PUBLIC KNOWLEDGE

MIND YOUR OWN BUSINESS:

Protecting Proprietary Third-Party Information From Digital Platforms

2020 | JUNE

HAROLD FELD

ACKNOWLEDGEMENTS

The author would like to thank those who provided feedback during the drafting of this paper, including Tom Wheeler, Visiting Fellow, Governance Studies, Center for Technology Innovation, Brookings Institution and Philip Verveer, Fellow, Shorenstein Center, Harvard Kennedy School. Thank you to Sadev Parikh, student at the Georgetown University Law Center and intern at Public Knowledge, for editing assistance. This paper, along with other work from Public Knowledge on platform competition, was made possible by the support of the Omidyar Network.

Table of Contents

EXECUTIVE SUMMARY

In *The Case for the Digital Platform Act*,[1] I have previously written why digital platforms are a unique sector of the economy that requires sector specific regulation. I have also explained why the experience in regulating the telecommunications sector can provide useful insight into what problems and solutions we must address to regulate digital platforms to promote competition and the public interest. In this paper, I expand on one remedy discussed briefly in *Digital Platform Act* designed to address a very specific problem: Customer Proprietary Network Information (CPNI).

Basic Problem Addressed and Proposed Remedy

For vendors to reach buyers through digital platforms such as Amazon or Etsy, vendors must expose proprietary information to the platform on an ongoing basis. This may include not merely information such as sales data collected through sales on the platform, but additional information such as quality assurance information and supply chain information that the platform insists is integral to ensuring a quality customer experience. The platform can then use this information to unfairly advantage itself in the market by producing rival products. Platforms may also favor products that use affiliated services or otherwise maximize revenue to the platform, while pretending to consumers that the recommendations are based on other factors such as price savings or superior quality.

For the reasons discussed in Part I, it is unreasonable to assume that the market will produce a solution without regulatory intervention. One can argue that new limitations should only be imposed on dominant firms. In support of this, one could point out that the Federal Communications Commission created the telecom CPNI regulations as a means of opening

[1] HAROLD FELD, PUBLIC KNOWLEDGE & ROOSEVELT INSTITUTE, THE CASE FOR THE DIGITAL PLATFORM ACT: BREAK UPS, STARFISH PROBLEMS AND TECH REGULATION (2019) (*Digital Platform Act*).

markets dominated by a regulated monopolist.[2] However, I argue below for broader application based on the nature of the digital platform sector. The ability of digital platforms of any kind to control the flow of information between parties on the platform, "perfect information asymmetry," combined with other factors such as customer lock-in, make it highly likely that even non-dominant firms will seek to unfairly advantage themselves by using proprietary data disclosed by third-party vendors.

CPNI limits the ability of platforms to engage in such behavior by limiting the way in which platforms can use the information they collect. Networks can be structured to create walls between business units and to avoid providing information in ways that are easily exploitable. The success of the telecom CPNI regime in enhancing competition strongly indicates that, with suitable adjustment, a regime based on similar principles of restricting the use of proprietary information by digital platforms can provide immediate improvement in the competitive environment without requiring broader structural changes or the creation of a new regulator. It therefore suggests itself as a good first step for legislation to address a real issue threatening competition and undermining confidence in online commerce.

Important Limitations of Approach, No First Amendment Barrier

While the remedy discussed is inspired by the success of the telecom CPNI regime, it is important to remember one of the fundamental cautions stressed in *The Digital Platform Act.* While a century of experience regulating electronic communications networks provides valuable lessons for how to approach the regulation of "virtual networks" such as digital platforms, we cannot simply copy previous solutions and mechanically apply them. While the similarities are important, so are the differences.

Readers should therefore think of the relationship between the "platform CPNI" proposed here and traditional "telecom CPNI" as similar to the relationship between *West Side Story* and *Romeo and Juliet*. While one is clearly an adaptation of the other, no one would mistake the

[2] *See* HAROLD FELD ET AL., PROTECTING PRIVACY, PROMOTING COMPETITION: A FRAMEWORK FOR UPDATING THE FEDERAL COMMUNICATIONS COMMISSION PRIVACY RULES FOR THE DIGITAL WORLD 9-11 (Feb. 2016), https://www.publicknowledge.org/assets/uploads/blog/article-cpni-whitepaper.pdf.

Broadway musical for the Elizabethan drama – or argue that *West Side Story* fails because it discards various characters and subplots in favor of modern dance numbers and because Maria lives. Similarly, one should not judge the proposed platform CPNI by how closely it resembles telecom CPNI. I do not intend that the proposed draft legislation should be an amendment to the existing Section 222 of the Communications Act.[3] Nor do I propose that the FCC enforce platform CPNI. I intend platform CPNI to fit the unique facts of this economic sector, and have therefore diverged considerably from the text of existing Section 222, while still using Section 222 as the basic blueprint for this proposal.

Similarly, although Section 222 is designed to protect consumer privacy as well as promote competition, I have not attempted to incorporate any consumer privacy protections in this proposed platform CPNI legislation. This proposal limits itself strictly to the purpose of promoting competition, similar to the FCC's original purpose for creating the telecom CPNI in the 1980s. I have accordingly created exceptions to the proposed platform CPNI legislation to permit platforms to continue to collect information for targeted advertising and to otherwise minimize impact on existing business models beyond addressing the problem of protecting third-party proprietary information. Public Knowledge separately continues to advocate for comprehensive privacy regulation which would alter existing business models and impose substantial new obligations on companies to protect consumer privacy, and the platform CPNI proposal is compatible with this advocacy.

Finally, it is important to understand that CPNI is a targeted solution to a fairly narrow (albeit important) problem – digital platforms unfairly advantaging themselves based on access to third-party proprietary information. This does not on its own prohibit self-preferencing or other anti-competitive conduct. As discussed in *Digital Platform Act*, platform CPNI should ideally be combined with other pro-competitive regulations. Recent news coverage suggests that the problem of access to proprietary information is increasingly urgent for competition in ecommerce,[4] and the proposed statute can be easily implemented on its own as a first step while Congress debates broader reforms.

---

[3] 47 U.S.C. § 222 (2018).

[4] *See, e.g.*, Dana Mattioli, *Amazon Scooped Up Data From Its Own Sellers to Launch Competing Products*, WALL ST. J., https://www.wsj.com/articles/amazon-scooped-up-data-from-its-own-sellers-to-launch-competing-products-11587650015 (last updated Apr. 23, 2020, 9:51 PM).

Restrictions on collection and use of information are frequently challenged on First Amendment grounds. While this paper does not attempt a lengthy analysis, I explore the issue sufficiently to satisfy objections that the proposed platform CPNI statute would violate the First Amendment. Because the statute promotes competition and does not in any way involve expressive conduct, there is no reason to suppose that it would raise any First Amendment issues.[5] Even if a court were to find that platform CPNI implicates First Amendment interests, this proposal would fall within the realm of permissible commercial speech regulation.

Structure of the Proposed Platform CPNI

The proposed platform CPNI regime is structured as follows.

1. *General duty of digital platforms to protect customer CPNI.* The first provision imposes a general duty on all digital platforms to protect the proprietary information of both vendors (those selling goods or services through the platform) and buyers (consumers who use the platform to reach vendors). The terms "digital platform," "customer," "buyer," "vendor," and "proprietary information" are all defined in the paper and in the proposed statute.

2. *Specific duty of platforms to protect vendor information*. The purpose of platform CPNI is to protect competition between third-party vendors and the platform in adjacent markets. This provision limits a platform to using proprietary information disclosed to it solely for the purpose disclosed, subject to certain exceptions enumerated below. Information may not be shared among the platform's affiliates, or by the affiliates with the platform. For example, whether or not a vendor uses the platform's affiliated delivery service is not information that the platform or its affiliates can use for other purposes, such as elevating or downgrading the product in the "buy window."

   The duty to protect vendor information is not waivable. If parties could agree to waive the protection, platforms with market power would simply require all vendors to do so, effectively eliminating the protection. In keeping with the principle that the information remains proprietary to the vendor, and only exposes the information to use the platform, the vendor retains control of the information (again, subject to appropriate exceptions for things such as billing and to protect the legal rights of the platform).

3. *Far more limited duty to protect buyer information.* As a general rule, the platform has a relationship with the buyer independent of the specific transaction with the specific vendor. Buyers understand that their information is collected for a wide number of purposes beyond facilitating a specific transaction, and may engage with the platform for

[5] *See, e.g.*, Barnes v. Glen Theatre, 501 U.S. 560, 576-77 (1991) (Scalia, J. concurring) (conduct must actually intend to express a message, in a form reasonably expected to be understood by the intended audience).

many purposes that have nothing whatsoever to do with transactions with third-party vendors. This lesser restriction is also in keeping with the principle that the collection of information and use of the information should be governed by the general expectation of the relationship, and that it is the unique nature of the technology (and any additional market power) that makes use of the information unfair. Furthermore, although platforms can use the search and recommendation features to self-preference unfairly, functioning search and recommendation algorithms that accurately assess individual preferences enhance the overall consumer experience and are an important part of competition between platforms.

Accordingly, platform CPNI merely proposes to limit the ability of the platform to use information provided by a buyer to directly compete with the vendor. A platform cannot use the information that a buyer bought a particular pair of shoes from a specific vendor, for example, to target that customer with its own rival pair of shows. Nor could it use the information to reverse engineer vendor CPNI by aggregating individual buyer CPNI. But the information could be included in the platform's search algorithm, even if that caused the platform's own shoes to rise to the top organically as a recommendation.

4. *Exceptions*. Like telecom CPNI, platform CPNI is tailored to prevent unfair competition and unjust enrichment. It should not interfere with the smooth functioning of the platform in the normal course of business, or prevent the platform from protecting users (or the platform itself) from fraud or abuse. The proposed statute therefore contains several explicit exceptions to protect the rights of the platform, the rights of other users of the platform, and to permit the platform to cooperate with authorities where appropriate. Additionally, the statute maintains what has become the traditional exception in information privacy law for aggregate data use, but with an explicit prohibition on any effort to re-identify the data, or to permit third parties to re-identify the information.

The paper concludes with a brief discussion of enforcement. Because this proposal is intended merely to flesh out the discussion in *The Digital Platform Act*, I refer the reader to the broader discussion on enforcement there. Suffice it to say the same enforcement possibilities exist here: a private right of action, enforcement by existing federal or state agencies, creation of a new federal regulator, or some combination of these approaches.

A draft statute is attached as an appendix to this paper.

INTRODUCTION

Over the last two years, multiple authorities have focused on "digital platforms"[6] as a distinct sector of the economy.[7] This paper continues the work begun in *The Case for the Digital Platform Act* which proposed creation of a general sector specific regulator for digital platforms, with a general mission to affirmatively promote competition and protect consumers. Here, I explore one specific idea recommended for promoting competition, creation of rules protecting proprietary information exposed by buyers and vendors[8] using the platform. I refer to this general proposal as Customer Proprietary Network Information rules, or CPNI, after the telecommunications rules on which I base the proposal.

While the bulk of discussion around privacy has generally focused on protecting personal privacy, this paper focuses on restricting the use of information collected by the digital platform from buyers or vendors using the platform to further the interests of competition. Although digital platforms are relatively new, they are not the first example in commerce of two-sided markets where parties must expose to the platform information that they would otherwise consider highly confidential for either personal or commercial reasons. In particular, in the

---

[6] The definition of "digital platform" is a matter of some debate. I use the definition I proposed in *The Case for the Digital Platform Act: Break Ups, Starfish Problems and Tech Regulation*: a service accessed via the Internet, constituting a 2-sided or multi-sided market with at least one side of the platform open to the public, in which participants are able to self-organize content and services and participate in multiple ways on the platform simultaneously. *See* FELD, *supra* note 1.

[7] *See, e.g.*, Matt Stoller et al., *Addressing Facebook and Google's Harms Through a Regulated Competition Approach* (Am. Econ. Liberties Project, Working Paper Series On Corporate Power No. 2, Apr. 2020), https://www.economicliberties.us/wp-content/uploads/2020/04/Working-Paper-Series-on-Corporate-Power_2.pdf; STIGLER COMM. ON DIGITAL PLATFORMS, FINAL REPORT (Sept. 2019), https://research.chicagobooth.edu/-/media/research/stigler/pdfs/digital-platforms---committee-report---stigler-center.pdf; Jacques Crémer et al., *Commission Report on Competition Policy for the digital era* (2019), https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf.

[8] As one of the elements of a digital platform is that users may simultaneously take on multiple roles, designating a party as a "buyer" and another party as a "vendor" applies on a transaction-specific basis. Nevertheless, it is generally helpful to think of buyers as generally being more like typical consumers in terms of behavior and market power, and vendors as traditional enterprise retailers or service providers of various size. It is important to remember, however, that there are many Business-2-Business (B2B) platforms where the same concerns apply, as well as platforms that facilitate transactions between members of the public where neither party is a traditional enterprise customer.

matter of communications, the need for parties communicating with one another to have assurance of confidentiality of not merely the details of the communication, but the fact of the communication itself, is well established.[9] But the duty to neither disclose nor use information provided where the relationship requires disclosure of sensitive information applies in multiple fields such as financial services, medical services and legal services.[10]

These privacy restrictions flowed from a combination of motivations. First, as a matter of inherent fairness, common law courts (and later legislatures) recognized that users of these services had no choice but to expose confidential information for the service to work. A patient must disclose symptoms and details about their behavior to a doctor for the doctor to make a diagnosis, and the diagnosis itself will be extremely personal, sensitive information. A merchant must disclose the details of money transfers to a banker. An investor must disclose the details of a financial trade to a broker. The law also recognizes that normal market mechanisms do not produce the desired result, regardless of the level of competition. The temptations to a banker or investor or even a doctor or lawyer to abuse the information are many and varied. Even without temptation, the lack of any affirmative obligation to protect the information means that information a third-party has no choice but to disclose may be revealed carelessly. Common law traditionally viewed the prohibition on using the information in question as a form of implied contract, or an application of the fiduciary duty of care or fiduciary duty of loyalty. Additionally, common law and legislatures have viewed restriction on the use of information in these circumstances as an equitable protection against unjust enrichment. Allowing parties to profit from this confidential information entrusted to them for other purposes gives an unfair advantage in business and provides additional rewards beyond the fee for the services rendered. Finally, legislatures have created such restriction where a failure to protect the confidentiality of the information potentially undermines confidence in the market. This is why, for example, the Securities and Exchange Commission (SEC) has interpreted the Securities and Exchange Act to prohibit various kinds of "insider trading." Allowing insiders to take advantage of their superior

---

[9] *See* Adam Candeub, *The Common Carrier Privacy Model*, 51 U.C. DAVIS L. REV. 805, 816-20 (2018).

[10] *Id.*; *see* Jack Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183 (2016).

access to information to manipulate markets risks discouraging investment, and is often seen as a sort of unfair fraud.[11]

During the 1980s, as the FCC sought to introduce competition into markets adjacent to "basic" telecommunications, such as alarm services and data processing, the FCC discovered that it needed to expand the traditional common law and statutory protections for proprietary information.[12] As explained in greater detail below, the FCC determined that it needed to require protection of information revealed to the telephone network by both the subscriber or the service provider. In addition, to facilitate competition, it was sometimes necessary for customer to direct the telephone network operator to disclose information to the provider of the rival service. For example, the FCC required the telephone network to provide information about the customer's telephone connection at a technical level unknown to the customer so that the alarm company could provide the necessary service. Even where the customer could arguably disclose the information, the FCC still gave the customer the right to direct the phone network to provide the necessary information to the rival service provider. Additionally, carriers were forbidden from using any information collected to provide these "enhanced services" – whether collected from the customer or collected from the rival provider – for any other purpose than to provide the contracted service.

Congress ultimately adopted these regulations as Section 222 of the Communications Act.[13] Section 222 imposes a general obligation to protect "Customer Proprietary Network Information" (CPNI), followed by a set of specific restrictions on the use of information collected. These regulations proved enormously successful in promoting competition in telecommunications services market. Indeed, although generally resisted by carriers

---

[11] *See* Peter A. Winn, *Confidentiality in Cyberspace: The HIPAA Privacy Rules and the Common Law*, 33 RUTGERS L.J. 617 (2002); *see also* Daniel J. Solove, *A Brief History of Information Privacy Law*, *in* PROSKAUER ON PRIVACY § 3.1 (PLI, 2006), https://scholarship.law.gwu.edu/faculty_publications/923/; *see generally* FELD ET AL., *supra* note 2 (discussing relationship between consumer protection and competition aspects of telecom CPNI.)

[12] FELD ET AL., *supra* note 2 at 10-11.

[13] 47 U.S.C. §222 (2018).

domestically, these same rules are supported for inclusion in the telecommunications chapter of recent international trade agreements because of their effectiveness in promoting competition.[14]

This paper proposes adapting the highly successful CPNI model to digital platforms. To be clear, the key word is "adapting." This paper proceeds from the same general principles described above that have animated such laws previously: (a) focus on limiting the ***use*** of information collected rather than trying to limit the type of information collected, by recognizing the implied contract that the party disclosing the information only discloses to receive a specific service; (b) prevent unjust enrichment; and, (c) promote commerce overall by enhancing the willingness of parties to use the new technologies and services. Because digital platforms are virtual networks similar to the physical networks of traditional electronic communications technologies, the same general principles apply. But because digital platforms are virtual networks rather than physical networks, the application and expression of these principles as a matter of law will require significant adjustment.

Part I describes the current situation with regard to digital platforms and the allegation of existing harms. Part II describes in greater detail the evolution of CPNI and the underlying theory as applied in the telecommunications sector.[15] Part III considers how to implement a CPNI-like scheme in the context of digital platforms, and considers whether CPNI should apply to all platforms or only dominant platforms. In keeping with the principles, this paper does not seek to address the consumer privacy protections of the existing telecom CPNI statute.

---

[14] *See, e.g.*, Australian Free Trade Agreement, Aus.-U.S., May 18, 2004, Art. 12.8(b), https://ustr.gov/sites/default/files/australian_FTA_telecom.pdf; Korean Free Trade Agreement, S. Korea-U.S., June 30, 2007, Arts. 14.3, 14.5(b), https://ustr.gov/sites/default/files/uploads/agreements/fta/korus/asset_upload_file985_12713.pdf; Peru Trade Promotion Agreement, Peru-U.S., Apr. 12, 2006, Arts. 14.3(b), 14.4(2)(b), https://ustr.gov/sites/default/files/uploads/agreements/fta/peru/asset_upload_file942_9515.pdf.

[15] I have written extensively in *Digital Platform Act* about the particular relevance of the history of telecommunications regulation to the regulation of digital platforms, including the applicability of CPNI. *See* FELD, *supra* note 1, at 28-47.

PART I:

THE PROBLEM: DIGITAL PLATFORMS HAVE THE CAPACITY TO ABUSE PROPRIETARY INFORMATION THAT THIRD PARTIES MUST DISCLOSE FOR THE PLATFORM TO WORK

In the first chapter of *The Digital Platform Act*, I provided my working definition for "digital platform": a service accessed via the internet, constituting a two-sided or multi-sided market with at least one side of the platform open to the public, in which participants are able to self-organize content and services and participate in multiple ways on the platform simultaneously. As explained there, this definition captures the unique features that make digital platforms a distinct sector of the economy.

The next step in regulating digital platforms requires translating this definition from descriptive language to legislative language. For purposes of drafting a law protecting digital platform CPNI, I define a "digital platform" as follows:

> DIGITAL PLATFORM. —The term 'digital platform' means a service that—
> (i) is accessed via the internet;
> (ii) provides a two-sided or multi-sided market where at least one side is open to the general public and allows the public to produce and interact with content; and
> (iii) permits users to:
> (1) simultaneously engage in multiple activities on the platform;
> (2) interact directly, or in a generally unmoderated manner, with other users of the platform;
> (3) allows users to self-organize into open or closed groups where users have freedom to share information, goods or services with each other.

As explained in greater detail in *The Case for the Digital Platform Act*, these factors create particularly powerful network effects. These network effects go beyond the purely linear network effect of increasing the value of the network arithmetically for every new member (a network type sometimes called a "Sarnoff network"). The ability of users to perform multiple roles and interact with each other increases the value by the number of potential new uses and groupings, essentially allowing the network effect to increase geometrically or even

logarithmically.[16] This creates an environment with "tipping effects," where capture of a sufficient share of the market makes it effectively impossible for a new entrant to contest the market. Silicon Valley venture capitalists call this strategy "blitz scaling."[17]

As a result, in several important segments of the economy, a handful of digital platforms have become dominant. One critical element of control for dominant digital platforms is control over all information provided by every participant on the platform, and the extent to which this information is revealed to platform participants. This creates a situation of perfect information asymmetry. The platform knows all, but the participant can only know what the platform choses to share. As platforms become increasingly important in economic transactions ranging from advertising to retail, it becomes increasingly impossible to avoid dealing with digital platforms and exposing proprietary information. This opens the door to a wide range of potential misuses, ranging from stealing customers from rivals in a related market, using the information to otherwise maximize revenue (such as shifting business to parties that use complimentary services over those that do not), to disintermediating the vendor and the buyer to prevent the vendor from circumventing the platform. Finally, given the importance of information in digital markets generally, simply forcing parties to expose information they would otherwise not wish to expose (or forcing them to go through the platform rather than communicating directly) can convey unfair advantages on a digital platform.

For example, Amazon has been the target of multiple allegations that it uses information collected from third-party sellers to develop its own competing products.[18] Others have accused Google of basing search rankings on advertising spending, favoring those who spend more on advertising.[19] Similarly, news outlets report that Amazon ranks recommendations based on which sales will generate the most revenue for Amazon (e.g., whether it is an Amazon product or

---

[16] It is important to keep in mind that these descriptions of network effects are generally descriptive, rather than as subject to mathematical certainty as these descriptions would suggest.
[17] Tim Sullivan, *Blitzscaling*, HARV. BUS. REV. (Apr. 2016), https://hbr.org/2016/04/blitzscaling.
[18] *See* Mattioli, *supra* note 4; Julie Cresswell, *How Amazon Steers Shoppers to Its Own Product*, N.Y. TIMES (June 23, 2018), https://www.nytimes.com/2018/06/23/business/amazon-the-brand-buster.html; Greg Ip, *The Antitrust Case Against Facebook, Google and Amazon*, WALL ST. J. (Jan. 16, 2018), https://www.wsj.com/articles/the-antitrust-case-against-facebook-google-amazon-and-apple-1516121561.
[19] *"A Fair Playing Field? Investigating Big Tech's Impact on Small Business" Before the H. Comm. on Small Business*, 116th Cong. (2019) (testimony of Allyson Cavaretta).

a third-party product, whether the third-party vendor uses Amazon's "fulfillment center" for shipping or does not).[20] Google and Amazon deny these allegations, but because Google and Amazon control all the relevant information there is no way to independently determine the truth.

In addition, the information collected by the platform from customers with regard to their relevant habits, both individually and collectively, makes it harder for any new entrant to contest the market. Google as the dominant advertising platform can claim, with considerable justification, that no rival platform can match its ability to precisely place advertisements based on a detailed description of the target demographic because Google has assembled more information on every target demographic than any other advertising platform, simply by virtue of its dominance.[21] Similarly, Amazon controls approximately 40 percent of U.S. online retail,[22] giving it unrivaled information with regard to consumer online purchasing habits. The information Amazon collects from third-party vendors reinforces the power of its own algorithms and market research, creating an ever-widening gap with potential rivals in the ability to develop, recommend, and display products.

---

[20] Mattioli, *supra* note 4; Stacy Mitchell & Shaoul Sussman, *How Amazon Rigs Its Shopping Algorithm*, PROMARKET (Nov. 6, 2019), https://promarket.org/2019/11/06/how-amazon-rigs-its-shopping-algorithm/.

[21] *See* Jacques Crémer et al., *Commission Report on Competition Policy for the digital era* (2019), https://ec.europa.eu/competition/publications/reports/kd0419345enn.pdf. Facebook, Google's chief rival for advertising, relies on placing ads in its newsfeed. While it enjoys enormous information advantages over users, the mechanics are different from Google's dominance in ad placement on the Internet at large. Keach Hagey & Vivien Ngo, *How Google Edged Out Rivals and Built the World's Dominant Ad Machine: A Visual Guide*, WALL ST. J. (Nov. 7, 2019), https://www.wsj.com/articles/how-google-edged-out-rivals-and-built-the-worlds-dominant-ad-machine-a-visual-guide-11573142071.

[22] Adam Levy, *Amazon Could Still Gain E-Commerce Market Share in 2020*, FOOL.COM (June 10, 2020), https://www.fool.com/investing/2020/06/10/amazon-still-gain-e-commerce-market-share-in-2020.aspx.

A: Termination Monopoly and Cost of Exclusion/Unavoidable Partners Prevent Development of Market-Based Solutions

As a general matter, when businesses must expose proprietary information as part of a transaction, they protect their proprietary information through contracts. But in the case of certain two-sided platforms, including digital platforms, certain factors prevent this. Platforms in general bring buyers and sellers together and facilitate transactions otherwise impossible. To do this, platforms will often require that each party expose information to facilitate the underlying transaction. This is not a matter of choice. For the system to work, the platform must have certain information from both the buyer and the vendor. For example, to place a mobile call, the telephone network must know the point of origin and point of termination, the duration of the call, the physical location of the caller, the type of handset, and other "metadata" associated with the call.[23] In addition, as a function of federal law, the network must retain the ability to access the content of the call so that law enforcement may have access subject to due process.[24]

Platforms have no incentive to compete on protecting the proprietary information buyers and vendors must expose from self-use for several reasons.[25] As an initial matter, platform competition is often limited due to the expense associated with creating platforms. A local flea market is a platform that is cheap to provide, and has little leverage to extract proprietary information. A global, or even national telephone network is very expensive to build. Even in a market with competing telephone networks, the platform has a *termination monopoly* for any given transaction. That is to say, a caller using the network for a set of calls is locked into the particular platform for those calls. Even if the caller selected a network based on protecting confidential information, the caller would still need to expose the information to the network of any person she wished to call. The only way the caller can reach the person on the rival network is through the particular platform to which the called party subscribes.

---

[23] Metadata is technically "data about data." In telecommunications, it generally means information associated with a communications other than the content, such as the point of origination, destination or duration of the transmission.

[24] Communications Assistance for Law Enforcement Act, Pub. L. No. 103-414, 108 Stat. 4279 (1994) (codified at 47 U.S.C. §§ 1001-1010 (2018)). (Nothing prevents the caller from encrypting the call, but even that cannot protect the associated "metadata," since the network cannot place the call without this information.)

[25] Platforms have incentive to prevent exposure to rivals, and therefore also have incentive to prevent accidental exposure.

Returning to the problem of digital platforms, vendors have no choice but to expose their information to platforms if they want to reach buyers on their platforms. Because people generally make their choices as to which platforms to use based on factors unrelated to protecting the proprietary information of vendors, vendors must either forgo the buyers on the platform or accept the terms. Some vendors may initially have sufficient market power to demand protection of their proprietary information. As specific platforms become more embedded in society, however, they become increasingly difficult to avoid. To take a few examples, it is impossible to imagine trying to conduct business without credit cards or some kind of equivalent electronic payment platform. Indeed, we have reached a point where states and localities must pass laws to protect the ability of low-income or credit-poor consumers to pay cash.[26] Similarly, it is increasingly difficult to participate in modern society without access to electronic communications such as a cell phone and/or broadband. Businesses must engage in real time ordering and communications, and doing so requires exposing their proprietary information to the communications network. Eventually, even the most powerful vendor must surrender access to proprietary information in order to use platforms that have become "must have" platforms to conduct business and reach buyers.

This is not market power in the classic sense. It is possible for a market to be competitive in antitrust terms but still require doing business with a platform that must have access to proprietary information to function, and that has no incentive to avoid using that information to its own advantage. We may think of the problem as being the "cost of exclusion" (CoE) from the customers on the digital platform. In general terms, we may think of the cost of exclusion as the power of foreclosure from the platform, adjusted for the power of the network effected that makes it harder for the vendor to pry the buyer away from the platform.[27]

---

[26] Charisse Jones, *Should You Ditch Your Cash? A Growing Number of Cities Say No Way*, USA TODAY (Sept. 9, 2019), https://www.usatoday.com/story/money/2019/09/09/going-cashless-if-you-do-these-cities-youre-breaking-law/2124163001/ (last updated Dec. 27, 2019, 2:34 PM).

[27] I provide a more precise definition in Chapter 1 of *The Case for the Digital Platform Act. See* FELD, *supra* note 1.

It is worth repeating that it is impossible to expect a market solution to emerge in this situation, even when other interventions are made to promote competition. For example, where interoperability requirements nullify the ability of platforms to capture buyers and achieve sufficient market power, it provides no advantage for any one platform to deny itself the use of a vendor's proprietary information, since the vendor will need to expose the same information to rival platforms to reach buyers on those rival platforms, and the digital platform's competitor will now have use of the vendor's information and can use it to steal the vendor from the competing platform. Nor can the vendor or the competing platform refuse to provide the information to the competing platform. The transaction does not work, and therefore the platform does not bring together buyer and vendor to perform the desired transaction, without the vendor and the buyer exposing their proprietary information to the platform.

B: Lock-In, Vertical Integration, and Information Asymmetry Increase the Potential for Abuse

The potential for abuse can be further aggravated by two additional factors, the power of lock-in and the capacity of the platform for vertical integration. In this case, "lock-in" refers to the difficulties either a buyer or vendor has in shifting to another platform. This includes potential disruption of existing buyer/vendor relationships and the difficulty a buyer and vendor will have in finding each other again if one or the other shifts platform. As a general matter, lock-in creates the opportunity for a platform to exploit their relationship with customers even in the absence of traditional market power.[28] In this case, lock-in impacts both the buyer and the vendor. Even if a vendor feels itself sufficiently threatened to attempt to move to another platform, even loyal buyers are unlikely to follow if buyer lock-in is sufficiently high.

Platforms can create lock-in in a variety of ways outside of traditional mechanisms such as high switching costs.[29] For example, Amazon has been accused of penalizing vendors whose products are offered on rival sites for lower prices – even if the vendor is not responsible for the

[28] Luke Garrod et al., *Competition Remedies in Consumer Markets*, 21 LOYOLA CONSUMER L. REV. 439, 444-45 (2009).

[29] Switching costs need not be purely monetary. Often for consumers switching costs involve the mental effort of learning new operating systems, developing new habits, or unlearning previously trained responses.

sale price offered by the rival.[30] This goes beyond a traditional "most favored nation" clause, where a vendor commits to providing to a platform or retailer the best price offered to any platform or retailer (i.e., that if the vendor offers a cheaper price to a third party, it will offer the same price to the platform). By even offering the product to a rival platform at the same or higher price than that offered to the first platform, the vendor takes the risk that the rival will discount the product as a loss leader, which will result in Amazon penalizing the vendor. This dramatically increases the difficulty for the vendor in developing business on an alternate platform, increasing lock-in.

Additionally, the ease with which digital platforms move into vertical markets makes it easier for platforms to exploit CPNI. As discussed in greater detail in chapter 1 of *The Case for the Digital Platform*, the structure of digital platforms creates certain advantages in expanding vertically. The use of the internet as the means of access and distribution saves costs. The reliance on information and knowledge of the public/buyer side of the platform helps the platform target vertical markets for expansion. As the Nobel prize winning economist Jean Tirole observed in 2018, today's dominant platforms all began serving niche markets and grew through a combination of horizontal growth and vertical expansion.[31]

Amazon provides a textbook example of how the unique structure of digital platforms allows rapid expansion into vertical markets, and how the use of proprietary information exposed by the buyer and vendor enhance these capabilities. Amazon began as an online book retailer. Once it established customer relations and channels of distribution, expanding to selling other products was far easier than it would have been for a traditional bookstore to add a physical appliance section. On the reverse side, Amazon could gradually expand vertically into warehousing, then shipping, then combining the two into "fulfillment centers." Ultimately, Amazon could move to manufacturing its own line of products and compete directly with third-party sellers on the platform.

---

[30] Karen Weise, *Prime Power: How Amazon Squeezes the Businesses Behind Its Store*, N.Y TIMES (Dec. 12, 2019), https://www.nytimes.com/2019/12/19/technology/amazon-sellers.html?action=click&module=Top%20Stories&pgtype=Homepage.

[31] Allison Schrager, *A Nobel-Winning Economist's Guide to Taming Tech Monopolies*, QUARTZ (June 27, 2018), https://qz.com/1310266/nobel-winning-economist-jean-tirole-on-how-to-regulate-techmonopolies/.

At each stage, Amazon could minimize the risk to itself by using the accumulated proprietary information collected on both sides of the platform. This includes information that vendors would not willingly disclose had they known that Amazon would use it to compete against them. But at the time the vendors began to use the platform, Amazon wasn't competing against them. Nor could vendors have reasonably anticipated that Amazon might decide to expand into their particular market. Indeed, it is arguably because Amazon has the capability to observe the sales data and other proprietary information of third-party vendors that it decides into which product lines to expand.

To conclude the basic statement of the problem: The unique position of digital platforms requires that both buyers and vendors expose proprietary information to the digital platform. Because exposure of this information is necessary for the platform to deliver the service, neither the buyer nor the vendor can simply refuse to provide the information. For the reasons explained above, even if some vendors may have sufficient power to protect themselves (at least initially), the market will not produce a solution. Digital platforms generally have the ability to exploit the information, and therefore the incentive to exploit the information. For all these reasons, addressing the problem requires a regulatory remedy.

PART II:

SOLUTION: LIMIT THE USE, NOT THE COLLECTION, OF CUSTOMER PROPRIETARY NETWORK INFORMATION

To some degree, law can limit the collection of information to that necessary to perform the necessary transaction. For the service to function, both buyer and vendor must disclose information they would consider proprietary to the platform. Nor is it easy to predict the nature of the information either party must disclose to the platform, given that platforms may offer a wide variety of services. Indeed, as platforms continue to innovate and expand, the types of services they permit vendors to offer buyers, the types of information vendors and buyers may need to disclose constantly changes.

CPNI therefore does not focus on limiting the collection of information. Rather, CPNI focuses on restricting the ***use*** of the information collected. CPNI assumes that both the buyer and the vendor continue to control their proprietary information as they normally would – but for the

technical requirement to reveal the information to the platform. Buyers retain the right to require platforms to disclose their information to competing vendors in usable form, essentially a form of "data portability." Platforms are prohibited from disclosing information collected from buyers or vendors to third parties without express, affirmative consent. Additionally, while the platform is permitted to use the information for the purpose collected, it is not generally permitted to use the information collected for other uses.

Consider the following example. To promote competition in the telephone industry, Congress required the development of "number portability" – the ability of consumer to move phone numbers from their current network to a rival network.[32] When a customer switches from one provider to another, the "winning" provider informs the "losing" provider and requires that the losing provider transfer the phone number. Since transferring the number used to take several days, Verizon initiated a "customer retention plan." Using the advance notice that a customer was leaving, Verizon would contact the customer and offer incentives to remain with Verizon before transferring the number – undermining the pro-competitive goals of the statute. The FCC ruled[33] (and the D.C. Circuit affirmed)[34] that using the number port request to market to a departing customer violated the CPNI rules by taking the information given by a rival carrier for the purpose of offering a telecommunication service and using it for an unauthorized purpose.

A: Limitations and Exceptions

It is important to recognize that while CPNI limits the ability of platforms to engage in certain types of anticompetitive activity, it is not the same as a prohibition on discrimination or other forms of self-preferencing. A platform knows which products are its own, and can favor them without taking advantage of proprietary information from buyers and vendors. To return to the example of cable, cable operators can give channels they own superior position on channel guides or in clusters with similar programming, while banishing rival channels to premium tiers

[32] *See* 47 U.S.C. § 251(e) (2018); 47 C.F.R. §§ 52.20-36 (2018).
[33] *In re* Implementation of the Subscriber Carrier Selection Changes Provisions of the Telecommunications Act of 1996: Policies and Rules Concerning Unauthorized Changes of Consumers' Long Distance Carriers, 18 FCC Rcd. 5099, 5109 ¶ 25 (Mar. 17, 2003).
[34] Verizon California, Inc., v. FCC, 555 F.3d 270 (D.C. Cir. 2009).

or locations where casual viewers are less likely to find them.[35] CPNI is an important tool in protecting competition, but it is best used in combination with multiple tools – such as non-discrimination and portability obligations – to achieve maximum effect.

In addition to its limits, the CPNI statute creates 3 primary types of exceptions to the general rule controlling use and disclosure. The first category involves protecting the carrier and other customers of the carrier. For example, the statute makes clear that a carrier can use CPNI to prevent harm to the network. The second category involves public safety, including disclosure to law enforcement. The third category permits carriers to use aggregate information, and to share aggregate information with third parties – provided they do so on a non-discriminatory basis. These exceptions respect the rights of the carrier and other users, and permit uses of the information Congress judged beneficial.[36]

As discussed in greater detail below, applying the basic principles of CPNI to digital platforms requires the development of similar exceptions. Digital platforms, like telecommunications carriers, need to protect their ability to bill vendors and (where appropriate) buyers. Platforms also have a responsibility to protect other users of the platform from potential abuse. This may require, for example, identifying buyers with a history of defaulting on payment or vendors with a history of poor performance. Finally, certain types of research and information in the aggregate are necessary to the recommendation functions of platforms. There is some tension between using aggregate CPNI to better develop recommendation software and limiting the ability of platforms to use the information in a potentially anticompetitive manner. Determining the right place to strike this balance will be one challenge in implementation.

B: Potential First Amendment Issues

In theory, regulating commercial uses of collecting data should no more raise First Amendment issues than would the regulation of collecting recycling. It is difficult to see as an

---

[35] *See In re* Applications of Comcast Corporation, General Electric Co. and NBC Universal, Inc.; For Consent to Assign Licenses and Transfer Control of Licenses, 26 FCC Rcd. 4238 ¶ 112 (Jan. 18, 2011).

[36] *See generally* S. COMM. ON SCIENCE, COMMERCE, AND TRANSP., TELECOMMUNICATIONS COMPETITION AND DEREGULATION ACT OF 1995, S. REP. NO. 104-23, at 89-91 (1995) (explaining balancing of interests in drafting Section 222).

initial matter how a collection of facts associated with an individual that have no expressive quality should raise a concern under the First Amendment. Prohibiting a platform from collecting sales information from a vendor or buyer to research products would likewise appear to lack any expressive meaning, and therefore raise no more First Amendment concerns than regulation of cement or rebar steel in construction.

The case law, however, is somewhat more complicated. In *U.S. West v. FCC*, 182 F.3d 1224 (10th Cir. 1999), the Federal Court of Appeals for the Tenth Circuit found that by preventing a carrier from using CPNI to "target" commercial speech, that the CPNI rules infringed on the carrier's First Amendment right. By this logic, of course, any statute which required someone to respect a "no trespassing" sign would violate the first Amendment by depriving the would-be speaker from narrowing the audience.[37] Likewise, under the same logic, prohibitions on spyware and eavesdropping should raise First Amendment concerns that such laws limit "targeting" an audience by using information collected without express consent. Nevertheless, other courts have also found some level of First Amendment interest by carriers in the use of CPNI, at least in the context of carriers seeking to market to customers. *See Verizon California, Inc. v. FCC*, 555 F.3d 270 (D.C. Cir. 2009).

Courts that have found a First Amendment interest on the part of carriers subject to CPNI restrictions have analyzed the right to target an audience under the "commercial speech" test of *Central Hudson Gas & Electric Corp. v. Public Service Commission of New York*, 447 U.S. 557 (1980) ("*Central Hudson*"). Under *Central Hudson*, the speech must not be misleading, the government interest in limiting the speech must be "substantial," and the regulation must directly advance the interest asserted. *See NCTA v. FCC*, 555 F.3d 996 (D.C. Cir. 2009) (applying *Central Hudson*). In analyzing the potential First Amendment risk to adapting CPNI regulation to digital platforms, one should therefore consider several important points.

First, courts considering the CPNI regulations have not considered limitations on the use of data for non-expressive purposes, such as product development – or even the sale of information to third parties. The First Amendment interest lies with the desire of the carrier to narrow its audience by using the information obtained through the carrier-customer relationship under 47 U.S.C. §222(c), or the proprietary information revealed by a carrier to another carrier

---

[37] For a more detailed critique of *U.S.West*, *See* Niel M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 U.C.L.A. L. REV. 1150, 1193-95 (2005).

for the purpose of providing a telecommunications service under 47 U.S.C. §222(b). No case has examined whether a carrier has a First Amendment interest in using collected data in non-expressive ways, such as developing a competing service, determining how to price a rival product, or using the information to fine tune an algorithm. There is no reason to assume that limitations on such uses should raise First Amendment issues.

Opponents of privacy regulation rely heavily on *Sorrell v. IMS Health, Inc.*, 564 U.S. 552 (2011) to argue that restrictions on the collection and use of information must survive "strict scrutiny," the highest degree of First Amendment scrutiny.[38] The law at issue in *Sorrell,* however, went well beyond general limitations on the use of data imposed by CPNI. *Sorrell* dealt with a prescription privacy law passed by the state of Vermont which expressly prohibited the sale or use of pharmaceutical prescription information for marketing, while expressly permitting it for other purposes. The Supreme Court found that targeted marketing constituted a viewpoint-specific limitation subject to strict scrutiny. Importantly, the Court explicitly declined to address whether limitations on collection and use of information generally give rise to First Amendment concerns because the Vermont law at issue imposed specific, content-based, viewpoint discrimination.[39] The Court also noted that "the First Amendment does not prevent restrictions directed at commerce or conduct from imposing incidental burdens on speech,"[40] so that the fact that laws promoting competition or prohibiting racial discrimination that prohibited certain written contracts did not raise First Amendment concerns. This certainly suggests that where CPNI prohibits non-expressive conduct – such as using sales information for product development – it raises no First Amendment concerns.

Finally, further undermining the argument against strict scrutiny, the Court went on to apply the *Central Hudson* test to the Vermont law at issue rather than traditional strict scrutiny.[41] It is therefore reasonable to assume that to the extent application of CPNI obligations to digital platforms raises First Amendment concerns, the rules must meet the "commercial speech" standard imposed by *Central Hudson* – i.e., the limitations on the identified speech interest must

[38] Under "strict scrutiny," a law must promote a compelling government interest, using the least restrictive means possible. So few regulations can survive such scrutiny that it is sometimes referred to as "strict in theory, fatal in fact."
[39] Sorrell v. IMS Health, Inc., 564 U.S. 552, 563-64 (2011).
[40] *Id.* at 567.
[41] *Id.* at 571-72.

serve an important government purpose, and must directly (rather than incidentally) advance the stated purpose. This view is further buttressed by other cases applying the commercial speech test to similar laws restricting using information for targeted advertising.[42]

Here, the government has several important purposes. First, the government has an interest in protecting both the traditional common law right of privacy of individuals and the traditional interest of businesses in protecting their proprietary information. Additionally, the government has a strong interest in not merely protecting, but in affirmatively promoting competition in an important sector of the economy. As discussed above, existing evidence gives rise to concern that abuses are already taking place in the market, and absent government intervention it is impossible to prevent abuses from occurring – or even to determine with certainty whether or not they are taking place. We should therefore anticipate that to the extent CPNI regulations in the digital platform context raise First Amendment concerns, reasonably constructed CPNI regulations will survive First Amendment scrutiny.

PART III:

IMPLEMENTING CPNI FOR DIGITAL PLATFORMS

Just as regulating digital platforms required both a description and statutory language, implementing CPNI for digital platforms likewise requires a similar translation. In the case of CPNI, we begin with a pre-existing statute. However, as *The Case for the Digital Platform Act* repeatedly cautions, while the regulation of telecommunications networks provides important lessons for the regulation of virtual networks such as digital platforms, one cannot simply cut and paste previously successful regulations and expect them to work. In particular, the lack of a clearly defined physical network makes the demarcation points between relevant lines of business harder to determine. The wide variation in the type of information platforms need to perform their functions – especially their search and recommendation functions – means rethinking the nature of the exceptions to the rule to facilitate beneficial uses while effectively guarding against anticompetitive behavior.

---

[42] *See, e.g.*, U.S. West v. FCC, 182 F.3d 1224 (10th Cir. 1999).

A: General Duty to Protect Customer CPNI

Nevertheless, we may begin with the same general duty to protect proprietary information found in Section 222(a), reworded for digital platforms. Existing Section 222(a) requires telecommunications carriers to protect the "confidentiality of proprietary information of, and relating to, other telecommunications carriers, equipment manufacturers, and customers, including telecommunications carriers reselling telecommunications services of a telecommunications carrier." The specific references to equipment manufacturers and telecommunications resellers address specific aspects of the communications marketplace as they evolved and existed in 1996. AT&T controlled equipment manufacturing as part of its monopoly over the telephone system during most of the 20th century. The FCC's original CPNI rules were designed to foster an independent market in equipment, and therefore applied the obligation to protect proprietary information relating to equipment to protect competition in the related equipment market as well as in the market for competing basic telecommunications and "enhanced" services.[43]

The rule for digital platforms, however, does not arise out of the effort to introduce competition into an existing monopoly and related monopoly markets. Rather, the goal here is to protect existing competition and prevent unfair self-dealing. Accordingly, the general duty can be limited to the parties on the platform: buyers and vendors. "A digital platform must protect the confidentiality of the proprietary information of any buyer or vendor relating to the use of the platform." As with the existing CPNI statute, the definition of "proprietary information" should be broad enough to encompass information that could be abused in the manner described in Part I as either conferring an anticompetitive advantage (such as aiding the platform in directly competing with a vendor) or some other form of unfair self-dealing (such as favoring a vendor using platform-affiliated services over one that does not).

In this, we should explicitly draw comparison with the definition used by the FCC. In interpreting the definition of "proprietary information" in the statute, the FCC has made it clear that it means any information that comes into the hands of the carrier "as a consequence of the

[43] FELD ET AL., *supra* note 2.

customer/carrier relationship."[44] For this reason, the general obligation proposed above for Section (a) of the new digital platform statute includes the phrase "related to the use of the platform." The intent is to capture things such as the use of affiliated services that are related to the sort of transactions that occur on the platform between buyers and vendors. For example, whether or not a vendor uses Amazon's fulfillment centers or handles shipping on its own would be "related to" a vendor's use of Amazon to sell its product.

This general prohibition is broad enough to address either deliberate or careless disclosure to third parties. While such a duty could be extended to a more generalized privacy protection statute, or to limit targeted advertising, that goes beyond the scope of this paper. The proposal here is intended to be a narrow one, focused exclusively on protecting and promoting competition among vendors on digital platforms. Interpretation of this general obligation should bear this in mind, and focus on protecting information that arises in the course of a vendor/buyer transaction rather than simply from consumer use of the platform (unless expanding general privacy protection is explicitly intended).

B: Specific Limitations on the Use of Vendor CPNI

Section 222(b) directly addresses information provided by rival telecommunications service providers for the purpose of offering a directly competing telecommunications service. In the absence of any interconnection requirement between digital platforms, there is no corresponding section requiring digital platforms to protect proprietary information of other digital platforms. In the event Congress were to adopt mandatory interconnection requirements or portability obligations, a provision analogous to Section 222(b) would be required to facilitate competition. As demonstrated by the *Verizon California* case discussed above, if the platform could use the request to port data or information exposed by a competitor through interconnection for its own purposes, it would frustrate the development of a competitive market. Since this paper assumes only adoption of a CPNI regime for digital platforms and no other pro-

[44] *See In re* Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information, *Declaratory Ruling*, 28 FCC Rcd. 9609 (June 13, 2013).

competitive regulations, the next requirement following a general duty to protect customer proprietary information is the specific definition of CPNI and the responsibility to protect it.

Instead, Section (b) of the digital platform CPNI statute should address the other competitive concern addressed by traditional CPNI, competition between the platform and vendors offering goods and services in related markets. This requires a prohibition on the platform using information provided by the vendor to the platform for any purpose beyond the express purpose of the platform providing the promised function. For example, if a vendor uses Amazon's "fulfilment center," that information should not be used by Amazon in determining whether to give that vendor preference in marketing. Whatever factors Amazon uses to create its recommendations, it should be prohibited from using any information provided to it by the vendor for another purpose.

Platforms often argue that they favor vendors using affiliated services as a form of quality control, or to ensure a better and more uniform customer experience. But these arguments do not stand up to close examination. As an initial matter, there is no guarantee that using a service affiliated with the digital platform rather than the vendor will provide a better experience for the buyer. Indeed, one way a vendor may try to distinguish itself from a platform with which it must compete is by providing better customer service in a variety of ways. For example, during the COVID-19 pandemic, Amazon experienced a massive surge in orders as huge swaths of the population were ordered to stay at home to try to control the outbreak. Amazon made the decision to prioritize critical food and medical supplies impacted by the disruption in supply chains and often in short supply from local retailers. This combination of factors, in addition to disruptions in Amazon's own supply chains, created massive delays in Amazon's delivery services. As a result, some vendors handling their own shipping rather than using Amazon's fulfilment services were capable of filling and delivering orders much faster than Amazon or vendors using Amazon's fulfillment service. Nevertheless, because the algorithm for recommendations in the "buy box" favored Amazon's own products and products using Amazon fulfillment services rather than vendors actually promising quicker delivery time, these competing vendors with superior delivery times were shut out of Amazon's buy box and therefore effectively invisible to buyers.[45] Prohibiting Amazon from using information related to

[45] Jason Del Rey, *Amazon Says It Unintentionally Hid Some Competitors' Faster Delivery Options*, VOX (Mar. 26, 2020, 8:32 PM),

the source of the product or whether the vendor uses affiliated services would force Amazon to rely on actual information about delivery times, genuinely creating a better customer experience and allowing vendors to compete on a level playing field.

Additionally, at least where the platform purports to offer the services separately,[46] the choice should be left to the vendor whether the advantages of using the platform's services outweigh the disadvantages. A vendor has many reasons why it might or might not want to use a platform's affiliated services, such as establishing a more direct relationship with a buyer, having greater control over the customer experience, or withholding additional revenue from a potential rival with whom it must do business to reach customers. This is especially true where the digital platform is dominant, or otherwise a "must have" partner for the success of the vendor.

Prohibiting the digital platform from using proprietary information for marketing, product development, or other means of competition with vendors does not prevent the digital platform from taking necessary steps to protect the customer experience or gather appropriate information for formulation of recommendation algorithms. Platforms are free, for example, to require various forms of reasonable quality assurance (such as proof of delivery to a buyer). This information would be collected for the specific purpose of quality assurance, and could be used only for that purpose. Similarly, a statement to vendors that their success or failure in quality metrics will impact their rankings in recommendation algorithms would make this information fair game for inclusion. Likewise, complaints from buyers to the platform about the vendor, or information about the vendor derived from other sources (such as routine credit checks or information appearing in the press or in trade publications) fall outside the scope of proprietary vendor information.

This is particularly important with regard to advertising services to the public. Advertisements are not generally regarded as "proprietary," even if they are limited in distribution. While the details a vendor may provide to an advertising platform may be

---

https://www.vox.com/recode/2020/3/26/21193928/amazon-delivery-delays-april-21-23-faster-speed-sellers-marketplace-buy-button.

[46] Like other pro-competitive obligations, the question of whether to impose unbundling requirements is separate from the question of CPNI. But certainly, where a digital platform maintains that it offers its services on an unbundled basis, or that use of an affiliated service does not impact recommendation rankings, CPNI should prohibit use of proprietary information to undermine these representations.

proprietary information, the content of the advertisement is not itself protected by the CPNI rules. Nor does the use of social media or online classified ads to advertise goods and services impose any obligation on the platform. If I post on Facebook that I am selling my comic book collection, that information is not "proprietary" within the meaning of the statute and may be treated as any other content.

Section 222(b) of the existing statute does not allow telecommunications carriers to waive the protection of the existing CPNI statute. This stands in marked contrast to the protections for retail customers, where the customer may direct the telecommunications provider to transfer the information to a third party or may waive the protections and allow the telecommunications carrier to use the information for other purposes. The reason for this is fairly straightforward. Allowing a carrier to waive the protections of Section 222(b) would simply invite dominant carriers to require such a "voluntary" waiver as a condition of doing business – effectively rendering Section 222(b) a nullity. For the same reason, the digital platform CPNI statute should not permit vendors to waive the protections on vendor proprietary information. Whereas customers/buyers may have an interest in directing the platform to disclose necessary information to third parties to make transactions easier (or to support pro-competitive requirements such as interconnection and portability), vendors are well suited to handling the transfer of such information themselves should it become necessary. There is therefore little, if anything, to be gained from allowing vendors to waive CPNI protections, whereas allowing it opens the door to abuse.

C: Specific Limitations on the Use of Buyer CPNI

The law generally distinguishes between the protections provided to businesses and consumers. In the original CPNI statute, the protections afforded to customers reflected both a pro-competitive policy of prohibiting carriers from using information derived from the customer side to "reverse engineer" the proprietary information of competing carriers or enhanced service providers, and consumer protection policy of guarding personal privacy. Certainly, a digital platform CPNI statute could encompass both goals. But the consumer expectation of privacy on digital platforms is radically different from what consumers expected with telecommunications providers at the time Congress adopted Section 222. People have always enjoyed an expectation

of privacy in their personal communications both under the common law[47] and since adoption of the Communications Act of 1934.[48] By contrast, the history to date of privacy on digital platforms is fairly dismal. Importing the consumer privacy protection aspects of CPNI into the world of digital platforms – while certainly welcome – would represent a radical change.

This paper therefore proposes modifications to the CPNI regime that emphasize the pro-competitive aspects of protecting customer CPNI, and proposes exceptions that permit existing practices such as targeted advertising. By doing so, Public Knowledge in no way endorses the existing privacy *status quo* or retreats from its aggressive advocacy on personal privacy. Rather, because the purpose of this paper is to focus on CPNI as a mechanism of enhancing competition, this paper will avoid proposals that would require fundamental changes in the business model of many digital platforms – however welcome such changes would be and however much Public Knowledge might support them in other contexts.

As the first modification, the digital platform CPNI statute should be limited to information deriving from the buyer/vendor transaction, not from the general transaction between the consumer buyer and the platform. The original CPNI statute dealt with common carrier telecommunications providers. In that context, the customers expected the carrier to act as a "dumb pipe" between the customer placing the call and the person or business receiving the call. If a consumer purchased a product over the telephone, the consumer did not traditionally expect the phone company to become involved. Even if a customer purchased an enhanced service such as dial-up internet access or a call forwarding and answering service, the only thing the customer held the telephone company accountable for was the quality of the phone line. By contrast, digital platforms position themselves as intermediaries between the vendor, often invoking this ability to protect customers and guarantee a consistent customer experience as one of the services of the platform. Even where platforms initially disclaim such responsibilities, users often contact platforms and try to hold them accountable for problems arising from transactions with vendors. Because the relationship between the buyer and the platform is substantially different from the vendor/platform relationship, a complete ban on the use of buyer CPNI comparable to vendor CPNI is neither necessary nor appropriate.

---

[47] *See* notes 9 & 11, *supra* and sources cited therein.
[48] *See* 47 U.S.C. §605 (2018).

Additionally, unlike the vendor, whose relationship with the platform is simply to reach buyers, digital platforms invest in a wide variety of services to attract users who become buyers. Indeed, as a key feature of digital platforms is that they allow users to self-organize, interact with each other, and engage in multiple activities simultaneously, it is appropriate for the digital platform to reap the rewards of its customer relationship for these services that are unrelated to the specific buyer/vendor transaction.

The search and recommendation function offered by digital platforms, and an integral part in facilitating the buyer/vendor transaction, illustrates the points of commonality and the highly significant points of allowing the digital platform access to buyer CPNI versus access to vendor CPNI. Vendors have the greatest potential for a conflict of interest with digital platforms, and the greatest vulnerability to a digital platform using CPNI to privilege itself unfairly. Vendors want to "win" the search/recommendation contest at all costs. Studies have repeatedly confirmed that appearing at the top of a search result list or in a "buy box" or as part of a series of recommendations (such as YouTube's recommended videos or Amazon's "people who bought this also bought" feature) dramatically increases the likelihood of attracting a buyer.[49] By contrast, failing to appear in the results, or appearing fairly low down in a search/recommendation result, renders the vendor effectively invisible to buyers.[50] If the digital platform is also a competing vendor, or has reason to favor one vendor over another, it can do so easily based on vendor CPNI. A simple rule prohibiting use of CPNI by the platform provides an easy and straightforward means of protecting vendors from such manipulation, as well as other forms of abuse.

But the overlap of interests between buyers and digital platforms is more complicated. It is often stated that the platform has the incentive to create the "best" search/recommendation function that most satisfies the customer, or customers will go to competing platforms. This is, however, overly simplistic. For one thing, the perfect information asymmetry problem created by

---

[49] *See* Renee Dudley, *Amazon's New Competitive Advantage: Putting Its Own Products First*, PROPUBLICA (June 6, 2020, 5:00 PM), https://www.propublica.org/article/amazons-new-competitive-advantage-putting-its-own-products-first; *see also* Stacy Mitchell & Shaoul Sussman, *How Amazon Rigs Its Shopping Algorithm*, PROMARKET (Nov. 6, 2019), https://promarket.org/2019/11/06/how-amazon-rigs-its-shopping-algorithm/.

[50] Some vendors may have particular "target audiences," and therefore may not wish to win every search/recommendation, but this does not change the overall conclusion.

the structure of digital platforms makes it extremely difficult, if not practically impossible, for platform users to determine whether a search/recommendation function is better or worse than a rival. This also ignores that buyers using a search/recommendation function frequently have a wide range of products they consider acceptable, and have no way to evaluate the missed opportunities because a platform used CPNI to maximize revenue to itself. Alternatively, other features of the platform may hold the buyer, making inferior results from the search/recommendation function acceptable over the switching cost. Finally, especially where a platform has market dominance, the revenue lost from some customer churn may be more than offset by the advantages gained from manipulating search/recommendation using CPNI to advantage itself.

Nevertheless, a digital platform still must make the search/recommendation function sufficiently useful and relevant to attract and hold customers. Furthermore, the likes and dislikes of individual customers are different. A tremendous strength of digital platforms and a positive use of collected personal data is increasingly accurate recommendations that genuinely help consumers find things they like and want. While "enhancing customer experience" can be used as an excuse for a wide variety of bad conduct, it works because enhancing customer experience is a laudable goal and one of the strengths of a competitive market. We do not want to construct CPNI rules that significantly degrade the ability of platforms to create responsive search/recommendation features. This makes a blanket rule against using even buyer/vendor information impractical. Even aggregate recommendation features need to know information about the individual to whom they are making the recommendation. "People who watched X also watched Y and Z" requires knowing that the buyer just watched X, as well as taking aggregate data for everyone who watched X.

We therefore should shape the limits on the use of customer CPNI to address the primary types of manipulation about which we are concerned: (a) using specific information to "poach" customers from vendors, or to enable rival vendors to interfere with the buyer/vendor relationship in exchange for consideration; (b) using buyer CPNI to "reverse engineer" seller CPNI; and (c) otherwise using buyer CPNI to disadvantage or punish vendors. For example, assume a situation where Amazon wants to pressure vendors to use its fulfilment centers. Amazon is prohibited from using the information about the vendor's use or non-use of fulfilment center for calculating its algorithm. But it knows when a buyer orders a product from a vendor

that does not use the fulfilment center from the buyer's CPNI. Amazon can use the buyer's CPNI to identify and punish vendors who handle their own shipping in numerous ways, unless prohibited from using buyer CPNI for that purpose.

In terms of drafting legislative language, the best approach is to prohibit use of buyer CPNI for these activities, with an explicit exception that inclusion of buyer CPNI in a search/recommendation algorithm, or to prevent targeted advertising or key word advertising by rival vendors. This exception needs to be explicit in the statute to prevent reading the prohibition on using buyer CPNI to market to buyers as prohibiting these uses. This mirrors the exception in the existing CPNI statute for publishing directories. Additionally, just as the existing CPNI statute only prohibits the use of personally identifying CPNI and permits aggregate use of CPNI data, the digital platform CPNI statute should only prohibit use of buyer CPNI that is clearly identifiable to the specific buyer/vendor transaction.[51] I discuss aggregate use in greater detail in the general exceptions section below.

D: Exceptions: Protecting the Platform and Protecting Other Users

As discussed in Part II, the original CPNI statute has three basic categories of exceptions: protecting the network and other customers of the network, protecting public safety, and the use of aggregate data. The reasons for the first two are straightforward, but their application in the digital platform space will be considerably different from in the carrier space. By contrast, the reason for the aggregate data exception derives from the general history of the evolution of privacy law in the 20th century, and therefore will generally apply in the same fashion – taking into account the increasing ability of third parties to disaggregate information and re-link it to individuals.

i: Protecting the Platform and Protecting Others

The statutory exceptions to the existing CPNI statute are fairly technically detailed. As a general rule, the narrower and more detailed the exception, the less likely it is to be abused. But the precision of the CPNI exceptions with regard to the telephone networks was made possible by the confluence of several unique factors. Telephone networks support the national 911 first

[51] Again, it would enhance personal privacy to de-identify the buyer, not merely the vendor, from any buyer CPNI. But this is not strictly necessary to achieve the competitive purpose.

responder network, and several of the specific exceptions are directed specifically to facilitating operation of 911. Additionally, in the years prior to passing the Telecommunications Act of 1996 and incorporating CPNI into the Communications Act, Congress had passed the Communications Assistance to Law Enforcement Act (CALEA)[52] and the Electronic Communications Privacy Act (ECPA).[53] At the time, therefore, the responsibilities of telecommunications carriers for law enforcement were understood. As common carriers, telecommunications carriers complied with the procedures set forth in CALEA and ECPA, and otherwise were prohibited from denying service to anyone or interfering with their communications.

Common carriage also protected telecommunications carriers from liability for transactions conducted between customers, or from one customer using the telephone to harass or swindle another customer. As a "dumb pipe," the telecommunications carrier not only had no responsibility to protect subscribers from obscene phone calls or prescreen vendors for fraud, it literally had no legal ability to do so. Indeed, the one time Congress tried to make the telephone network the gatekeeper – by requiring telephone networks to prevent minors from calling "dial-a-porn" services – the Supreme Court found that this violated the First Amendment. As the Supreme Court explained, because the telephone network operated as a common carrier, the First Amendment right belonged to the speaker and listener on either end of the connection, and could not be regulated as a commercial practice of the telephone network.[54]

By contrast, the legal responsibilities of digital platforms remain in flux and subject to intense public policy debate. At the present time, some governments have required digital platforms to take certain actions regarding online transactions – particularly online content. The United States, and many other countries, rely on social and political pressure to moderate certain types of undesirable merchandising; protect consumers from counterfeit or dangerous products; or take other actions to protect users and behave "responsibly," with the threat of legislation if companies are not sufficiently responsive.

---

[52] Communications Assistance for Law Enforcement Act (CALEA), 47 U.S.C. §§ 1001–1010 (2012).
[53] Electronic Communications Privacy Act of 1986 (ECPA), Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2701-12, 3121-27).
[54] *See* Sable Communications of Cal., Inc. v. FCC, 492 U.S. 115 (1989).

As a result, it is unclear what uses of either vendor information or buyer information may be necessary to protect platforms or their users. Accordingly, at least initially, the exceptions for public safety and protection of platform users must be worded fairly broadly. Whenever exceptions are worded broadly, they invite abuse. In the future, it may be possible to narrow the language and have narrowly defined exceptions in the way that Section 222 has. But that is not possible today. To alleviate this difficulty, as discussed at length in *The Case for the Digital Platform Act*, Congress should delegate enforcement and rulemaking power to an agency, either an existing agency or a new agency with jurisdiction over digital platforms. Should the statute rely purely on enforcement through a private right of action, the courts must construe these exceptions within the overall purpose of the statute to promote competition by protecting customer proprietary information.

Protecting the rights of the platform includes not merely protecting the platform from direct harm, but also enabling the platform to conduct ordinary business practices to protect its rights – such as producing CPNI in litigation against a buyer or vendor to prove a claim or defend against one. The language of protection of rights should also enable the platform to carry on ordinary business practices such as billing, which are mentioned specifically in Section 222. The language should be broad enough to permit the platform to warn others – including those off the platform – of a vendor's or buyer's bad behavior (e.g., defaulting on payment, selling counterfeit goods), as well as to report suspicious activity or potential violation of law to relevant authorities.

ii: Use of Aggregate Information

The use of aggregate information traditionally means not merely anonymizing individual information so that it no longer links back to a specific, identifiable individual, but blending together the information of many individuals in aggregate form. This use derives from the Fair Information Privacy Principles (FIPPS) proposed in the 1973 report of the Department of Health, Education, and Welfare: *Records, Computers, and the Rights of Citizens*.[55] The exception for aggregate data reflects the diminished interest of the individual in the data once it has been both

[55] *See* U.S. DEP'T OF HEALTH, EDUC., AND WELFARE, RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS (July, 1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf [hereinafter *HEW Report*].

de-linked from the individual and blended with information of others, and the value to the record keeper and society as a whole of being able to use this data for a variety of purposes. As a consequence, an exception for aggregated data is contained not merely in the CPNI statute, but in other privacy statutes such as the Cable Privacy Act of 1984.[56]

It is reasonable to include an exception for aggregate information in the digital platform CPNI statute as well. This will allow the digital platform operator to engage in certain types of market research based on buyer and seller activity. But this sort of aggregated data analysis has not been considered unduly anticompetitive in the context of Section 222, and there does not seem to be any reason to consider it unduly anticompetitive here. Applying the requirement of blending data of multiple buyers and/or vendors with anonymization of the data with regard to specific transactions, specific buyers and specific vendors should provide sufficient protection while allowing the platform to derive value from its role in facilitating the transaction and processing the data.[57] For example, a retail platform like Etsy could use aggregate data to determine that certain types of products, such as pendants or hairpins, were becoming increasingly popular. But it would not allow Etsy to determine if a specific vendor's design was surging in popularity so that Etsy could copy it.

Because one of the primary benefits of permitting use of aggregate information is promoting scholarly research, the aggregate information exception should permit access to aggregated information by third parties. Because of First Amendment concerns, however, disclosure of the aggregated information cannot be restricted to academic researchers.[58] The statute can, however, impose a content neutral provision that before disclosing the aggregated CPNI to any third party, the platform must take reasonable steps to ensure that the third party cannot disaggregate the information, and subsequently re-link it to the original buyers and vendors.

To be clear, nothing in the statute would require a digital platform to make aggregate information available to third parties. The purpose of the exception is simply to permit digital platforms to continue the beneficial practice of making information available for academic

---

[56] Codified at 47 U.S.C. §551 (2018).
[57] *See HEW Report, supra* note 54.
[58] *See* Sorrell v. IMS Health, Inc., 564 U.S. 552 (2011).

research, in addition to whatever other profit-oriented research the digital platform may wish to pursue.

E: Enforcement

Statutory protections mean little without some enforcement mechanism. The FCC enforces Section 222 as part of its general responsibility to enforce the Communications Act. In addition, 47 U.S.C. §207 provides a private right of action for any actual damages. But the United States lacks an agency with express jurisdiction over digital platforms to delegate enforcement authority. Given this absence, Congress could simply create a civil penalty and leave enforcement to the Department of Justice. Alternatively, Congress could delegate power to the Federal Trade Commission or the Federal Communications Commission. In *The Case for the Digital Platform Act*, I discuss the advantages and disadvantages of each of these approaches.

Additionally, or alternatively, Congress could provide for private enforcement through a private right of action. Given that it is likely vendors who have the greatest incentive to vindicate their rights under the proposed statute, it makes a great deal of sense to allow vendors to pursue a private right of action similar to the private right of action permitted under the antitrust laws. The misuse of proprietary information should be regarded as a fairly straightforward harm conferring standing without the need to show additional lost sales or profits. In addition to recovery for actual provable damages, Congress should authorize triple damages (as under the antitrust laws) and attorneys' fees.

CONCLUSION

Over the last few years, the conversation around digital platforms has shifted from "is there a need for regulation" to "what regulation do we need." As noted in *The Case for the Digital Platform Act*, it took 20 years from the first tentative efforts to regulate radio and telephone service until the creation of the Communications Act of 1934. While we would hope that Congress will move considerably more quickly to create a comprehensive regulator for this increasingly important sector of the economy, we anticipate that it will not happen all at once. Although Public Knowledge has called for broader regulation of digital platforms to address a wide variety of competition and consumer protection concerns, we have also recognized that the first legislative steps will likely begin in a highly targeted fashion to address specific concerns.

The proposed draft platform Customer Proprietary Network Information statute is a simple and straightforward measure designed to address a well-documented concern in the digital platform space. This approach has a history of success in telecommunications networks. Properly adapted, it should work as either a stand-alone statute or as part of a broader set of policies designed to promote competition. The impact of the COVID-19 pandemic shifting increasing amounts of shopping online, and the rising concern that a handful of platforms are increasingly aggressive in their efforts to undermine competition, makes this proposal both extremely timely and important to implement.

Platform Customer Proprietary Network Information

(a) **General duty of digital platforms to protect customer proprietary information.** In addition to the specific responsibilities listed below, and in addition to any other obligations imposed by federal or state law, every digital platform must protect the proprietary information of any customer relating to the customer's use of the platform.

(b) **Obligation to protect vendor information, prohibition on using vendor proprietary information to compete.**
A digital platform, or the affiliate of a digital platform, that receives proprietary information from a vendor for the purpose of providing a specific service shall use that information only for such purpose. A digital platform may not use such information for its own marketing purposes, product development purposes, or use the information to otherwise gain advantage in competition with the vendor on or off the digital platform.

(c) **Specific responsibilities of digital platforms to protect buyer proprietary information.** Except as provided by law, a digital platform that receives or obtains proprietary information from a buyer for the purpose of facilitating a transaction with a vendor shall not use that information to:

(1) market competing products or services to the buyer;
(2) use the information to develop competing products or services;
(3) use the information to circumvent the limitations of Section (b);
(4) use the information to otherwise interfere with the buyer/vendor relationship.

(d) **Exception for search, recommendation and targeted advertising.**
Nothing in Section (c) shall prevent a digital platform from using buyer proprietary information in its search or recommendation functions, or in targeted advertising, *provided* that the digital platform does not use buyer CPNI to unfairly advantage its own products or services, or unfairly disadvantage vendors or advertisers.

(e) **Exceptions.**

(1) *Aggregate customer information*. A digital platform in possession of customer proprietary information as a consequence of facilitating a transaction between a buyer and a vendor (including information received from an affiliate of the digital platform for purpose of facilitating the transaction) may use, disclose or permit access to aggregate information, provided that, in the event access is provided to a third party, the digital platform shall take reasonable precautions to ensure that the information may not be disaggregated.

(2) *Protection of rights of digital platform, rights of digital platform users*. Nothing in this section shall prevent a digital platform from using or disclosing CPNI to:
   A. protect the rights and property of the digital platform, or the rights, property and safety of any user of the platform.
   B. Protect users of the digital platform, or other digital platforms, from fraudulent, abusive, or unlawful conduct.

C. As part of a process for sanctioning a vendor or buyer under a platform's terms of service, including as part of a defense against an accusation.
D. Bring to the attention of the appropriate authorities any evidence of suspected criminal activity or threat to the safety or well-being of others.
E. Comply with any law outside the jurisdiction of the United States.

(3) In regard to the exceptions given in (e)(2), the digital platform shall seek to minimize any unnecessary disclosure consistent with the duty imposed under (a).

Definitions. For purposes of this statute:

Aggregate customer information shall have the same meaning as that given by 47 U.S.C. §222(h)(2), except that "customer" shall have the meaning assigned by this section.

Buyer means a user of a digital platform that purchases goods or services from a vendor, subject to terms and conditions established by the platform.

Customer means either a buyer or a vendor.

Digital Platform means a service that—
(i) is accessed via the internet;
(ii) provides a two-sided or multi-sided market where at least one side is open to the general public and allows the public to produce and interact with content; and
(iii) permits users to:
(1) simultaneously engage in multiple activities on the platform;
(2) interact directly, or in a generally unmoderated manner, with other users of the platform;
(3) allows users to self-organize into open or closed groups where users have freedom to share information, goods or services with each other.

Proprietary Information shall have the same meaning as "confidential business information" in the Tariff Act of 1930, as set forth in 19 U.S.C. 1677f(b) and 19 C.F.R. 201.6(a).

Purchase means buy, rent, lease, or otherwise acquire, in exchange for any consideration, any good or service.

Vendor means a user of a digital platform that makes available, for a fee, goods or services to other users of the same platform, subject to terms and conditions established by the platform.