPAA privacy rules' right of access, and as otherwise determined by HHS in regulations to be similarly necessary and appropriate." *Id.*

[72] 20 U.S.C. § 1232g(a).

[73] *See id.* § 1232g(b)(1)(A)-(B). There is a list of exceptions where educational institutions can release information from student records without consent, but these

The commercial data protection approach, however, would represent an entirely different paradigm from FERPA though, because the enforcement mechanism in FERPA is the denial of federal funding to educational institutions that fail to comply with privacy protections. Given that online platforms receive no federal subsidies, there is little rationale for importing a FERPA-like approach into the digital realm, beyond some of its basic principles. For a statutory regime to have any bite, there needs to be a cause of action available to those who are harmed by online service providers' data practices.

The statutory approach is complex, requires additional action by administrative agencies, and could require additional congressional action even once the statutory scheme is in place. However, while HIPAA and HITECH impose a significant bureaucratic burden on healthcare providers and insurers, the obligations imposed upon them in terms of data privacy are concrete. Covered entities can take steps to ensure their compliance a priori. This brings the benefit, lacking in Balkin's information fiduciary approach discussed above, of predictability and stability.

Congress should propose federal legislation in the same mold as HIPAA and FERPA to address potential abuses of commercial data, such as those alleged against Amazon. Like existing data protection legislation, proposed legislation should (i) define what type of online platforms are covered and owe a duty to protect data, (ii) identify to whom that duty is owed, (iii) detail what kind of information is protected, and (iv) prescribe the contours of a fiduciary-like duty owed to e-commerce sellers. It should also give sellers a private cause of action for violations of these duties.

Legislation should apply to any website or digital platform where third parties sell goods or services to the public. Operators of such marketplaces should extend data protection to any merchant who sells goods or services on the platform. The operators should be obligated to protect sensitive commercial data. I will discuss the contours of the duty owed in the next section.

B. *Looking to Securities Regulations to Establish the Contours of a Fiduciary-like Standard in Protecting Commercial Data*

Legislators should draw from federal securities regulation to provide some more concrete content to the scope of the duties owed to sellers on online marketplaces, rather than the broad mandates of the fiduciary duties that Balkin proposes. However, these duties should still

---

exceptions largely have a nexus with furthering a student's education, such as other educators or school officials outside the student's educational institution.

be informed by the fiduciary duties of loyalty, confidentiality, and care that Balkin's information fiduciary proposal echoes. Drawing upon securities law provides a workable basis for these duties because the securities industry features relationships that range from purely commercial to one governed by fiduciary obligations. Federal securities law strikes a balance between broadly mandating duties that financial professionals and institutions owe to their clients with bright-line rules.

The most obvious analogies between online marketplaces and the securities industry are broker-dealers and securities exchanges. Broker-dealers and securities exchanges are regulated by a number of statutes, most notably the Securities and Exchange Act of 1934 (SEA). This statute provides for the creation of the Securities and Exchange Commission (SEC) and grants the SEC the power to establish regulations to carry out the aims of the SEA.[74] Broker-dealers and other exchange participants are also regulated by industry regulators, like FINRA (formerly NASD), whose missions run parallel to the SEC's.[75]

While not a perfect analogy, the securities market features several dynamics reminiscent of the issues that sellers face on Amazon Marketplace. Investors face an asymmetry of information because their broker-dealers have a much more complete, although not perfect, view of the securities market through greater expertise and superior technology.[76] Front-running and trading ahead are practices in which a broker receives a client order and then takes a position or makes a transaction that will profit the broker based on that knowledge, usually to the client's detriment.[77] As on Amazon Marketplace, the broker takes advantage of his or her superior knowledge of the security market to, for example, sell a security at a higher price before its client's order to sell the same security drives the price down. This is roughly analogous to Amazon's ability to "adopt" successful products.

---

[74] 15 U.S.C. § 78d, 78w.

[75] A broker-dealer is "a person or firm in the business of buying and selling securities for its own account or on behalf of its customers" and consequently acts as either an agent or a principal. Adam Hayes, *Broker-Dealer*, INVESTOPEDIA https://www.investopedia.com/terms/b/broker-dealer.asp#:~:text=A%20broker%2Ddealer%20(B%2DD),as%20both%20agents%20and%20principals (last accessed Dec. 5, 2020, 11:03 AM).

[76] This asymmetry is tempered by obligations like FINRA Rule 5310 to use "reasonable diligence to ascertain the best market for the subject security and buy or sell in such market so that the resultant price to the customer is as favorable as possible under prevailing market conditions."

[77] Front-running and trading ahead are technically different practices, but both are abuses of brokers' superior knowledge of the market that stems from the trust placed in them by clients. *Trading Ahead*, NASDAQ, https://www.nasdaq.com/glossary/t/trading-ahead (last visited Feb. 14, 2021); *Front running*, NASDAQ, https://www.nasdaq.com/glossary/f/front-running (last visited Feb. 14, 2021). Front-running is prohibited by FINRA Rule 5270. Trading ahead is prohibited by FINRA Rule 5320.

There is also a degree of competition between clients and broker-dealers who operate as market-makers. Market-makers in the securities context are individuals or member firms of an exchange that buy and sell securities for their own accounts and profit on the bid-ask spread.[78] Both broker-dealers and market-makers operate in a marketplace that is sometimes two-sided and both types of actors will either facilitate transactions between buyers and sellers or will sometimes take the opposite side of a transaction in order to facilitate liquidity in the marketplace.[79] Amazon's behavior is at least broadly similar in that it links buyers and sellers in Amazon Marketplace but also acts as a seller (although not a buyer).

Under securities law, market making does not, by itself, generate a fiduciary duty toward market participants, but certain business practices that market-makers engage in might be analyzed under a fiduciary duty structure.[80] Amazon could be analogized to a broker-dealer or market-maker, and thus similar principles that drive the regulation of broker-dealers' trading practices and treatment of their clients could be applied to digital marketplaces.

In lieu of imposing a duty of loyalty generally, Congress could impose a tailored duty on online marketplaces that would require those marketplaces to use sensitive commercial data only in the merchant's best interest or for other expressly authorized purposes. The SEC has recently imposed a similar standard on broker-dealers, Regulation Best Interest, in the context of recommending security purchases to retail customers.[81] Online platforms might be able to access such data without

---

[78] Andrew Bloomenthal, *Market Makers*, INVESTOPEDIA https://www.investopedia.com/terms/m/marketmaker.asp#:~:text=A%20market%20maker%20is%20a,exceeds%20the%20bid%20price%20a (last accessed Dec. 5, 2020, 10:47 AM).

[79] Dolgopolov, *supra* note 45, at 32.

[80] *Id.* at 63-64.

[81] Regulation Best Interest: The Broker-Dealer Standard of Conduct, 84 Fed. Reg. 33,318, 33,319 (July 12, 2019) (to be codified at 17. C.F.R. pt. 240) ("[r]egulation Best Interest enhances the broker-dealer standard of conduct beyond existing suitability obligations, and aligns the standard of conduct with retail customers' reasonable expectations by requiring broker-dealers, among other things, to: [a]ct in the best interest of the retail customer at the time the recommendation is made, without placing the financial or other interest of the broker-dealer ahead of the interests of the retail customer; and address conflicts of interest by establishing, maintaining, and enforcing policies and procedures reasonably designed to identify and fully and fairly disclose material facts about conflicts of interest, and in instances where we have determined that disclosure is insufficient to reasonably address the conflict, to mitigate or, in certain instances, eliminate the conflict."). Previously, broker-dealers had no fiduciary obligation when making recommendations beyond assessing whether a security was "suitable" for a particular investor. See FINRA Rule 2111. Brokers could advise clients to purchase securities that secured higher commissions for themselves, so long they had reason to believe an investment (1) was suitable for any investor, (2) was suitable for a particular customer based on their unique investment

authorization in situations where they are providing support related to a client request but would otherwise not have access to do so. If the online marketplace in question also sells goods, it should have to affirmatively receive authorization before accessing a merchant's data.[82]

Congress could also give some content to the duty of care by imposing a requirement that online marketplaces put in place a system to control internal access to merchant data. The SEC requires brokers to follow Regulation S-P, a measure which aims to restrict the disclosure of nonpublic personal information of financial institutions' clients to third parties.[83] As an additional protection, employees should have to document why they are accessing protected commercial data to provide an audit trail should questions arise later.[84]

While these suggestions are overall modest, they do provide a degree of protection to those merchants who hand over sensitive commercial data to online marketplaces. These duties are not as broad as the fiduciary duties that Balkin proposes. However, their benefit is that they provide some guidance to companies that would allow them to comply more easily than with broad and vaguely defined fiduciary duties. Additionally, merchants would benefit from a more straightforward understanding of their rights vis-à-vis online marketplaces. In the event that there was a breach of a statutory duty, an audit trail of data access would enable plaintiff-merchants to pinpoint the inappropriate use of their data.

C. Limitations of a Statutory Approach to Protecting Commercial Data

A statutory approach to commercial data protection is not a panacea to all the ills of the digital economy. Any approach to regulation that develops prospective duties runs the risk that digital platforms will lobby to water down protections. Additionally, a commercial data protection bill would be one more of a constellation of data protection

---

profile, and (3) was not unreasonable in light of broader trading activity the broker conducts on the client's behalf. FINRA, *Suitability*, https://www.finra.org/rules-guidance/key-topics/suitability (last visited Feb 13, 2021).

[82] In her 2020 presidential campaign, Elizabeth Warren argued that companies should not be able to both run and participate in an online marketplace. Matt Stevens, *Elizabeth Warren on Breaking Up Big Tech*, N.Y. TIMES (June 26, 2019), https://www.nytimes.com/2019/06/26/us/politics/elizabeth-warren-break-up-amazon-facebook.html. Such a bright line rule stands as an alternative to a requirement to divulge this information as a conflict of interest.

[83] 17 C.F.R. § 248.1 (2020).

[84] This suggestion comes from HIPAA's audit trail mandate, 45 C.F.R. § 164.312(b) (2020) (requiring covered entities to "[i]mplement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information").

schemes with which small businesses may struggle to conform. It would also constitute a barrier to entry for new competitors.[85]

As Balkin has argued with his information fiduciary model, the commercial data protection approach needs to be complemented by additional reforms.[86] First and foremost, more robust antitrust enforcement is needed in digital spaces. Data protection schemes on their own will not reduce economic concentration online, nor will they create more competition.[87] Greater competition, especially in e-commerce, is a necessary, but not sufficient, condition for fairer online marketplaces. Unless small-scale merchants can vote with their feet and operate on different e-commerce platforms, they may be vulnerable to anticompetitive behavior unrelated to their commercial data.

Commercial data protections will obviously not resolve issues surrounding abuses of personal data. Personal data is qualitatively different in nature from commercial data and the stakes for abuse are much higher.[88] While this note has embraced a modified application of Balkin's information fiduciary concept in the e-commerce setting, it has taken no position on the appropriateness of applying broad fiduciary duties toward personal data. Likewise, my definition of commercial data would exclude data gathered from consumers on e-commerce platforms. Additional protections, like the information fiduciary obligation, would likely be necessary to protect such consumers' personal data from misuse.

While this approach will not dramatically change e-commerce overnight, it will provide a workable solution to rebuild trust in e-commerce platforms. Small-scale sellers face a highly competitive environment online and the abuse of their data by the platforms on which they sell could gradually erode the incentives to sell online at all. A prospective approach with bright-line rules surrounding e-commerce platforms' use of third-party sellers' data also increases the likelihood of compliance since platforms will know whether their current data practices comply with new standards. By knowing the scope of their

---

[85] For a critical view of such an approach in the context of personal privacy, see Lindsey Barrett, *Confiding in Con Men: U.S. Privacy Law, the GDPR and Information Fiduciaries*, 42 SEATTLE U. L. REV. 1057, 1068-1071 (2018). Barrett's view is skeptical of a sectoral approach to privacy regulation because it fails to conceptualize individual privacy as an all-encompassing right, and instead simply fences off small areas where individuals are free from invasions of privacy from private actors.

[86] *The Fiduciary Model of Privacy*, *supra* note 27, at 20-22.

[87] Kahn & Pozen, *supra* note 41, at 526-28.

[88] *See* Jonathan Zittrain, *Facebook Could Decide an Election Without Anyone Ever Finding Out*, THE NEW REPUBLIC, https://newrepublic.com/article/117878/information-fiduciary-solution-facebook-digital-gerrymandering (June 1, 2014) (arguing that Facebook could use the personal data it gathers from users to influence the outcome of an election).

duties, platforms may be less likely to push the boundaries of broad yet vague fiduciary duties through litigation.

CONCLUSION

Digital marketplaces connect buyers and sellers in ways that overcome geography and language, and tie together disparate markets. They facilitate commerce in ways that could only have been dreamt of in a pre-internet age. But as digital marketplaces have matured, they have developed a number of issues that society writ large needs to address. Amazon's commanding and enduring grip on e-commerce is a major one. Despite the abuse of their data, third-party sellers on Amazon Marketplace have virtually no viable alternatives but to continue operating on Amazon because of a lack of competition.

While antitrust structural remedies would be the most obvious legal remedy, existing doctrine provides a considerable hurdle. The Supreme Court's ruling in *Ohio v. American Express*[89] requires that plaintiffs show harm on both sides of a two-sided market to establish an antitrust violation. Because Amazon's retail business provides cheap and plentiful goods to consumers, any plaintiff seeking to challenge Amazon's dominance of e-commerce in the United States would face an uphill battle. Congress would likely need to act before Amazon would ever be subject to structural antitrust remedies as the law currently stands.

But structural remedies may only be the beginning of what is necessary to protect trust in digital marketplaces. Amazon is hardly alone in abusing its sellers' data. Other monopolistic platforms have also misused sensitive user data. Because information is the "oil of the digital era," online platforms often have powerful financial incentives to monetize the information they collect.[90] Moreover, structural remedies need to be carefully crafted, because, as Amazon shows, different business units may prop each other up and decoupling them may make the less profitable unit non-viable after a bust-up. A theoretical post-Amazon internet with multiple viable online e-commerce platforms might simply see a proliferation of abusers. Additionally, platform effects might incentivize online sellers to stick with the devil they know because they have already established customer bases and reputations on Amazon.

Jack Balkin's information fiduciaries provides a potential avenue to a more trustworthy e-commerce landscape for sellers. Were online platforms required to treat sensitive business data with care, sellers could avoid future abuses either by Amazon or other e-commerce platforms

---

[89] 138 S. Ct. 2274 (2018).
[90] Tellis, *supra* note 61.

that seek to profit in some way from data abuse. While Balkin's information fiduciary concept has been most discussed in the context of platforms protecting the personal information of natural persons, it would be natural to extend that duty to a purely commercial context because professionals such as lawyers already owe fiduciary duties to corporate persons.

The information fiduciary concept has already gained traction in both state and federal legislation. But as some commentators have pointed out, the information fiduciary concept may sit uneasily with existing fiduciary obligations. Although its application in the context of online marketplaces would lead to greater data protections, the information fiduciary idea was not built for commercial relationships and extending it to an otherwise arm's length transaction would mangle both fiduciary law and Balkin's information fiduciary proposal.

However, the concept of safeguarding sensitive information is neither foreign to nor incompatible with American law. A constellation of situationally specific statutes dictate how sensitive data can be protected, most notably including HIPAA and FERPA. A statutory scheme similar to these, rather than a statute that unartfully subjects online platforms to broad yet vaguely defined fiduciary duties, could protect sensitive data while giving platforms the opportunity to proactively change their business models.

A data protection scheme modeled off of HIPPA and FERPA could take concrete concepts from securities law to define an online marketplace's duties toward its sellers. This approach would allow online platforms to operate in a predictable manner, but without the potential for abuses of data. The injection of widely accepted privacy practices and regulatory duties drawn from another commercial context would instill a sense of trust back into online marketplaces.

Trust is the critical ingredient to any viable marketplace. Without it, buyers and sellers refuse to enter into transactions and commerce ceases. Digital marketplaces are of course no different. But they do pose a number of novel issues, especially monopolization, competition within the marketplace from the marketplace's operator, and the potential for the abuse of data. Restoring trust into online marketplaces is imperative to securing the benefits e-commerce has long promised.