Antitrust Chronicle

JULY · SUMMER 2022 · VOLUME 2(2)

Platforms: Value Creation and Potential Harms

CPI COMPETITION POLICY™ INTERNATIONAL

TABLE OF CONTENTS

LETTER FROM THE EDITOR

Dear Readers,

The practice of antitrust law is essentially an exercise in tradeoffs. How does a given practice by businesses benefit consumers? And how does it potentially harm them? Some practices are unambiguous: cartels, for example, produce no conceivable consumer benefit (and depress the economy as a whole). Other practices (particularly involving potential abuses of dominance) involve a more complex analysis of the inherent tradeoffs involved. This is all the more true as the economy becomes increasingly complex (particularly as regards digital markets, and platform businesses). The pieces in this Chronicle analyze the increasingly difficult question of how these tradeoffs should be addressed, with a focus on the digital economy.

Carmelo Cennamo & Juan Santaló begin by setting out the tradeoffs addressed by the EU Digital Markets Act. This piece of legislation makes clear certain choices about important tradeoffs in value to constrain the arbitrary power and dominance of gatekeepers over digital markets and guarantee a more equitable distribution of value with business users. The piece argues that the extent to which those objectives will be realized depend largely on the nature of competition one favors: both the type of competition (within vs. across platform) and the competition dynamics (winner-takes-all vs. differentiation).

Catherine Tucker addresses how platforms create value through a process known as "coring." Coring refers to steps a digital platform takes to make sure that interactions between different user groups go well, and that as a consequence they wish to return to the platform and use it again. Platforms typically therefore take on a governance role and actively manage interactions between different user groups. The piece discusses two implications of this concept for competition economics: Market definition and the recent Supreme Court Decision in Amex.

Ariel Ezrachi & Maurice E. Stucke discuss how Silicon Valley's concentration of talent, combined with limited regulation, promised a new age of technological innovation in which entrepreneurs would fuel unprecedented job growth, improve overall wellbeing, and address pressing issues. Rather than accepting this narrative, the authors discuss how, instead, in their view,, the leading tech companies design their sprawling ecosystems to extract value (often at the expense of individuals and business users), while crushing entrepreneurs that pose a threat. This essay highlights several important themes from their new book, *How Big-Tech Barons Smash Innovation and How to Strike Back*.

Similarly, **Alexander Raskovich & John M. Yun** discuss the economic principle that "there is no such thing as a free lunch." More formally, any benefit must come at some cost; economic resources must be expended, and someone will have to cover those expenditures. The authors discuss how this principle explains the harms that this principle imposes on society, in particular with respect to the digital economy. **Sean F. Ennis** strikes a similar note, observing that unfair competition may occur if a competitive outcome is influenced my misled expectations, notably if the company that wins the competition either misled consumers or did not affirmatively correct consumer expectations that were incorrect. The ability to exploit customers whose expectations have been misled is particularly strong for networks that have "tipped."

Marco Iansiti et al explore how digital recommender systems provide consumers with recommendations across a variety of contexts. While recommender systems generate efficiencies by lowering the cost and improving the quality of product discovery, their impact on individuals' purchases and consumption has the potential of affecting downstream competition of products and industries. These systems may also present sensitive issues for national security, democracy, and public health. Recommender systems have therefore come under increasing scrutiny from governments around the world in recent years.

Sarit Markovich & Yaron Yehezkel turn to the increasingly important issue of data. Many platforms base their business model on the commercialization of their users' data. For example, search engines, navigation apps, media streaming platforms, and wearables, such as all base their business models, to varying degrees, on collecting data on users' activities and preferences. These platforms can then use the data to improve their services, but at the same time, the data can also be used for commercial purposes such as selling it to advertisers or to other third-party providers. This raises the question of who should own the property rights over users' data? Specifically, who should have the right to decide which data items to collect and which to commercialize?

On a related note, **Mikołaj Barczentewicz** explores how the EU Digital Markets Act purports to benefit consumers and improve the competitiveness of digital markets, concluding that it is likely to have negative and The pieces focuses on the DMA's interoperability mandates. Only one of those obligations — on the interoperability of messaging services — is accompanied by a potentially adequate safeguard: a requirement that any third-party service must offer at least the same level of user security as the original service. This is a very demanding standard, which may render the interoperability provision a dead letter for the foreseeable future.

Finally, **Rosa Abrantes-Metz & Mame Maloney** analyze the competitive interplay of prices among retail channels: offline (brick-and-mortar) and online (such as retailers' websites and online marketplaces). Their empirical analysis draws from two data sources: a novel hand-collected price dataset, and a national aggregate scanner dataset. The piece finds evidence of a close competitive relationship between the online and offline channels, and that prices in one channel are highly responsive to changes in the other's channel's prices.

In sum, the pieces in this Chronicle provide an overview of the increasingly complex calculus facing antitrust policymakers in today's ever-developing environment.

As always, many thanks to our great panel of authors.

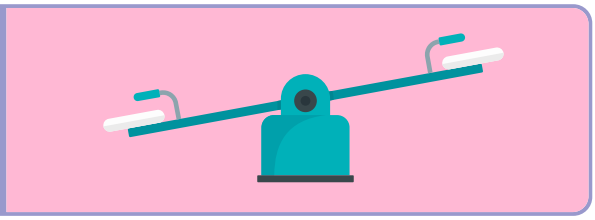
Sincerely,

CPI Team[1]

1 CPI thanks CCIA for their sponsorship of this issue of the Antitrust Chronicle. Sponsoring an issue of the Chronicle entails the suggestion of a specific topic or theme for discussion in a given publication. CPI determines whether the suggestion merits a dedicated conversation, as is the case with the current issue of the Chronicle. As always, CPI takes steps to ensure that the viewpoints relevant to a balanced debate are invited to participate and that the quality of our content maintains our high standards.

SUMMARIES

09



VALUE IN DIGITAL PLATFORMS: THE CHOICE OF TRADEOFFS IN THE DIGITAL MARKETS ACT

By Carmelo Cennamo & Juan Santaló

The Digital Markets Act makes clear choices about important tradeoffs in value to constrain the arbitrary power and dominance of gatekeepers over digital markets and guarantee a more equitable distribution of value with business users. We argue that the extent those objectives will be realized depend largely on the nature of competition, both the type of competition (within vs. across platforms) and the competition dynamics (Winner-Take-All vs. differentiation). We anticipate that the choices about the tradeoffs in value taken in the DMA will prevent gatekeepers to monopolize the focal market but in very limited cases. This is because the DMA seems to protect specific competitors (some large business users against gatekeepers) rather than competition, as well as protecting only one type of competition (*within* platform) instead of also, and the more salient for contestability in digital markets, *cross* platform competition. We discuss these tradeoffs and the implications for competition, value distribution and welfare.

16

HOW PLATFORMS CREATE VALUE THROUGH CORING AND IMPLICATIONS FOR MARKET DEFINITION

By Catherine Tucker

In business school, we teach that platforms create value through coring. Coring is the steps a digital platform takes to make sure that interactions between different user groups go well, and that as a consequence they wish to return to the platform and use it again. As such, platforms typically take on a governance role and actively manage interactions between different user groups. This article discusses two implications of this business school concept for competition economics: Market definition and the recent Supreme Court Decision for Amex.

20

TOXIC INNOVATION IN THE DIGITAL ECONOMY

By Ariel Ezrachi & Maurice E. Stucke

Silicon Valley's genius combined with limited regulation promised a new age of technological innovation in which entrepreneurs would fuel unprecedented job growth, improve overall well-being, and address pressing issues. Instead, the leading tech companies design their sprawling ecosystems to extract value (often at the expense of individuals and business users), while crushing entrepreneurs that pose a threat. As a result, we get less disruptive innovation that actually benefits us and more innovations that surpass the dreams of yesteryears' autocracies. This essay highlights several important themes from our new book, How Big-Tech Barons Smash Innovation and How to Strike Back which examines and debunks the self-serving ideological platter that the Tech Barons serve, in depicting themselves as the engines of innovation in the digital economy.

25

RECOMMENDER SYSTEMS: APPROACHES TO SHAPE A SAFE, COMPETITIVE, AND INNOVATION-DRIVEN FUTURE

By Marco Iansiti, Rohit Chatterjee, Bartley Tablante, Sean Durkin, Anurag Gandhi & Abby Drokhlyansky

In most digital platforms recommender systems provide consumers with recommendations across a variety of contexts. While recommender systems generate efficiencies by lowering the cost and improving the quality of product discovery, their impact on individuals' purchase and consumption has the potential of affecting downstream competition of products and industries. These systems may also present sensitive issues for national security, democracy, and public health. Recommender systems have therefore come under increasing scrutiny from governments around the world in recent years. The scale of efficiencies and benefits offered by recommender systems motivates their continued use and expansion in the future. In this paper we explore approaches that merge innovation and regulation as part of technological advancement. We offer an approach built on increased transparency on the side of companies regarding both their data and algorithms, as well as through collaborations between digital platforms, academics, and regulators. By taking responsibility for regulating their recommender systems in the short-term, companies will be well-positioned to reap long-term benefits and to serve as leaders in the ecosystem. Improved regulation and monitoring by external bodies will also help cultivate the market. With digital regulations of these systems still being in a relatively nascent stage adopting these types of approaches can help shape a safe, competitive, and innovation-driven future.

SUMMARIES

32

ZERO-PRICE PLATFORM SERVICES: THERE IS NO FREE LUNCH IN APPLYING THE "NO FREE LUNCH" PRINCIPLE

By Alexander Raskovich & John M. Yun

The well-known economic principle that "there is no such thing as a free lunch" ("NFLP") has enjoyed a recent revival in the assessment of digital markets in antitrust. There is a belief that NFLP implies zero-price platform services must somehow be "paid for" by consumers in some manner—such as the loss of privacy and valuable data. Others have gone further, asserting that consumers are not only made worse off by the data collection and use that attend zero-price platform services, but that this state of affairs necessarily points to a lack of competitive alternatives. Both assertions are invalid, pressing the NFLP beyond the limits of logical inference. Inferences about who pays resource costs, and whether those payments reflect market power, are empirical questions as illuminated by other economic principles. Answers to such critical questions cannot be plucked from an NFLP magic hat. The NFLP is the truism that, at the margin, any benefit must come at some cost; economic resources must be expended, and *someone* will have to cover those expenditures. But the NFLP does not, without more, specify *who* bears the costs. The potential error here is a subtle one, but with profound consequences. It is wrong to conflate the resource costs required to provide a service with the effective price paid by those receiving the service. The NFLP does not imply the two must be equal.

37

"FOR THE PUBLIC BENEFIT": WHO SHOULD CONTROL OUR DATA?

By Sarit Markovich & Yaron Yehezkel

Data-driven platforms collect and commercialize users' data through advertisements or by selling the data to other third part providers. This practice raises the question of who should have the right to decide which data to collect and commercialize, users or the platform? In this article, we describe the results of our research concerning regulating platforms' data collection. The main feature of our research is the distinction between the user's private benefit from data and the data's public benefit—i.e., the benefit a user's data provide to other users on the platform, regardless of whether they are sharing their data. We find that when users differ in their disutility from the commercialization of their data and the public benefit of data is high (low), it is welfare enhancing to let the platform (users) control the data. In contrast, when heterogeneity is in the disutility from the commercialization of different data items, it is welfare enhancing to let users (the platform) control the data when the public benefit of data is high (low). Furthermore, we find that an entrant platform may choose to give users control over their data as doing so can help it overcome the advantage the incumbent enjoys.

43

MINIMIZING PRIVACY RISKS IN REGULATING DIGITAL PLATFORMS: INTEROPERABILITY IN THE EU DMA

By Mikołaj Barczentewicz

The EU Digital Markets Act purports to benefit consumers and improve the competitiveness of digital markets. It is likely to have negative and unaddressed consequences, however, in terms of information privacy and security. I illustrate this by focusing on the DMA's interoperability mandates. Only one of those obligations — on the interoperability of messaging services — is accompanied by a potentially adequate safeguard: a requirement that any third-party service must offer at least the same level of user security as the original service. This is a very demanding standard, which may render the interoperability provision a dead letter for the foreseeable future, but which nonetheless offers welcome privacy benefits from the consumer perspective. The remaining obligations that I analyze are accompanied either by no safeguards, or by insufficient safeguards.

51

COMPETITIVE DYNAMICS OF ONLINE AND BRICK-AND-MORTAR RETAIL PRICES

By Rosa Abrantes-Metz & Mame Maloney

This article analyzes the competitive interplay of prices among retail channels: offline (brick-and-mortar) and online (such as retailers' websites and online marketplaces). Our empirical analysis draws from two data sources: a novel hand-collected price dataset, and a national aggregate scanner dataset. We find evidence of a close competitive relationship between the online and offline channels, and that prices in one channel are highly responsive to changes in the other channel's prices. Based on time series analyses, we find that online prices are more responsive to brick-and-mortar prices than the reverse, as well as evidence of asymmetric responses depending on which channel's price is higher. Our findings suggest that consumers online face almost identical pricing to consumers offline. Of relevance for competition and regulation, our findings suggest that competition among retail goods is vigorous, that these respond quickly to each other's prices and that, as a consequence, regulation affecting online commerce would be expected to affect prices in brick-and-mortar stores, and *vice versa.*

SUMMARIES

63

CONSUMER EXPECTATIONS AND FAIR CONTRACTING FOR DIGITAL PRODUCTS

By Sean F. Ennis

The formation of consumer expectations for digital products affects competition between digital platforms that offer competing products. Unfair competition may occur if the competitive outcome is influenced my misled expectations, notably if the company that wins the competition either misled consumers or did not affirmatively correct consumer expectations that were incorrect. The ability to exploit customers whose expectations have been misled is particularly strong for networks that have tipped, as outside alternatives for dissatisfied consumers may no longer be realistic or viable alternatives for consumers. Unilateral deviations by a company's product away from the future product expectations that have been created around their products may be unfair and create anti-competitive outcomes in growing digital markets.

WHAT'S NEXT?

For August 2022, we will feature an Antitrust Chronicle focused on issues related to (1) **EAB Antipasto**; and (2) **State AGs**.

ANNOUNCEMENTS

CPI wants to hear from our subscribers. In 2022, we will be reaching out to members of our community for your feedback and ideas. Let us know what you want (or don't want) to see, at: antitrustchronicle@competitionpolicyinternational.com.

CPI ANTITRUST CHRONICLES September 2022

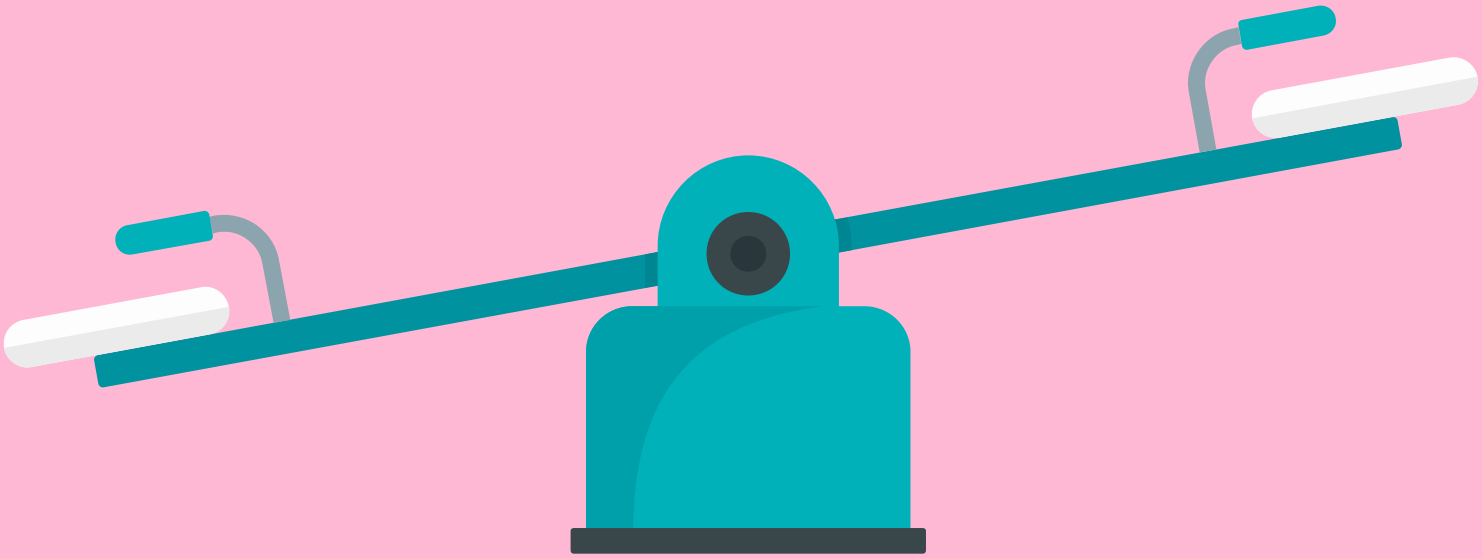
For September 2022, we will feature an Antitrust Chronicle focused on issues related to (1) **Cartels**; and (2) **Vertical Agreements**.

Contributions to the Antitrust Chronicle are about 2,500 – 4,000 words long. They should be lightly cited and not be written as long law-review articles with many in-depth footnotes. As with all CPI publications, articles for the CPI Antitrust Chronicle should be written clearly and with the reader always in mind.

Interested authors should send their contributions to Sam Sadden (ssadden@competitionpolicyinternational.com) with the subject line "Antitrust Chronicle," a short bio and picture(s) of the author(s).

The CPI Editorial Team will evaluate all submissions and will publish the best papers. Authors can submit papers on any topic related to competition and regulation, however, priority will be given to articles addressing the abovementioned topics. Co-authors are always welcome.

VALUE IN DIGITAL PLATFORMS: THE CHOICE OF TRADEOFFS IN THE DIGITAL MARKETS ACT



BY CARMELO CENNAMO & JUAN SANTALÓ[1]

1 Copenhagen Business School & SDA Bocconi School of Management / IE University, respectively. The subject we cover in this article is highly controversial, can be approached from different analytical angles as well as viewpoints depending on the vested interests one would consider, so that the ones we take here and the conclusions we arrive at can easily run counter to commonly held opinions. We are very wary of the difficulties of the task at hand; and we have no presumption that our approach and logic is superior to the alternatives, let alone that our conclusions are correct. We are only confident of one thing: the problem we are engaging with has not been sufficiently recognized and is such that requires deep engagement from multiple viewpoints to develop knowledge about.

I. INTRODUCTION

The Digital Markets Act ("DMA") introduces new regulations to limit business strategy discretion of "gatekeepers" – i.e. large, dominant digital platforms acting as intermediaries of core digital services that control main gateways to markets[2] – with the aim of guaranteeing more equitable distribution of value between the gatekeeper and its business users - to what the DMA refers to as "fairness." Also, a number of obligations are introduced to avoid that gatekeepers block potential direct competition from business users, which would then limit market contestability in the digital space.

Broadly, we can group the most relevant obligations in three categories. First, the DMA introduces obligations for gatekeepers with regards to data sharing. Specifically, the DMA requires both user data portability and free of charge access to gatekeeper data linked to business users. Second, another set of obligations revolve around the issue of privacy and data aggregation. The DMA requires explicit consent by end users to combine personal data from different services offered by and via the gatekeeper's platform. Finally, a number of obligations are set to counter power imbalance of business users with the gatekeeper and establish "fairness" in digital markets. Among other things, the DMA forbids favoring the gatekeeper's own products over those of business users in the ranking services; forbids the so-called price coherence (also known as "most favored nation") clause according to which the platform provider requires third parties not to sell their products in other channels at a price below the one set on the digital platform; it forces transparency in advertising conditions and it does not allow gatekeepers to use data not publicly available to compete with business users in its platform marketplace; and it also forbids the enforcement of in app payment systems as unique way to handle the transaction with the end user.

The long and detailed list of prescriptions and prohibitions would suggest that regulators drafting the DMA have performed a careful analysis of the kind of tradeoffs between guaranteeing greater creation of value for end users (and overall for the digital economy) and more equitable distribution of value between gatekeepers and business users, and selected accordingly the aspects to prioritize. This choice, and the overall regulatory architecture is argued to be set for the greater good, benefiting business users at large by rebalancing the power asymmetry with the platform provider, and elevating competition and innovation in digital markets. In fact, as also emerging from related debate around the drafting of the DMA, many would advance that there are no tradeoffs; in the long term, (the expected greater) dynamic competition will bring benefits that compensate for any potential loss in efficiencies in the short term that these restrictions might cause. Eventually, this logic goes, end users, because of the new competitive context, are also expected to benefit in terms of more, innovative, and better services.

Will this be a natural course of events? How will platform providers' incentives be affected by this regulatory-induced shift in value creation-distribution dynamics? What are the ripple effects on the overall ecosystem of business users relying on platforms' services to produce their own offerings? While the DMA puts business users all in one bucket, there is ample heterogeneity among them: the specific choice of settling the value tradeoffs in the DMA will likely produce positive outcomes for *some* business users but can also disrupt the value creation or competitiveness capacity of other business users, as well as the capacity of some of the current gatekeepers to challenge other gatekeepers' dominant position in a core service on the ground of a different business model and platform core service design.[3] The latter, that is, *cross*-platform competition, is the most vibrant form of competition in digital markets that can establish some contestability of gatekeepers' dominant position. Yet, the DMA largely ignores this type of competition and rather focuses on *within* platform competition, that is, competition among business users on the platform and among business users and the gatekeeper itself.

We believe that this choice does set important tradeoffs in terms of competition and value that the DMA can help attain, which can not only potentially produce unintended consequences in terms of value loss for some business users; it can also determine by design winners and losers. If competition policy should not be about protecting some competitors against others but about competition itself and overall welfare, then the value tradeoffs' choices taken in the DMA might set the law on a wrong path. Assessing more systematically these tradeoffs and their implications is thus important particularly for the implementation criteria of the DMA to avoid introducing *de jure* distortions on the market based upon a normative stance against few specific, albeit powerful companies in the market.

We propose two key dimensions for determining the nature of these tradeoffs as well as the identity of winners and losers. The first

2 See article 3 of the Digital Markets Act, "designation of gatekeepers" recital.

3 Large platforms often expand their core service activity into adjacent markets by adding additional features and ancillary services, a practice called "platform envelopment," which challenges the competitive position of smaller planforms specializing in that market vertical (see Eisenmann T., Parker G., Van Alstyne M. (2011). "Platform envelopment," Strategic Management Journal 32: 1270-1285). Visnjic and Cennamo document how, over the years, Amazon, Apple, Google and Meta have engaged in multiple envelopment and counter-envelopment moves, which led to greater market overlap and competition among these players in ever redefining competitive landscape, a new context which they refer to as "supra-platform market" competition (Visnjic, I., Cennamo, C. (2013). "The Gang of Four: Acquaintances, Friends or Foes? Towards an Integrated Perspective on Platform Competition." ESADE Business School Research Paper No. 245, Available at SSRN: https://ssrn.com/abstract=2264869.

dimension refers to the competition type: whether the relevant type of competition is *within* the platform market versus competition *across* platform markets. The second dimension refers to the underlying nature of network effects that determine the competition dynamics: whether the market follows *winner-take-all ("WTA")* competitive dynamics, or whether it allows for the coexistence of competing platforms that compete for users (business- and end-users) based on distinctiveness, i.e. differentiated platform technology design and market structuring and positioning (*differentiation*).[4]

II. TRADE-OFFS IN THE DMA

We identify three relevant trade-offs that implicitly or explicitly the DMA's provisions summarized above map into:

A. Data Sharing and Interoperability vs. Platform Innovation.

Companies are able to use data to better personalize their services and better target distinct consumer segments creating new bundles of products or services. However, there is a non-negligible cost of collecting and processing the data into the appropriate format needed to generate knowledge that inspires these new services and products. Although raw digital records can be stored at very little cost, data accumulation only leads to new products or services when companies invest substantial resources in formatting these records into inputs that can create new insights and knowledge. Data sharing and portability requirements means that competitors can benefit from the same data-generated knowledge without incurring the data creation and processing costs. This automatically creates a free riding problem that diminishes firm incentives to invest in the creation and processing of the data needed to sustain business users' activity and potentially innovation from the gatekeeper (to the extent it cannot properly appropriate value from this innovation).

How big a problem this can be depends on the relevant competition type and dynamics. Generating, accessing and processing data are in fact vital activities to improve existing interactions (i.e. simple business transactions), but also create new interactions either by unlocking latent interactions (i.e. facilitated by demand aggregation) or by enabling novel interactions (i.e. searching or ratings).[5] Particularly for the enabling of novel interactions, the design of the platform digital infrastructure and tools for generating, aggregating and processing data in specific ways become a relevant area of innovation as well as differentiation of the digital platform and the benefits and customer experience it provides.

Accordingly, in the case in which competition *across* platforms is based on differentiation rather than WTA, a platform's infrastructures for data structuring and processing are critical levers to create differentiation and compete for different customer journey and experience based on different interactions. Imposing data sharing and interoperability across platforms would be bad in the case of markets in which platforms compete on the basis of differentiation since it will reduce this critical source of differentiation and kill the incentives (if not the capacity) for cross-platform competition. Data being created will become increasingly a shared asset and public good, with the usual incentives' problems for high-quality and innovation contribution these triggers; overall innovation and quality might degrade.[6]

A similar point is made elsewhere,[7] whereby the authors make the distinction between vertical (within platform in our parlance) vs. horizontal (cross platforms in our parlance) interoperability, with the latter having the downside of reduced possibilities of differentiation, hence limiting the incentives to invest in differentiated core services to compete *for the* market. As a result, despite data interoperability, we might have a context of ossified cross-platform competition, whereby the large, dominant platform may remain the default option for end users for the core service, and thus retain its dominant position.

When considering the tradeoff from the within platform competition perspective though, data sharing and interoperability between the platform provider and business users can likely stimulate innovation spillovers as well as more (within platform) competition. The platform provider can indirectly capture value from this greater share of activity/interactions within the digital platform. Therefore, incentives for upgrading the infrastructure for data creation and sharing can be preserved, within platform competition boosted, and novel interactions and innovation enhanced eventually. A win-win situation might emerge.

---

4 An analysis of such competition dynamics and the related platform market cases is offered in Cennamo C. "Competing in digital markets: A platform-based perspective." (2021) Academy of Management Perspectives 35(2): 265-291. Also available at https://ssrn.com/abstract=3410982.

5 See Cennamo C., Kretschmer T., "Business model agnostic? An innovation-centric view of the DMA." Working paper.

6 See e.g. Cennamo C., & Santaló J. "Generativity tension and value creation in platform ecosystems" (2019) Organization Science 30(3): 617-641. https://doi.org/10.1287/orsc.2018.1270.

7 Bourreau M., Kramer J., Buiten M. (2022). "Interoperability in digital markets." CERRE report: https://cerre.eu/publications/interoperability-in-digital-markets/.

B. Privacy vs. Competition

The more companies have access to detailed individual data, the more companies can offer targeted/personalized services generating value and vibrant within platform competition at the cost of privacy risks. Regulatory constraints on data usage designed to preserve privacy may thus imply less intense competition in the marketplace.

When considering *within* platform competition, more privacy implies a higher burden for smaller providers in accessing relevant data and information about users, which are critical not only to target them but also to build customized offerings. End users tend to trust large providers[8] when it comes to give their consent to use and combine data about their profile and activities. Accordingly, smaller providers with relatively less established brand compared to large providers are penalized. To the extent that access to end user data is instrumental to product/service design and value proposition, smaller and novel providers will be at competitive disadvantage. This implies a competitive asymmetry and a reduced overall competition activity level within platform, which will likely result in greater concentration among large players within platforms. Privacy enforcement might thus risk of being anticompetitive for within platform market competition, and, in fact, unfair to the extent that affects negatively smaller versus larger business users.

When considering competition across platforms, the effect can be positive (i.e. pro-competitive) to the extent that platforms compete for the same core service and competition is of the WTA type but with an asymmetric size (i.e. a smaller platform challenging the big one). In these conditions, absent the privacy restraint, the large platform may enjoy a data advantage from combining end user data across multiple services and leverage it to outcompete the smaller platform. If the big platform cannot use and combine data from the multiple services it offers unless granted consent by the end user, then smaller, specialized platforms offering just the core service will not suffer a "data disadvantage" and can potentially challenge the big platform on the merit of the quality of the service. There is a proviso though, as shown by studies on the effects of GDPR: end users may do grant consent to the bigger but not the smaller, less known platform. The pro-competitive effect of the privacy obligation will thus be greatly diluted.

In the case though that competition is not WTA but based on differentiation, restriction on privacy would likely reduce competition *across* platforms by constraining the opportunities for differentiation based on distinct ways of offering personalized services. Also, when degrees of freedom are allowed on whether and how platforms can handle user data for their offerings, to the extent this is made transparent to end users and thus can enter as an additional element in their decisional choice set, the differentiation nature of competition would also imply a possible competitive equilibrium of differentiation based upon privacy provision, whereby one(some) platform(s) may offer maximum privacy protection while another(s) can offer less privacy but cheaper service. This type of differentiation based on end users' preferences about privacy may enhance overall competition in the market across platforms.

C. Business Fairness vs. Consumer Welfare

Business fairness stresses the importance of preserving (*within* platform) competition per se, regardless of its effects on consumer surplus. Ex-ante obligations in the DMA to guarantee business fairness would inevitably apply uniformly to different digital platform cases and contexts independently of whether the targeted practice has benefits for consumers. We might then have cases in which this standardized treatment towards any product and service from platform's business users may lead to decreases in consumer welfare either through decreases in value creation capacity at the platform ecosystem level or through increases in transaction costs (i.e. decreases in selection and transaction efficiencies of the platform).

Consider the case of self-preferencing, the restraint imposed on gatekeepers to promote and favor their own products and services on their platform infrastructures (against third-party providers). Though the DMA connotates self-preferencing almost in and by itself as a theory of harm to business and end users, many of these activities are implemented not just for the gatekeeper to capture greater value (against business users) but to unlock value and benefits for end-users. Self-preferencing may bring benefits in terms of efficiency gains proceeding either from reduced transaction costs for the end user and/or from enhanced competition for services among business users (to the extent that business users can compete on equal foot with the platform provider).[9] For instance, Amazon Prime increases the benefits from the existing interactions for the end-user who can experience lower transaction costs from engaging in the relationship with an Amazon Prime business user than with

8 See e.g. recent work by Peukert C., Bechtold S., Batikas M. & Kretschmer T. "Regulatory spillovers and data governance: Evidence from the GDPR" (2022) Marketing Science, forthcoming. https://pubsonline.informs.org/doi/10.1287/mksc.2021.1339.

9 See e.g. Hagiu A., Teh T-H. & Wright J. "Should Platforms Be Allowed to Sell on Their Own Marketplaces?" (2020) RAND Journal of Economics forthcoming, Available at https://ssrn.com/abstract=3606055.

business users that are not part of the Amazon Prime program. Similarly, an ancillary service such as Apple Pay adds to existing interactions between business users and end users using Apple platforms by further reducing the transaction costs related to the interaction.[10] In such cases, *within* platform competition might in fact increase,[11] unlocking greater efficiencies and heterogeneity of offerings, both of which enhance consumer welfare.

Business fairness may indeed go hand in hand with enhanced consumer surplus when the fairness restrictions prevent a WTA result in which the gatekeeper gets to dominate a new market. Hence, in those cases, business fairness prevents monopolization that may decrease consumer surplus. However, for non-WTA markets, the tradeoff between fair competition and consumer surplus may indeed become relevant. If the gatekeeper is the most efficient competitor, fair competition measures may decrease consumer surplus at the benefit of less efficient competitors.

Consider again the case of Amazon Prime (and the potential self-preferencing effect). If the logistic and fulfillment services offered by Amazon to Prime sellers is a way to improve market interactions and consumption experience, and by its means differentiate the core service from other platform marketplaces (such as e.g. eBay), promoting Prime sellers is the way for Amazon to deliver on its key value proposition. While this might be perceived as anticompetitive from a *within* market competition perspective between prime sellers vs. non-prime sellers, it is pro-competitive from a cross market competition perspective as it allows greater service differentiation and the creation of novel and different type of market interactions between end and business users.

The legal constraints on data sharing imposed to Google acquisition of Fitbit in 2020 and its implications on the recent launch of the new Google Pixel watch also illustrate this point clearly. As a result of the 2020 agreement with the European Commission, Fitbit and Google data must remain private and separate[12]. This implies that any health data collected on the new Pixel Watch will remain under Fitbit's control, separate from Google's. Hence, it seems Pixel users will need to keep two different accounts, one for their general watch and one for the fitness component. This lack of integration harms user experience and more generally consumer welfare. Furthermore, although this measure may indeed help Pixel competitors like Samsung, Garmin or Xiaomi to compete against Google Pixel, it may severely hamper the competitive stand against the Apple watch that indeed offers a full integration between health data and the rest. Competition across platforms can be thus hampered as a result.

III. WINNERS AND LOSERS OF THE DMA CHOICES

A. Amazon Winning Over the Shopify-Meta duo (Alternative Platform Market)

We can identify some likely winners and losers of the DMA choices in relation to the tradeoffs discussed above. Paradoxically, given how this regulation has been publicized as against Big Tech, Amazon can be the real winner of these DMA choices, specifically in relation to the first and second tradeoff (though its business might suffer negative repercussions from the third tradeoff). This can be better understood if we take the perspective of competition *across* platforms rather than competition within platforms. From this perspective, small and medium size businesses that want to use ecommerce to sell their offerings have two broad choices. They can use the Amazon platform to reach a massive worldwide audience, using Amazon's search algorithm to gain relatively good consumer exposure or advertise within the Amazon marketplace itself. Alternatively, small and medium size enterprises, SMEs, could use the standardized ecommerce tools provided by Shopify to establish direct-to-consumer online business and sell directly through their own webpage. The benefit of this second option is that they avoid the commoditization generated by the Amazon search algorithm. The cons are that SMEs face the challenge of building an audience for their product offerings.

Companies using the direct route and bypassing Amazon have often built this audience resorting to the (relatively cheap) targeted advertisement service provided by Meta's Facebook platform. With a high level of efficacy, Meta advertisement has allowed SMEs to get in touch with a worldwide audience potentially interested in small niche products. Hence, even if Amazon and Shopify do not seem to overlap in any product market or service, and thus compete for a core service, when we consider the big go-to-market choices of SMEs, then the Shopify/Meta tandem is an Amazon's competitor indeed, being it a viable alternative to the Amazon marketplace. The recent experience of the App Tracking Transparency, ATT, implemented by Apple in September 2020, has proven how privacy driven restrictions in the way consumer data can be tracked and shared across multiple apps has benefited the Amazon ecosystem at the expense of the Shopify-Meta ecosystem, diluting the latter's capacity to compete with Amazon.

10 See Cennamo, Kretschmer, Constantinides, Alaimo & Santaló (2022), cited supra, for a comprehensive analysis of the contingent positive and negative effects of self-preferencing.

11 Hagiu, Teh & Wright (2020), cited *supra.*

12 https://www.theverge.com/2022/5/11/23064072/google-pixel-watch-fitbit-io-2022.

Consumers massively choosing not to be tracked because of the ATT final implementation have disrupted the results of all companies that relied on targeted advertising to reach consumer audiences[13]. Meta estimates a cost of $10 billion in lost revenue entirely driven by Apple ATT.[14] Shopify's stock market value recently crashed 15 percent when disclosing first quarter losses of $1 billion.[15] Snap suffered a drop of more than 25 percent in its stock market value after reporting lower growth expectation as a result of the Apple ATT rules.[16] On the winning side, Amazon disclosed for the first time it obtains $9.7 billion revenue in advertising.[17] Due to the lack of past disclosure data, we cannot assess whether there has been any increase driven by Apple ATT rules, but it looks premonitory that just now, in the middle of these seismic changes in online advertising, Amazon has chosen for the first time to disclose separately its advertising revenue.

B. Large Content Fortresses Winning at the Expense of Companies with Smaller User Base

As the ATT has also shown, these explicit tradeoff choices in the DMA benefit companies that have direct access to user data without the need to port or aggregate any data coming from a variety of sources. Other than Amazon, companies like Apple or Netflix can use this so-called content fortress to sell advertising with a return on investment, ROI, that can be unmatched by companies with a smaller user base. In other words, since ATT *de facto* implies consumer behavior cannot be tracked across apps, apps that have a larger user base can indeed better monitor consumer behavior and offer targeted advertising with a higher ROI than apps with a smaller user base. Overall, this generates asymmetric effects of competition reinforcing the competitive advantage of big players (with direct access to consumer's data) at the expense of smaller ones. This may, in fact, ossify cross-platform competition by consolidating the dominant position of established platforms in their own verticals instead of making digital markets more contestable.

C. Traditional Advertising Winning at the Expense of Targeted Advertising

Given how the efficacy of targeted advertising could be diminished by the DMA's data restrictions, other unexpected winners of the DMA are going to be all suppliers of more traditional mass advertising like TV stations and newspapers that should experience a surge in demand of this type of advertising that comes from (large) advertisers abandoning targeted advertising channels. More generally, large companies that have the scale to invest in massive advertising are going to benefit from the DMA inserting sticks in the wheels on the efficacy of targeted advertising at the expense of small business users that will have to increase marketing costs (and duplicate it for each vertical channel) to reach out to the same audience. In fact, small direct-to-consumer companies can experience important increases in marketing costs.

IV. CLOSING REMARKS

The DMA is making clear choices about important tradeoffs in value. While the intended objectives are to constrain the arbitrary power and dominance over digital markets of gatekeepers and guarantee a more equitable distribution of value with business users, the extent those objectives will be realized depend largely on the nature of competition, both the type (within vs. across) and dynamics (WTA vs. differentiation). The DMA seems to be agnostic about both dimensions, implicitly assuming that competition dynamics are always of the WTA type in all digital markets, and focusing only on within platform market competition. We are afraid this is too a restrictive focus, one which fails to account for important potential negative consequences that the current restrictions may have for fostering competition across platforms and enhancing not just the variety of services being offered via the platform but the innovation in and variety of alternative digital marketplaces (and customer journey) for such services.

We anticipate that the choices about the tradeoffs in value taken in the DMA will prevent gatekeepers to monopolize the focal market but in very limited cases. This is because the DMA seems to protect specific competitors (some large business users against gatekeepers) rather than competition, as well as protecting only one type of competition (*within* platform) instead of also, and the more salient for contestability in digital markets, *cross* platform competition.

13 For details and analysis of the potential anticompetitive effects of Apple's ATT practice see e.g. Sokol D., Zhu F. "Harming competition and consumers under the guise of protecting privacy: An analysis of Apple's iOS 14 policy updates" (2021) Working Paper available at https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3852744.

14 See Newman D. "Apple, Meta and the $10 billion impact of privacy changes" (2022), Forbes.com: https://www.forbes.com/sites/danielnewman/2022/02/10/apple-meta-and-the-ten-billion-dollar-impact-of-privacy-changes/.

15 See Kindig B. "Shopify stock hit by plethora of headwinds in Q1" (2022), Forbes.com: https://www.forbes.com/sites/bethkindig/2022/05/05/shopify-stock-hit-by-plethora-of-headwinds-in-q1/.

16 See Dang S. "Snap shares plunge 25% as Apple privacy changes hit ads business," (2021) Reuters.com: https://www.reuters.com/technology/snap-revenue-falls-short-apple-privacy-changes-hurt-ads-business-2021-10-21/.

17 See Exchnage4media.com (Feb 4, 2022), "Amazon's advertising services grew 32% YoY to $9.7 billion." https://www.exchange4media.com/digital-news/amazon-reports-94-per-cent-hike-in-revenue-at-1374-billion-118253.html.

Be that as it may, the DMA is largely agnostic about the implications for the benefits that end users are expected to have from the specific obligations that gatekeepers are subject to, other than the general hope of expected benefits from greater within-market competition and from preventing monopolization in the focal markets. However, in many cases competition in and for the focal market does not follow a WTA course; in such cases, much more relevant is fostering competition *across* platforms via differentiation (rather than standardization) to reduce monopolization, and facilitate greater innovation by gatekeepers as well as business users that will preserve the capacity of these economic structures and business models to bring large benefits to end users and society at large.

HOW PLATFORMS CREATE VALUE THROUGH CORING AND IMPLICATIONS FOR MARKET DEFINITION

BY CATHERINE TUCKER[1]

1 Catherine Tucker is the Sloan Distinguished Professor of Management Science at MIT Sloan School of Management. She has consulted for many technology companies - please see https://mitmgmtfaculty.mit.edu/cetucker/disclosure/.

I. WHAT IS CORING?

Platforms enable multiple distinct groups of users to interact with one another, and platform economists refer to the practice of actively managing these interactions to ensure they go well as "coring."[2]

A platform acts as a "core" for these interactions by adopting technology, policies, and procedures that facilitate the interaction taking place, build trust in the interactions, and provide incentives for interactions to stay on the platform. This often requires transaction platforms to establish governance mechanisms based on observable transactions that ensure successful interactions.

With interactions that are observable, transaction platform operators can track the quality of the interactions and user satisfaction based on the nature of the transactions (e.g., guaranteeing secure transfer of payment information or identifying accurate matches for user searches). Transaction platforms can continually adjust their policies so that all sides will continue to use the platform to transact through high-quality interactions rather than turn to an alternative.

Coring efforts may increase quality, promote trust, or increase security, and may restrict the ways in which one or both sides can use the platform. Because multi-sided platforms must balance the preferences and actions of all user sides when designing their policies and processes, coring may result in policies restrictive for one side in isolation, but that are pro-competitive and improve the platform as a whole and the quality and value of the interaction for all user sides.

Examples of coring include the creation of reliable rating systems that give insight into the often-unobservable quality of platform participants, such as when device users who download an app from an app store leave a rating or a review. This transparency helps platforms to maintain their reputations and brands, even in the face of some lower quality platform participants. Other examples of coring are constraints on who can use the platform, and policing behavior by some users that may spill over negatively on other users.

Coring can also include limitations on what kinds of products are available, for example limitations on what kind of firms are allowed to advertise at trade shows, if these products lead to dilution of the focus of the trade show. These are all examples of platform competition requiring restriction to better serve the needs of users and respond to potential competitors and new entrants that would exploit negative spillovers and offer better alternatives. The transaction platform creates value from interactions between sides, and requires coring by the operators to enhance overall user welfare.

For example, Uber riders' willingness to use Uber depends on their trust that rides will be safe and punctual. Absent this trust, riders will be less willing to use Uber, which decreases the value of Uber to drivers, and the overall value of Uber's platform in the long term. A coring activity that builds user trust in the quality of interactions is removing users who undermine trust in the quality of interactions on the platform. For example, Uber may remove drivers with bad reviews, as these drivers undermine rider trust in the safety and punctuality of rides.

In terms of the underlying economics, usually coring activities by platforms are aimed at reducing search and transaction costs.[3] Search costs are incurred by users to identify someone on the other side of the platform with whom a beneficial match is possible. Transaction costs are incurred by users after they have found each other and started to interact.

The reduction in search and transaction costs helps unlock the value inherent in network effects that characterize platforms by making it easier to find the appropriate match and cheaper to execute the resulting interaction as the number of users on the platform increase.

For instance, AirBnB, through its integrated search technology, makes it easier for a guest to find the right accommodation at the right time and read reviews to ensure that the place they choose is likely to be a good fit. AirBnB also reduces transaction costs for hosts by providing a secure environment for consumers to pay hosts, and helping settle any disputes that arise between hosts and guests during the stay. The more hosts available on AirBnB, the higher the value that AirBnB's technology, payments and review system creates for guests as they will be able to find better options and transact with them with lower costs.

Effective coring, designed to enhance the attractiveness of the platform for both sides, is also critical to the platform's ongoing viability and innovation. A platform profits from its ability to capture some of the value that its facilitation technology creates. The payments made to the

2 Gawer, Annabelle & Michael A. Cusumano. "Platform leaders." MIT Sloan management review (2015): 68-75.

3 Hagiu, Andrei, "Strategic decisions for multisided platforms," MIT Sloan Management Review, Vol. 55 No. 2, Winter 2014.

platform, either by one or both sides must be used to fund the platform and to continually innovate to compete with other platforms. As such, a platform must encourage the use of its platform by both customer groups to facilitate valuable interactions from which to capture a portion of the surplus. Coring strategies are therefore central to any antitrust analysis of platform market definition, market power, and conduct.

Coring needs evolve as platforms compete, learn about what works, observe their competitors, and monitor evolving interactions on their platform. Continuous coring is particularly critical when a platform is facing competition. While product improvements may occur with or without competition, competition increases the speed with which platforms must respond through such efforts to attract and retain users on both sides in response to competitive pressure.

For example, Uber has increased its coring efforts over time, to build and maintain flexible driving supply capacity and a healthy rider base. In response to issues surrounding rider safety, Uber implemented increased driver screening protocols such as recurring background checks in 2017, adding onto existing driver screening requirements such as completion of a city knowledge test and a quality inspection of cars. In 2018, Uber introduced a safety center for riders, a dashboard with safety tools such as a button to share details and location with others and a panic button to call emergency services, giving customers more tools to ensure their personal safety.

Coring efforts were not limited to the rider side and were also more directly related to competition from other ride-share services. On the driver side, Uber has also introduced new policies over time to attract and retain drivers. In 2014, Uber provided new commercial insurance to close the insurance gap when drivers were on the road without passengers. In 2019, Uber created new driver benefits to attract and maintain talent, such as a new driver lease program and a driver-appreciation bonus coinciding with its IPO.

The trust by buyers and sellers alike that the other party will fulfill its side of the bargain will erode absent corrections and policies from the platform operator to maintain trust and ensure high quality interactions. Specifically, buyers must trust that products will have the advertised characteristics and will not be associated with costs beyond those advertised. Similarly, sellers must trust that payment will be received as agreed for the products they sell and that their reputation will not be damaged by poor behavior by others or systemic failures by the platform. Finally, both buyers and sellers must trust that the interaction will not result in unwanted follow-on transactions or experiences and that the hardware through which they are completing the transaction will not be damaged.

Diminished trust will erode the number of interactions on the platform as well as the number of sellers and buyers. This will in turn erode indirect network effects and leave the platform at a disadvantage relative to other, better-managed platform competitors.

II. HOW DOES THIS BUSINESS SCHOOL CONCEPT OF CORING RELATE TO THE CONCEPT OF TRANSACTION PLATFORMS?

The Supreme Court decision in American Express.[4] has introduced the terminology of a transaction platform into the broader debate about the application of antitrust principles to two-sided platform markets. As defined in the academic article cited by the Supreme Court in its decision, transaction platforms are platforms where the interactions (or "transactions") between both sides of the platform are observable and the transaction itself is also immediately observable. As a result, the platform cannot serve one side without simultaneously serving the other, and the interaction can be facilitated and tailored by the platform.

In contrast, the non-observability of interactions in other contexts severely limits and may eliminate a platform's ability to reduce search and transaction costs in a way that can unlock the same level of value for the platform users. For example, one may argue that a newspaper could be considered a two-sided platform because it connects advertisers with readers and exhibits network effects since advertisers benefit from a greater number of users and users from a greater number of advertisers (assuming advertisers provide information).

It would not, however, be by this definition a transaction platform because although it brings together readers and advertisers, the interaction between readers and advertisers is not observable at the transaction level, nor something the newspaper manages and controls directly. Traditional newspapers cannot tailor advertisements to specific readers and cannot observe whether, for example, a reader opens or reviews an advertising insert or disposes of it. As such, in contrast to operators of two-sided transaction platforms, newspapers do not actively manage the interactions of advertisers and readers and therefore are not primarily focused on managing or optimizing the value of the underlying network effects of the system.

4 *Ohio et al v. American Express Co. et al, Supreme Court of the United States, Docket No. 16-1454, decided June 25, 2018.*

Simply put therefore, a transaction platform is one where the platform conducts serious "coring" activity to facilitate interactions between two groups of users. A non-transaction platform is one where the platform does not attempt to take serious "coring" actions and facilitate interactions between different user groups.

III. IMPLICATIONS FOR MARKET DEFINITION

Market definition is a tool economists use in antitrust cases to help courts evaluate a firm's conduct. By defining a market and understanding what alternatives exist for customers, it is possible to then analyze the likely positive or negative effects of a firm's conduct on consumers.

The key challenge this author sees for market definition in digital platforms is the conflation of a platform's coring actions with a market.

To illustrate this it is useful to take a non-digital example. For example, when I teach platforms, I often refer to the example of an Auckland fish market that brings together fish buyers and fish sellers as a non-digital platform. This encourages some useful discussion of what really is a platform. We talk about how non-digital platforms possess many of the same features as digital platforms, but are often unexciting because they are not easy to scale.

We then turn to talk about coring. Often students have the picture of a fish market as being one where shoppers wander around piles of fish on stands and choose between them. Such an image suggests very little coring activity. This preconception, though, could not be more wrong. The Auckland fish market actually engages in a great deal of coring activities. In particular, it runs an electronic "Dutch auction." In this Dutch auction, a large bidding clock displays a description of each lot on offer. The auctioneer started the clock at about $2 above the expected price per kilo. The price drops every 10 seconds – until a buyer enters a bid on their keypad. At the point the buyer's name appears above the clock. In other words, this is an example of a non-digital platform where the platform takes its job of coring seriously, and reduces search and transaction costs for participants.

In this case the product market should be defined as the facilitation of interactions between fish buyers and fish sellers. To see why this makes sense, think about the real competitive constraints on the fish market – it is the potential that fish sellers and fish buyers could find other ways of interacting.

However, what I see happening again and again in multiple antitrust cases, is that the market is defined as something analogous to "the provision of Dutch auction services at the Auckland fish market," or, even more specifically, "the provision of digital bidding clocks at the Auckland fish market." In other words, the coring actions of the platforms are conflated with a market definition. This has two problematic implications. First, simply because of the nature of platforms, this means that using an incorrectly narrow market definition will almost by definition produce a conclusion of monopoly power. Second, because the market definition is incorrect, when this wrong market definition is used to evaluate conduct, that evaluation will almost certain miss out on analyzing the benefits that this coring action brings to users of this platform in terms of reducing underlying search and transaction costs.

Therefore, this article will end with a plea to courts, which is to understand that the business of platforms is to bring together different groups of users together and make their subsequent interactions go well through coring. The coring actions that the platform takes, however, are not a market, nor an after-market, nor any kind of market. Instead, they should simply be viewed as the actions the platform takes which aim to make interactions go well.

TOXIC INNOVATION IN THE DIGITAL ECONOMY

BY ARIEL EZRACHI & MAURICE E. STUCKE[1]

1 Ariel Ezrachi is the Slaughter and May Professor of Competition Law at the University of Oxford and the Director of the University of Oxford Centre for Competition Law and Policy. Maurice E. Stucke is the Douglas A. Blaze Distinguished Professor of Law at the University of Tennessee and principal of the law firm Konkurrenz.

I. INTRODUCTION

The digital platform economy delivers on many fronts, offering us new products, technologies, and means to communicate, trade, and explore. And one of the celebrated aspects of the digital economy is the ensuing innovation. And even more so when speaking about the platform economy, where platforms, like coral reefs, attract innovators, disruptors, and new businesses and offer them unparalleled access to markets and users.

Indeed, there is little doubt as to the significant investments in research and development by leading tech firms, such as Google, Apple, Facebook, Amazon, and Microsoft. But behind the impressive numbers, lies a more complex tale that questions the merit of our quantitative fixation on numbers. A fixation that views the volume of investment as assurance for future prosperity. A fixation that ignores the value, nature, and plurality of innovation.

In our new book *How Big-Tech Barons Smash Innovation and How to Strike Back* (HarperCollins 2022), we look behind the numbers and explore the means through which these large tech firms, in controlling digital ecosystems, can distort the paths of innovation and undermine disruption.

Our inquiry into the distorting effects began in late 2017 when the European Commission asked us to research innovation in the digital economy. Our earlier work, including *Virtual Competition*, raised the concern of policymakers as we uncovered several significant risks of the digital economy, including sellers' pricing algorithms colluding. But on innovation, we, like many others, were optimistic. At first, we didn't think our innovation policies were working.

As we dug into the data over the next few years, we found multiple fallacies about innovation in the digital economy. After submitting our report, we continued our inquiry into the effects that these big tech barons have on innovation and how they not only affect the dynamics of competition within their tightly-controlled ecosystems but also the nature of innovation we receive. While Tech Barons tolerate innovations that do not threaten their ecosystems, they will smash disruption that threatens their profit models. This is problematic, especially as the Tech Barons' ecosystems expand.

Based on our research, including our discussions with market participants, four things became clear:

- *first*, the Tech Barons design their ecosystems to favor their interests (at the cost of crushing beneficial innovations);
- *second*, the Tech Barons' value chain dictates the type and scope of innovation that you will find, and in looking at the value chains, we can predict that the inventions will become creepier;
- *third*, even if you can avoid some or all of the Tech Barons' ecosystems, you cannot avoid the toxicity of some of their innovations; and
- *finally*, while the Big Tech Barons are in the news for their mounting antitrust attacks, the likely relief, if any, will not fix the underlying problems.

II. SO HOW DO TECH BARONS SUPPRESS DISRUPTION?

In controlling their ecosystems, they are in an advantageous position that offers them near-perfect market surveillance needed to identify and neutralize nascent threats. Using advanced technologies, the Tech Barons can identify market patterns and discern trends (and threats) well before others, including the government. This data advantage turns the nowcasting technology into a game-changer. Facebook, for example, acquired the data-security Onavo, to track users' smartphone activity. That technology was central in its acquisitions of perceived competitive threats, including WhatsApp.

With a clear view of risks beyond the horizons, the Tech Barons can engage in strategies aimed at distorting the supply of disruptive innovation. This includes their exclusion of disruptors from the ecosystem by refusing access or reducing interoperability. Strategies to distort the growth of disruptive technology may also involve the copycat of technologies to deprive disruptors of the scale necessary to survive, limiting disruptors' access to long-term funding, and of course, the acquisition of these disruptors.

Next, the Tech Barons can manipulate user demand for innovation. To reduce the adoption rate of disruptive innovations, the Tech Barons increase retention of users, reduce friction to the complementary sustaining innovations that fortify their ecosystem, and increase friction to the potentially disruptive innovations. The path to the Tech Baron's creations is frictionless (think, for example, how Amazon's Buy Box reduces

friction for purchasing items). In contrast, our path to the disruptive innovators, whom we describe as the Tech Pirates, has many obstacles, enough to deprive them of scale and experimentation (think of the challenges associated with side loading of apps). While many of us may have a sense of autonomy when we choose services online, we are walking down a path that was carefully designed for us. Using dark patterns, self-favoritism, and other means, the Tech Barons can nudge us toward innovations they want us to adopt and away from disruptors.

III. TOXIC INNOVATION

What happens when the Tech Barons distort the supply and demand of innovation? As our book explores, we receive fewer disruptive innovations, more innovations that sustain the Tech Barons' power, and more innovations that extract or destroy value. Once the Tech Barons can affect the supply and demand of innovation, the nature and value of innovation change. Value-creating innovations will be gradually displaced by innovations that focus on extracting value from the downstream users or upstream suppliers and primarily benefit the Tech Barons.

Of course, this is not an all-or-nothing scenario. As the Tech Barons' power increases, we won't be inundated with solely value-destroying innovations. Instead, it reflects a material but subtle change in the value and nature of innovation as the plurality of innovation diminishes. A look at the patents and research by the leading ecosystems confirms this trend, with advanced technologies that go far beyond predicting our behavior to some genuinely frightening methods of exploitation, manipulation, and extraction of value.

IV. RIPPLE EFFECTS

Many of us already sense that these toxic innovations weaken social cohesion, increase tribalism, and undermine democracy. But avoiding the Tech Barons' ecosystems, even if we could, is not the answer. As our book explores, the ripple effects from the toxic innovation extend far beyond the Tech Barons' ecosystems, the digital economy, the user experience, and the impact on disruptors. These toxic innovations ultimately erode our social and political fabric and harm our autonomy, democracy, and well-being. The value chains and profit motives have left us with new technologies that are ripping apart the social fabric and the foundations of our society.

We see these effects, for example, when we look at the business models and retention strategies at the heart of social media and online behavioral advertising. Tribalism and rancor are part of the price we pay for the loss of innovation plurality. Similarly, democracy is weakened from advanced microtargeting and manipulation, as profit motives lead to distortions that undermine the foundations on which our society is established.

Many are familiar with the story of Cambridge Analytica, but importantly, it is only one example of the microtargeting, manipulation, and deception of voters spawned by these toxic innovations. It is a symptom of a spreading problem where data advantage and negative messaging are the ultimate tools to control the crowd. Political campaigns are now designed to trigger the desired emotional reaction of individual voters. So, if you are among those with a high need for arousal, expect more violent, sexual, and fear-provoking content. An evolving disinformation machine at a scale and efficiency never seen before.

With disruptors crushed, these innovations fortify the prevailing value chain and business model. And while the Tech Barons offer tools to mitigate some of these effects (like requiring certain political ads to include disclaimers with the name and entity that paid for the ads), they cannot prevent their platforms from being weaponized or their toxic innovations from being deployed to undermine democracy. They must feed the beast, and that beast is destroying us.

V. WHY THE PROPOSED REGULATORY REFORMS ARE INSUFFICIENT

We all talk about innovation but don't appreciate the inadequacy of current enforcement policies and regulations. Most importantly, current policies do not address the key driver – the value chain – which is affecting the Tech Barons' strategies.

With these faults at the base of our policies, there is little wonder that we are off course. After all, any navigator knows a basic rule. A small degree error, insignificant in a short voyage, will increase the longer one travels. It's known as the "1 in 60 rule of thumb." A one-degree error in navigation will lead a pilot one mile away from her destination for every 60 miles of travel. This rule helps illustrate how seemingly insignificant flaws in past assumptions and policies have led us off course. It helps us appreciate the impact and actual costs of past economic and industrial policies that failed to adapt to the changing dynamics of competition and innovation in the digital economy. Considering the supersonic

speed in which we travel in the digital economy, and the significant degrees of error, it is perhaps not surprising that we find ourselves at a crisis point.

Of course, the Tech Barons prefer that we stick with the current antitrust policies, designed many years ago and ill-suited to deter their power to affect the supply and demand of innovation across their vast ecosystems. To ensure this, they challenge any change to the *status quo* and offer an ideological platter of claims that any change to the current policies will only chill innovation and put us at a competitive disadvantage against China. They tout how their ecosystems act as coral reefs in lowering the cost for others to innovate. And of course, the notion that disruptive innovation is around the corner, and therefore any intervention is superfluous. The power of these claims lies in their having a kernel of truth, and being oft-repeated. Even though they do not withstand scrutiny, conventional wisdom remains hard to resist.

Consequently, as a result of the Tech Barons' lobbying and resistance to change, our antitrust laws have failed to rein in the Tech Barons or deter them from smashing disruptive innovations. Even though competition authorities around the world by 2022 were challenging most of the Tech Barons, the lethal cocktail of ideology and lobbying has led the courts to marginalize antitrust, or at the very least its ability to protect against future disruption. Under the U.S. courts' price-centric approach, it is difficult to prove that the Tech Baron is indeed a monopoly (consider the struggles Epic and the FTC had in their monopolization cases against Apple and Facebook, respectively). Even if the agency overcomes that hurdle, it is often difficult for the agency to prove that the Tech Baron abused its dominance. Even if the agency succeeds, the relief will often be too little too late.

To address this gap, the U.S., EU, and elsewhere have proposed new regulations to deter the Tech Barons' anticompetitive behavior and make the digital economy more contestable and fairer. As we discuss, the new policies can go a long way to help protect future innovation, but they also suffer from limitations that will prevent them from eliminating the toxic innovation.

To see why we consider duck hunting. In hunting ducks, one needs to shoot where the duck is heading, not where it is now. Otherwise, the duck will be gone by the time the shot reaches its initial position. So you calculate the duck's likely path and shoot ahead of it. If you practice enough, you can predict the flight path. But in following the duck's flight path, you can become fixated on calculating the proper lead.

Why raise duck hunting when discussing the Tech Barons? Of course, the aim isn't to kill the Tech Barons. Driving them out of business would chill innovation. Underlying all the policy proposals is the desire to avoid chilling value-creating innovation, including those from the Tech Barons. Instead, the aim is to kill the Tech Barons' anti-competitive practices.

With this in mind, the duck hunting analogy illustrates the potential pitfalls of the existing reforms for the digital economy. In particular, one should not focus solely on past violations when designing new regulatory tools. Most of the specific obligations under Europe's and the U.S. proposals aim at the Tech Barons' past anticompetitive restraints. But policymakers need to consider that as technologies evolve, the Tech Barons may no longer require their earlier anti-competitive practices to maintain their power and influence innovation paths. Thus, the policy challenge is not cataloging earlier anti-competitive behavior but anticipating the Tech Barons' future anti-competitive tactics to colonize new platforms and expand their ecosystem. The new policy tools must be specific enough to identify anti-competitive practices but sufficiently flexible to adjust to changing market realities. Policymakers, however, are ill-equipped to accurately predict the Tech Barons' future anti-competitive moves. So, they mostly shoot where the duck was, not where it is heading. Thus, even with the Digital Markets Act, Digital Services Act, and Data Act, Europe will still feel the ripple effects of toxic innovation. Ditto for the U.S. (even if Congress finally enacted the bipartisan-sponsored bills).

VI. WHAT CAN BE DONE?

There is no simple fix to deter toxic innovation and promote disruptive innovations that actually create value. Instead, our book offers three key principles to guide the design and enforcement of innovation policies:

- First, policymakers must consider the value of the innovation and whether it creates, destroys, or extracts value. Innovation is neither inevitable nor invariably desirable. Since not all innovation increases value, policymakers, and enforcers must inquire about the type of innovation (sustaining or disruptive) and whether it increases or reduces our well-being (that is, whether it destroys, extracts, or increases value).
- Second, policymakers must consider the incentives at stake, which are directly influenced by the ecosystem's value chain. Policymakers must inquire about who's designing the ecosystem and influencing the innovation paths, what are the ecosystem's value chains, and what incentives it fosters. As our book explores, what's good for the Tech Baron is not necessarily what's good for us. And so, one must understand the incentives at play (that flow from the value chain) and ensure these

incentives align with our interests. Every ecosystem is regulated — whether by Tech Barons, informal norms, or laws, rules, and regulations (that incentivize a range of actions and strategies). If policymakers assume that the marketplace is naturally self-regulating and that the market participants' incentives will always align with our interests, they are ill-informed.

- The third principle is the *diversity of innovation*. The antitrust policies should promote an effective competitive process that enables disruption and innovation plurality and offers Tech Pirates a viable opportunity to prosper. The diversity of innovation paths is crucial for future prosperity. We cannot predict who will emerge as the next disruptor, given their high rate of failure and the evolutionary selection on which we rely to ensure that the right innovations prosper. But we can hedge our bets by fostering a plurality of innovators and the ensuing collision of ideas from different fields.

We illustrate how the Value, Incentives, and Diversity principles can inform policy choices on two complementary levels: *first* through Optimization Policies that ensure that the innovation serves society's interests, not the Tech Barons', and second through Innovation Support Policies that sustain and promote Tech Pirates' disruptive innovation through the provision of aid through grants, tax breaks, and other supportive means. One surprising finding is the benefits of in investing cities to support innovation.

VII. CONCLUSION

Our message is clear. The current incentives and policies have put the digital economy on the wrong trajectory. Instead of improving our standard of living, the technological advances may prolong (and in some countries worsen) the already significant wealth inequality, reduce our autonomy and well-being, and be used to destabilize democracies. And we can't expect this trajectory to self-correct. Betting on the entrenched Tech Barons, whose incentives are not necessarily aligned with ours, to provide the paradigm-shifting innovation is a terrible bet. We should be betting on and investing in disruptors, cities, plurality, and diversity.

RECOMMENDER SYSTEMS: APPROACHES TO SHAPE A SAFE, COMPETITIVE, AND INNOVATION-DRIVEN FUTURE

BY MARCO IANSITI, ROHIT CHATTERJEE, BARTLEY TABLANTE, SEAN DURKIN, ANURAG GANDHI & ABBY DROKHLYANSKY[1]

1 Keystone Strategy. Marco Iansiti is also affiliated with Harvard Business School, Harvard University. The authors would also like to disclose that Keystone Strategy has worked with most digital platform firms, including Amazon, Meta and Microsoft as well as a number of regulatory agencies involved in platform related regulation or controversy, including the US Department of Justice and other U.S. and European regulatory authorities and governing bodies.

I. INTRODUCTION

In most digital platforms recommender systems provide consumers with recommendations across a variety of contexts (e.g. list of products in the "You might also like" section on Amazon). While recommender systems generate efficiencies by lowering the cost and improving the quality of product discovery, their impact on individuals' purchase and consumption has the potential of affecting downstream competition of products and industries. Additionally, these systems may also present sensitive issues for national security, democracy, and public health. Unsurprisingly, recommender systems have therefore come under increasing scrutiny from governments around the world in recent years.

Despite the associated risks, the scale of efficiencies and benefits offered by recommender systems motivates their continued use and expansion in the future. In this paper we explore approaches that merge innovation and regulation as part of technological advancement. We offer an approach built on increased transparency on the side of companies regarding both their data and algorithms, as well as through collaborations between digital platforms, academics, and regulators. By taking responsibility for regulating their recommender systems in the short-term, companies will be well-positioned to reap long-term benefits and to serve as leaders in the ecosystem. To further address the potential externalities of recommender systems, improved regulation and monitoring by external bodies will also help cultivate the market. With digital regulations of these systems still being in a relatively nascent stage adopting these types of approaches can help shape a safe, competitive and innovation-driven future.

II. RECOMMENDER SYSTEMS ENABLE PROVISION OF PERSONALIZED CONTENT

Recommender systems are one of the most common types of machine learning systems, with billions of consumer interactions each day. Recommender systems provide consumers with recommendations across a variety of contexts, including consumer retail product recommendations, music, movies, television, and social media content. In certain contexts (e.g. social media), recommender systems maybe commonly referred to as "the algorithm" that recommends content on online digital platforms.

Recommender systems are an innovation that generates efficiencies by simplifying and lowering the cost of product discovery. For example, Amazon uses a recommender system to suggest products a user may wish to purchase based on current and historical product views and purchases, and it offers this as an Amazon Personalize product to other companies. Spotify uses a recommender system to generate "made for you" playlists of new music based on the listening history of users and those similar to them. Facebook's News Feed, Twitter, and TikTok's "For You Page" all use recommender systems to determine which posts, tweets, or short videos to surface to users based on their engagement with prior content.

Recommender systems also have the potential to affect competitive dynamics, changing the products that individuals purchase and consume, affecting consumer preferences and changing long-term behavior in ways that are not yet well-understood. Due to the prevalence of recommender systems and their uncertain long-term effects, some regulators have promulgated regulations, proposed to regulate, or even suggested outright bans on the use of recommender systems in certain contexts.

A more nuanced approach to controlling the effects of recommender systems than overarching bans could still mitigate harms without precluding the tremendous efficiencies recommender systems create for consumers. Recent work in economics, computer science, and management science offers insights for how to further investigate recommender systems while preserving the benefits this innovation offers.

III. RECOMMENDER SYSTEMS TURN HISTORIC DECISIONS INTO PERSONALIZED RECOMMENDATIONS

Unlike humans, computer systems cannot easily or effectively reason in the abstract about the meaning of a work or its suitability to a given audience. Computer scientists have developed two methods which computers can perform that are mathematically simple but yield highly effective recommendations.

The first approach is to recommend products or content similar to what a user has enjoyed in the past. This is known as **content-based filtering**. It is relatively fast, so it scales up well to millions of users, and it does not require knowing anything beyond the preferences of the

specific user in question. However, it requires carefully modeling the type of content being provided by hand-engineering "features," or aspects of the book or movie upon which the recommendation will be based, for example "genre: horror."

The second approach is to recommend content similar to what other similar users have watched or enjoyed in the past. This approach is known as **collaborative filtering**. Collaborative filtering can also scale up with sufficient computational power and avoids the need for hand-engineering features by learning what aspects of the content are important directly from the data itself. These two approaches to recommender system implementations can be used independently or in tandem to maximize monetization, data, and user engagement on a platform.

A product manager exploring technologies for example, may choose to trade investments in data and modeling for improved engagement, increased monetization, and even more data. In this example, the data required for recommender systems are user interactions with content. Several factors, including user heterogeneity and content heterogeneity influence the volume and type of data required. As an example, in 2017, when Netflix replaced the 5-point rating scale with a binary "thumbs up" or "thumbs down", that feature change resulted in significantly more responses from viewers on their platform.

Companies use the output from recommender systems in several ways:

- To select a specific product or content to recommend
- To determine the ordering in a list of products or content
- To select a customized menu of products as a bundle or sequential offering (for example, Amazon's "Frequently bought together" option)

Successful recommender systems provide products which a consumer will purchase or content with which they will engage. This has several benefits for the implementor including:

- **Increased transactions** which can directly increase monetization if algorithmic output results in financial transactions. These sales can be either direct like in ecommerce sales or indirect from advertising.
- **Increased satisfaction** from using the product, which can result in greater use by individual users, and marginal users engaging with the recommendations.
- **Increased data** to feed back into the recommender system to improve the accuracy of future recommendations, creating a positive feedback loop.

Because of the significant benefits available from improved recommender systems, companies invest significantly in their design. For example, in 2006 Netflix announced the Netflix Prize, an open challenge inviting teams to improve Netflix's recommendation engine and offering a million dollars as a reward.[2] The benchmark was to improve predictive power by 10 percent, which essentially entailed reducing the root mean squared error of recommendations.

The Netflix prize showcased two key aspects of AI advancement. First, that external teams could assist a technology-first company like Netflix on the impact of its algorithms. Second, that large quantities of user data could be tagged with a finite set of features that an algorithm could be trained on to eventually make successful recommendations. The benefits of recommender systems motivate their prevalence, enabling platforms to target users in a way that enables content personalization at an unprecedented scale. Recommender systems also, however, entail certain caveats that require consideration to determine the full scope of associated risks.

IV. RECOMMENDER SYSTEMS CREATE RISKS

Potential harms that recommender systems can generate are complex, and there is no common consensus on how to mitigate these harms. One of the potential harms that applies broadly across fields is that recommender systems can create **filter bubbles**, as described by Prof. Michael Kearns in his book *The Ethical Algorithm*. By selectively serving information a user may find engaging and not serving contradictory viewpoints, recommender systems reinforce users' existing worldviews and biases; this intellectual isolation is called a filter bubble.

There is emerging evidence from the fields of management science, industrial economics, healthcare, and computer science that recommender systems may cause impacts across a variety of domains of interest to policy makers. These domains include competition, national security, privacy, and public health.

2 https://lsa.umich.edu/social-solutions/diversity-democracy/oci-series/excerpts/volume-ii/the-netflix-prize.html.

A. Effects on Competition

Recommender systems can impact competition in two main ways. First, recommender systems may exhibit strong network effects, and the recommendations they issue may be reliant upon data that is of sufficient quality, scale, scope, and uniqueness to present a durable barrier to competition. For example, despite a large social network with which to bootstrap its launch, Instagram's Reels has struggled to compete with TikTok, a product based on a short form video recommender system. In this case, the next generation of AI-based digital platforms may exacerbate the winner-take-all nature of previous generations of online digital platforms.

Second, recommender systems may allow for various forms of self-preferencing, wherein a platform's recommender system biases toward recommendations for a platform's own products or services. Because recommender systems are generally not transparent in design to either users or regulators, such efforts may go undetected.

B. Effects on National Security

Recommender systems pose several potential harms to national security. Recommender systems may increase political polarization and extremism, particularly when designed to optimize platform engagement. For example, early recommender systems may have steered users interested in the politics of Islamic states toward increasingly extremist content.

Recommender systems controlled by one nation-state may present an opportunity for covert influence over the citizens of another nation state. For example, several nations have banned or conducted national security reviews of ByteDance's TikTok application.[3] Industry analysts at the time feared that videos pushed by the platform's recommender system could steer unwitting users toward views supportive of China's government.[4] In September 2020, the DOJ filed an explanation of its proposed ban of TikTok, alleging that the application "is a mouthpiece for the CCP in that it is committed to promoting the CCP's agenda and messaging."[5] This ban was overturned[6] by a Federal judge in December 2020, before the Biden administration ultimately agreed to drop the litigation against TikTok in June 2021, pending a review by the Commerce Department.[7]

C. Effects on Privacy

Recommender systems may unintentionally leak information about one user's prior behavior to other users of the system. For example, one user visiting a platform from the same internet connection as another user who viewed privacy-sensitive content may see that content recommended to them.

D. Effects on Public Health

The usage of social media may be correlated with negative psychiatric effects such as increased anxiety and depression, particularly in children and young adults. While the state of causal evidence remains unclear, these potential effects have prompted government investigations. Some platforms, such as TikTok,[8] have recognized that optimizing content for personalization and relevance results in homogenous streams of content that can have addictive properties.

V. ALTHOUGH IN EARLY STAGES, RECOMMENDER SYSTEMS ARE UNDER INCREASING SCRUTINY FROM REGULATORS ACROSS THE WORLD

Recommender systems have come under increasing scrutiny from governments around the world in recent years. Digital regulations are in a relatively nascent stage and lawmakers in different countries are exploring various potential solutions that address both the creation and dissemination of content on digital platforms.

3 https://www.axios.com/2020/08/06/tiktok-bans-worldwide-china.

4 https://stratechery.com/2020/the-tiktok-war/.

5 *TikTok Inc. v. Trump,* DOJ Memorandum in Opposition to Motion for Preliminary Injunction, https://www.documentcloud.org/documents/7218230-DOJ-s-MEMORANDUM-in-OPPOSITION-to-TIKTOK.html.

6 https://abcnews.go.com/Politics/wireStory/judge-blocks-trumps-tiktok-ban-app-limbo-74604450.

7 https://www.pacermonitor.com/view/LHZIOGA/TIKTOK_INC_et_al_v_TRUMP_et_al__dcdce-20-02658__0071.0.pdf?mcid=tGE3TEOA.

8 https://newsroom.tiktok.com/en-us/how-tiktok-recommends-videos-for-you.

A. United States

In the United States, former and current employees of the largest social media platforms have blown the whistle on concerns such the spread of misinformation and polarization. In response, a bipartisan group of lawmakers drafted the Filter Bubble Transparency Act,[9] which would require platforms to let people use a version of their services where content is not selected by "opaque algorithms" driven by personal data. The requirements stipulated in this law do not apply when algorithmic ranking systems use personal data "expressly provided" by the user "to determine the order or manner in which information is delivered to them" (such as search terms, filters, speech patterns, saved preferences, social media profiles and content followed by the user.) The Senate version of this bill[10] would empower the Federal Trade Commission to enforce the new regulations and impose civil penalties.

Another bill introduced in the House last year is the Justice Against Malicious Algorithms Act,[11] which would amend section 230 of the Communications Act of 1934 and limit liability protections granted to providers of internet services. If this bill were to pass, platforms could face lawsuits for allegations of serving false, misleading, and dangerous information to their users.

B. China

In China, the Cyberspace Administration is developing a set of regulations which will govern the design of recommender systems and give users the ability to stop platforms from using their data. They announced in a statement late last year that companies must abide by business ethics and principles of fairness and should not set up algorithmic models that entice users to spend large amounts of money or to spend money in ways that may disrupt public order.[12] These new regulations are the first of their kind and will require tech companies operating in China to make significant investments in compliance and change the way they operate. Whereas critics of these regulations claim that they could result in infringements on free speech, it is noteworthy that China is a global leader in the regulation of the AI algorithm space.

C. European Union

The European Union is also developing its own set of regulations under the broader umbrella of the Digital Services Act ("DSA"), which aims to create a safer digital space where the rights of users are protected, and businesses can compete on a level playing field.[13] Article 29 of the draft DSA requires Very Large Online Platforms ("VLOPs") to set out in their terms and conditions the main parameters used in their recommender systems, as well as any options for users to modify those parameters, including at least one not based on profiling.[14]

VI. UNLOCKING THE VALUE OF RECOMMENDER SYSTEMS REQUIRES FURTHER STUDY OF BEHAVIORAL AND SOCIETAL OUTCOMES

In the absence of a regulatory consensus, we recommend steps to gather additional data incentivizing cooperation, increasing transparency, and expanding joint efforts among digital platforms, regulators, and academia. Such efforts can enable policy makers to better understand and address the potential harms of recommender systems while preserving the efficiencies they offer.

Before the issues with recommender systems can be understood well enough to approach solutions, the clashing incentives between digital platforms, academics, and regulators must be aligned.

Academics possess robust tools and theoretical approaches which may ameliorate harms but lack the access to data and systems to test their hypotheses. Currently, academics are constrained to conduct analyses based primarily on external observations of a recommender systems' operation and limited tools such as user surveys. These methods can often reveal correlational evidence, but struggle with problems of

9 https://www.govtrack.us/congress/bills/117/s2024/text.

10 https://www.thune.senate.gov/public/_cache/files/27e9a4ad-1d45-4191-8e46-8694dc5b0bbe/F1482EA8F7D55FB810C2D651F784C490.lyn21514.pdf.

11 https://www.congress.gov/bill/117th-congress/house-bill/5596/text.

12 https://mp.weixin.qq.com/s/XdQVqqjJdLRlL0p6jlbwsQ.

13 https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package.

14 Draft DSA, pp. 61-62.

reverse causality. For example, teens who use social media with high frequency may suffer higher rates of depression, but it may be the depression causing the social media use rather than the inverse.

Digital platforms possess the data and systems necessary to measure the effects of recommender systems on various outcomes of interest to policy makers. However, because the costs of recommender system malfunction are externalized to users and society at large, digital platforms have little incentive to investigate these issues. Even those digital platforms wishing to investigate societal harm fear increasing their own liability if their own investigations were to substantiate regulatory concerns.

By instead choosing to invest in the transparency of their recommendation algorithms, companies can position themselves in a way that prepares them for potential future regulations, promotes sustainable collaborations with external parties, generates user trust and satisfaction, and prevents undesirable externalities in the long-term. For example, platforms can conduct and publish regular audits of their recommender systems and monitor their performance to proactively avoid causing harms. By leveraging transparent partnerships with academic researchers and regulators, companies can prevent information silos and receive cross-functional input to prevent potential harms across fields. For example, a recommender system causing privacy harms could also impact children's mental health, and without input from experts in both domains, this could result in duplicative efforts to address the two issues separately.

Digital platforms should adopt an approach of maximal public transparency and regulatory cooperation in the near term. Since digital platforms exist in the same societal substrate as their users, they rely upon the continued stability of their users' societies for their long-term profitability. It is therefore in the long run self-interest of digital platforms to investigate societal harms. Investing in best practices for recommender system regulations and algorithmic transparency in the short-term will enable digital platforms to be well-positioned to respond to future regulations, ensure survivability, and garner positive publicity.

Regulators also have a number of tools at their disposal to encourage companies to better investigate and document potential issues arising from recommender systems. As one example, privacy regulators can investigate and where necessary litigate to address privacy harms arising from recommender systems.

The greatest potential harms of recommender systems, those related to polarization, extremism, and mental health, are also the most diffuse. As a result, their extent is difficult to establish. Because of the potential political impacts of the effects of recommender systems in these areas, there is high potential for accusations of bias and mismanagement. Research into these issues needs to be conducted in a thoroughly scientific non-partisan fashion for these harms to be effectively addressed.

Legislation can both increase the immediacy of long-run societal costs through fines and lower the barriers to transparency by creating mechanisms for review such as audits. Legislation can also create historical exceptions for digital platforms for prior harms caused by recommender systems, in exchange for greater future regulatory access to necessary data and tools.

Understanding the potential harms caused by widely deployed new technologies, including recommender systems, is an ongoing effort. As these problems are complex and multi-disciplinary, input from a variety of stakeholders is necessary to approach solutions.

VII. COMPANIES SHOULD TAKE THE OPPORTUNITY TO IMPLEMENT REGULATIONS OF RECOMMENDER SYSTEMS

Since regulations are not yet in force, now is the time for corporations to develop best practices and sustainable standards for their approaches to recommender systems. Corporations have the opportunity to lead in establishing comprehensive programs integrated within their business operations to generate exemplary industry protocols for all. Several key components to consider for such a program are: Inventory, Metrics, Compliance and Governance, and Transparency and Education.

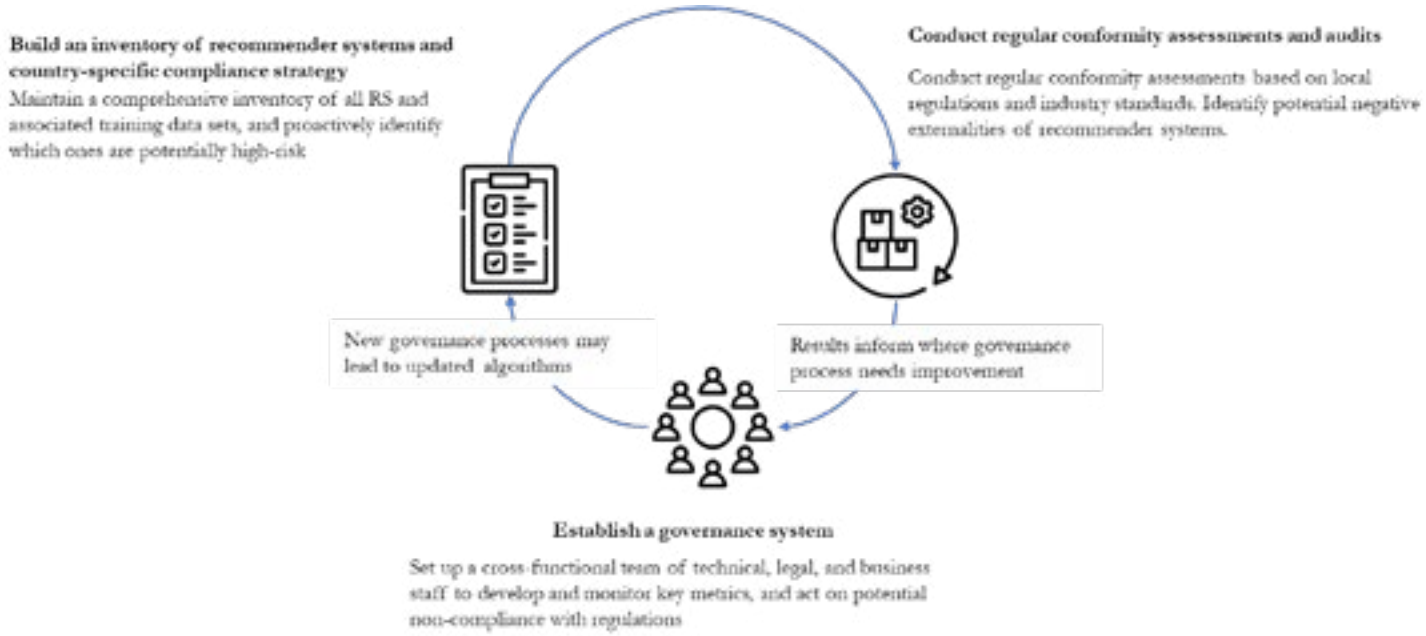
- **Inventory**: Firms can maintain an inventory of all recommendation algorithms used on their platform, along with their corresponding training datasets. This would provide a resource for tracking ecosystem effects over time and auditing algorithmic performance and biases.
- **Audit and Measurement**: Firms can develop metrics, such as tracking content homogeneity or assessing time spent by users on the platform as a check for addiction, to measure how their recommendation algorithms affect the ecosystem.
- **Compliance and Governance**: Firms can develop a holistic strategy for the role AI/ML will play within the organization and clear re-

porting structures that allow for multiple checks of recommender systems before and after they are put into production use. Firms can actively track the latest regulations in all jurisdictions where they operate and adapt their recommendation algorithms in compliance with local law or to address user complaints.

- **Transparency and Education**: Firms can allow users easy access to details of how their data is being used and why they are being recommended certain content. They can also make such information easily accessible for academics, non-profits, and regulators. Where information transfer alone is not sufficient to answer key public policy questions, digital platforms should work with regulators to structure analyses that can be conducted using companies' tooling and data in a manner sensitive to user privacy.

Building off these foundational components, firms can develop a continuous feedback loop to further hone their recommender system risk management programs (See Figure 1). This feedback loop has three steps – build an inventory of recommendation algorithms, conduct regular conformity assessments and audits, and establish a governance system.

Figure 1: Feedback loop to improve risk management program



ZERO-PRICE PLATFORM SERVICES: THERE IS NO FREE LUNCH IN APPLYING THE "NO FREE LUNCH" PRINCIPLE

BY ALEXANDER RASKOVICH & JOHN M. YUN[1]

1 Alexander Raskovich is the Global Antitrust Institute's Director of Research and formerly served for more than three decades as a research economist in the Antitrust Division of the U.S. Department of Justice. John M. Yun is an Associate Professor, Antonin Scalia Law School, George Mason University, and the Global Antitrust Institute's Deputy Executive Director; formerly served as an Acting Deputy Assistant Director in the Bureau of Economics at the U.S. Federal Trade Commission.

There is a well-known economic principle that goes by the acronym TINSTAAFL, meaning "there is no such thing as a free lunch."[2] Hereafter, we simplify the acronym to the NFLP ("no free lunch principle"). The NFLP is the truism that, at the margin, any benefit must come at some cost; economic resources must be expended, and someone will have to cover those expenditures. But the NFLP does not, without more, specify *who* bears the costs.

If a friend treats you to lunch, the lunch is free to you, but your friend must pay. It would be invalid to infer from the NFLP that in fact you are paying for the lunch, perhaps by enduring your companion's unpleasant company in exchange for food and drink. That might be true but need not be. In the context of friendship, lunch — however procured — typically is win-win. This is an example of the fundamental economic principle that voluntary trade tends to benefit both parties to the exchange. Trade is not a zero-sum game.

What can be reasonably inferred from the lunch, based on the gains-from-trade principle, is that companions voluntarily participate in a lunch because each one benefits on net from the interaction, in non-pecuniary or pecuniary terms. And based on the closely related economic principle of revealed preference, the one paying for the lunch can be reasonably inferred to value the interaction by more than the amount paid.

It appears, however, that the NFLP has been misunderstood and misapplied in the context of zero-price platform services. Some have asserted that the NFLP implies zero-price platform services must be paid for by consumers in some other way, such as the loss through data collection of privacy valued by consumers.[3] Others have gone further, asserting that consumers are not only made worse off by the data collection and use that attend zero-price platform services, but that this state of affairs necessarily points to a lack of competitive alternatives.[4] Both assertions are invalid, pressing the NFLP beyond the limits of logical inference. So broad is the scope of the NFLP that it applies to itself: there is no free lunch in applying the No Free Lunch Principle to zero-price platform services. Inferences about who pays resource costs, and whether those payments reflect market power, are empirical questions as illuminated by other economic principles. Answers to such critical questions cannot be plucked from an NFLP magic hat.

Providing zero-price platform services is of course costly. By the NFLP, the platform itself, or participants on another side of a multisided platform, may bear those costs when consumers pay nothing. But, once again, it would be invalid to infer from the NFLP that *consumers* necessarily pay for a zero-price platform service in non-price ways, such as through data collection with corresponding losses of privacy valued by consumers. As with the case of lunch with an unpleasant companion, that might be true but need not be. What can be inferred (without more) from the observation of a zero-price service, applying the NFLP and with an economic presumption of platform rationality, is that the platform expects to recover the associated resource costs in some other way than charging a price to consumers.[5]

The potential error here is a subtle one, but with profound consequences. It is wrong to conflate the resource costs required to provide a service with the effective price paid by those receiving the service. The NFLP does not imply the two must be equal. On the contrary, by the economics of multisided platforms, the relative prices and marginal costs of platform services may not be equated on any given side of a multisided platform.[6]

In the presence of indirect network effects — that incremental participation on one side of a network yields spillover benefits to another side — those spillovers are optimally considered by a platform when it sets its prices. The higher the spillover benefits generated by participation on a given side, the lower the price charged to participants on that side tends to be, because the platform can monetize the resulting spillovers through prices charged to participants on the other side. If the spillovers are large enough, the price may be zero or even negative for the side that generates those spillovers.

---

2 See, e.g. The Phrase Finder, *There's no such thing as a free lunch*, https://www.phrases.org.uk/meanings/tanstaafl.html (the phrase "denoted the free food that American saloon keepers used to attract drinkers; for example, this advertisement for a Milwaukee saloon, in The Commercial Advertiser, June 1850: At The Crescent...Can be found the choicest of Segars, Wines and Liquors...N. B. - A free lunch every day at 11 o'clock will be served up.").

3 See, e.g. Jonas Koponen & Annamaria Mangiaracina, *No Free Lunch: Personal Data and Privacy in EU Competition Law*, 9 Competition L. Int'l 183 (2013).

4 See, e.g. Majority Staff Report and Recommendations, Subcommittee on Antitrust, Commercial and Administrative Law of the Committee on the Judiciary 18 ("Online platforms rarely charge consumers a monetary price—products appear to be 'free' but are monetized through people's attention or with their data. In the absence of genuine competitive threats, dominant firms offer fewer privacy protections than they otherwise would, and the quality of these services has deteriorated over time. As a result, consumers are forced to either use a service with poor privacy safeguards or forego the service altogether.").

5 See, e.g. Complaint, *United States et al. v. Google, LLC*, 1:20-CV-03010 (D.D.C. Oct 20, 2020), https://www.justice.gov/atr/case-document/file/1329131/download ("Most general search engines do not charge a cash price to consumers. … That does not mean, however, that these general search engines are free. When a consumer uses Google, the consumer provides personal information and attention in exchange for search results. Google then monetizes the consumer's information and attention by selling ads."). True or not, the Complaint's allegations are not based on an appeal to the NFLP alone.

6 See, e.g. Jean-Charles Rochet & Jean Tirole, *Platform Competition in Two-Sided Markets*, 1 J. Eur. Econ. Ass'n 990, 994-98 (2003) (showing that profit maximization for a multisided platform involves a joint optimization across all sides rather than on any given side).

This principle of balancing prices across sides is largely independent of the issue of platform market power. A platform with substantial market power may charge high prices overall but will nonetheless balance those prices across sides to best internalize spillover externalities and thereby maximize the gains from network participation. Put differently, a platform with market power faces a tradeoff in its price setting between the extraction of rents from network participation and the extent of that participation; higher overall prices reduce overall participation.

There is an analogy here to the classic microeconomic analysis of profit maximization by a firm, which can be treated as a two-stage process wherein "first" the firm chooses the optimal mixes of inputs to minimize the cost of producing any given level output and "then" chooses the output level to maximize profit. Fundamentally, the analysis applies regardless of the degree of market power the firm may wield.[7] Likewise a platform, whether it has market power or not, can be usefully thought of as "first" choosing an optimal mix of participants on its various sides through relative prices, "then" choosing a magnitude of network participation to maximize profit.

As already noted, some have claimed that a zero-price coupled with data collection in of itself implies that a platform has substantial market power.[8] This is clearly wrong given the analysis above, despite the seductively counterintuitive allure of this claim. It is precisely because consumers have viable alternatives to which they could turn that a platform, regardless of its market power, is impelled to set a low or zero price to them so as to best harvest the valuable spillover benefits consumers bring to the network.

Nor does a zero price on one side imply that a platform must be exercising market power on another side. A two-sided platform facing vigorous competition on both sides may be impelled by that very competition to price below marginal cost on one side and above marginal cost on the other, yielding the platform only a competitive rate of return. In such a setting of vigorous competition, a platform that fails to balance prices in such a way across the two sides would fail to attract the optimal mix of participants and would thereby offer a less attractive network alternative to that of its rivals.

It likewise would be wrong to infer from pricing below marginal cost that a platform is therefore engaging in predation. The example of printed newspapers is illustrative here. The printing and delivery of a newspaper carry significant marginal costs; the subscription rates charged by newspapers in their heyday may well have fallen short of these costs. But having a large circulation generated substantial revenues from advertising, much of it in back of the news tucked away in a "classified" section. This business model of harvesting spillover benefits to advertising through low subscription rates collapsed as alternative outlets for advertising sprang up — along with a reduction in demand from the reader-side.[9] But even to this day some weekly papers continue to be available for free. The NFLP implies only that those papers must be recovering their costs in some other way, begging the question of how. It is the economics of multisided platforms that points to spillover benefits to advertisers as a putative answer to the question.

Summing up the argument on market power thus far: In assessing whether (and the degree to which) a platform has market power, applying the NFLP to the observation of a zero-price service can yield no reliable inference without much more.

Returning now to the related question of whether the observation of a zero-price platform service implies that the consumer is paying for the service in some non-price way, meaning that the consumer is sacrificing something *of value to the consumer*, recall that such an inference cannot be drawn from the NFLP alone. Rather, all can be reasonably inferred from a zero-price service together with the NFLP and an economic presumption of platform rationality is that the platform, in bearing the cost of proving the service, must be doing so in expectation of receiving benefits at least as large as those costs.

The NFLP merely points to the existence of such costs; the expected receipt of countervailing benefits by the platform can be inferred from the platform's rationality as an ongoing concern. The platform's expectation of the *receipt* of non-price benefits from the provision of a zero-price service is distinct from consumers' *payment* for the service in non-price ways. This distinction is commonly lost in debates about platform performance. A platform's receipt of benefits need not equate to a commensurate loss to consumers. As with voluntary trade generally, the transaction of platform services is not a zero-sum game but win-win.

With regard to a platform's collection and use of consumer data, a relevant question is whether this activity imposes a distasteful burden on consumers or redounds to their benefit.[10] Once again, the NFLP alone cannot resolve this question.

7 If a firm has power in the input or output markets, the prices attained in those markets can change with quantities, but the two-step nature of the analysis still holds.

8 See, e.g. *Hearing on Online Platforms and Market Power, Part 3: The Role of Data and Privacy in Competition*, 119th Cong. 4 (2019) (statement of Rohit Chopra, Comm'r. F.T.C.) ("If the internet were truly competitive, people could vote with their feet and select services that offer privacy and anonymity.").

9 See, e.g. Seth Sacher, *Antitrust Issues in Defining Markets in the Newspaper Industry*, Dec. 2, 2011, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1967667.

10 See, e.g. Alessandro Acquisti, Curtis Taylor, & Liad Wagman, *The Economics of Privacy*, 54 J. Econ. Literature 442, 445 (2016) (detailing how "individuals can directly benefit from sharing their data. Advantages can be both psychological…and economic: for instance, personalized services and discounts one receives after joining a merchant's loyalty program; or reduced search costs and increased accuracy of information retrieval one experiences when a search engine tracks them more closely.").

Some consumer surveys indicate that many users of social media place a low value on privacy,[11] which looks to be borne out (revealed preference) by the copious sharing of intimate personal information by many social media users. Such users skew younger, and their preferences with respect to privacy appear to differ from those of their parents and grandparents.[12]

From a paternalistic perspective, it could be argued that platform users should value their privacy more highly, and that therefore government regulation is needed to protect them from themselves. Or, more in line with consumer sovereignty, it might be argued that platform users do value their privacy highly, but are unaware of how much privacy they cede with platform use, or perhaps are deceived into believing the cession is smaller than it is.[13]

This latter perspective might, at best, lend support for a government mandate for fuller disclosure of the privacy policies and effects of platform use, but not restrictions on consumers' rights to choose to cede privacy in exchange for zero-price services.

To repeat, what can be reasonably inferred from zero-price services is that resource expenditures to provide such services are lower than the associated benefits to the platform of widespread adoption by consumers. A principal reason is that the transaction data obtained thereby generates advertising revenue for the platform. Of course, there are different business models as it applies to collecting data. For instance, contrast the approaches that Apple and Facebook take to data collection. Services such as Facebook rely heavily on targeted advertising, and disruptions to the efficacy of that model can lead to significant losses in profit.[14]

Apple, on the other hand, seeks to attract users who value privacy and security and implements features designed to cater to those preferences. Even within advertising, Apple has touted the efficacy of its business model in serving ads that are not based on user-data targeting.[15] There is no one-size-fits-all approach to online data collection, however. This idea is perhaps best illustrated by recent regulatory attempts to give consumers more control over their data, which can ultimately lead to unintended consequences that result in an overall loss in welfare.[16]

But the fact that advertisers highly value information about potential customers, and that this can generate large advertising revenues for platforms, does not settle the question of whether consumers are burdened or benefited by the collection and use of data. A platform user may be akin to a person who accepts an invitation to a free lunch knowing the unpleasant companionship it will entail. Or, contrary to this analogy, consumers may benefit from the use to which data is put. This is an empirical question.

The impact that advertising has on consumer welfare is a complicated question.[17] This is not surprising if we consider the heterogeneity in ad formats and consumer preferences. Further, consumers' receptivity to ads likely depends on the context and circumstance. Nonetheless, the widespread belief that consumers tend to find advertising unpleasant persists. Thus, there is a natural presumption that consumers exposed to ads are effectively putting up with unpleasant companionship as the cost of a free lunch. Even so, and it is not al-

11 See, e.g. Spyros Kokolakis, *Privacy Attitudes and Privacy Behaviour: A Review of Current Research on the Privacy Paradox Phenomenon*, 64 Computers & Security 122 (2017) (detailing some surveys and experiments indicating that users, often contrary to stated preferences, behave in ways that reveal a low valuation for privacy; although, other experiments find contrary results). See also Acquisti et al., *supra* note 10, at 477-78 (presenting various economic explanations as to why there are conflicting studies regarding the existence of a "privacy paradox").

12 See, e.g. Brooke Auxier et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, Pew Research Center, Nov. 15, 2019, https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/ ("[Y]oung adults ages 18 to 29 are more likely than older adults to find acceptable the idea that social media companies monitor users for signs of depression and to allow fitness tracking user data to be shared with medical researchers.").

13 See, e.g. Acquisti et al., *supra* note 10, at 477 ("some individuals may not be aware of the extent to which their personal information is collected and identified online…").

14 For instance, when Apple recently added a "do not track" option to iOS 14.5 (which prevents an app from collecting data once users leave that app), this created a significant, negative impact on Facebook's ad revenues. See, e.g. Michael Simon, *Apple's Simple iPhone Alert is Costing Facebook $10 Billion a Year*, Macworld, Feb. 3, 2022.

15 See, e.g. Chance Miller, *Apple: Most iOS 15 Users Opt Out of Personalized Ads; No Impact on App Store Search Ads Conversions*, 9to5Mac, May 11, 2022, https://9to5mac.com/2022/05/11/ios-15-users-opt-out-of-personalized-ads/ ("[D]ata from Apple indicates that the average conversion rate between users with personalized ads enabled and personalized ads disabled is nearly identical. For customers who opted in to personalized ads, advertisers see a 62.1 percent conversion rate. Among users with personalized ads disabled, that conversion rate is 62.5 percent.").

16 For example, the EU's General Data Protection Regulation ("GDPR") was passed with great promise. Yet, after two years, evidence is beginning to emerge indicating it has harmed consumers. See, e.g. Rebecca Janßen et al., *GDPR and the Lost Generation of Innovative Apps*, NBER Working Paper No. 30028, May 2022, http://www.nber.org/papers/w30028 at 2 ("Whatever the benefits of GDPR's privacy protection, it appears to have been accompanied by substantial costs to consumers, from a diminished choice set, and to producers from depressed revenue and increased costs.").

17 See, e.g. Gary S. Becker & Kevin M. Murphy, *A Simple Theory of Advertising as a Good or Bad*, 108 Q.J. Econ. 941 (1993).

ways clear that this is the case,[18] the data collected may deliver better targeted ads and so may not be a net harm to consumers for several reasons.

First, ads targeted to interested consumers are less burdensome, more salient, and more valuable to those consumers. Targeted advertising is a substitute for consumer search, economizing on search costs. Likewise, within an online marketplace, data collected by the platform can ease the time costs consumers face in searching for products matching their preferences and tends to improve the quality of the match. Consequently, data collection and its subsequent use can materially improve the quality of a product for each consumer. Targeted advertising, and the data collection and use that may facilitate it, could be a benefit rather than a burden to consumers. The issue, once again, is ultimately empirical.

In conclusion, let us return to the purported origin of the NFLP phrase: tavern owners offering free lunch to drinkers.[19] While the resources required to provide lunch at taverns are anything but free, there is little basis to believe that tavern patrons who enjoy the free lunch are somehow "paying for it" — in the sense they are giving up something of value for the lunch. The free lunch, in this case, is better thought of as an expense to bring in patrons, have them interact, and stay a while. The end goal is to serve more ale. Similarly, a platform's end goal in offering zero-price services is, at least in part, to attract consumers to the network and serve more profitable ads. But whether consumers are burdened or benefited by the uses to which data is put, and the degree to which the modern-day platform analogues to the tavern keepers of old have market power—these are fact intensive and economics intensive questions, the resolution of which requires a rolling up of the sleeves. There is no free lunch in antitrust analysis.

18 See, e.g. Navdeep S. Sahni & Charles Zhang, *Are Consumers Averse to Sponsored Messages? The Role of Search Advertising in Information Discovery*, Mar. 2022, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3441786 ("Taken together, patterns in our data are consistent with a constructive role of search advertising where advertising fills significant information gaps by conveying new information, which is difficult for the search engines to gather and therefore missed by their organic algorithms. On average, viewing search ads makes consumers better off at the margin we study.").

19 See *supra* note 2.

“FOR THE PUBLIC BENEFIT”: WHO SHOULD CONTROL OUR DATA?

BY SARIT MARKOVICH & YARON YEHEZKEL[1]

1 Kellogg School of Management, Northwestern University (s-markovich@kellogg.northwestern.edu). and Coller School of Management, Tel Aviv University (yehezkel@tauex.tau.ac.il)., respectively.

I. INTRODUCTION

Many platforms base their business model on the commercialization of their users' data. For example, search engines, such as Google, can collect data on users' location and keyword search. Navigation apps, such as Waze, can collect data on users' preferred routes and other driving habits. Media streaming platforms, such as Spotify, Pandora, and Deezer can collect data on users' music preferences and listening habits. Wearables, such as Fitbit, Garmin, and Samsung Watch can collect data on users' sport activities and performances. These platforms can then use the data to improve their services, but at the same time, the data can also be used for commercial purposes such as selling it to advertisers or to other third-party providers.

This raises the question of who should own the property rights over users' data? Specifically, who should have the right to decide which data items to collect and which to commercialize? On the one hand, the platform is the party that collects and analyzes the data, and users give their consent to data collection when joining the platform. In fact, it is the platform that turns the data into a valuable resource. On the other hand, users are the party that generates the data, and in many cases, bear a disutility from having their data shared. Furthermore, users typically do not have the choice to join the platform without agreeing to give away the rights over their own data.

This question has important implications for the ongoing debate on the need for data regulation. Existing U.S. laws give the property right over data to the entity that collects it. Platforms can collect and own users' data on the basis of users' consent to join the platform.[2]

Yet, when platforms have strong market power, users' voluntary consent to the platform's data policy is controversial. For example, in 2020, the U.S. Department of Justice filed a suit against Google, claiming (among other things) that "American consumers are forced to accept Google's privacy practices, and use of personal data..."[3]

Another case in point is Facebook's questionable announcement in 2021, that its users must agree to let Facebook and its subsidiaries collect their personal data on WhatsApp, including phone numbers and locations. In an extension to competing platform, preliminary results show that platforms may choose different data policies. The platform that benefits from a leading position in the market chooses to control the data while the new platform enables users that join it to control their data.

If users don't accept the new terms and conditions, they will be forced out of the app.[4] This is especially interesting given that WhatsApp has always positioned itself as a privacy focused service – encrypting all users' messages. Indeed, WhatsApp potentially has access to a lot of its users' data – phone number, contact lists, messages' content. Its intention to keep encrypting messages and not sharing this data while sharing other data items, like phone number and location, suggests that WhatsApp believes that users' disutility from sharing phone number information with Facebook is lower than their disutility from sharing messages content.[5]

In contrast to the U.S., the EU General Data Protection Regulation ("GDPR") is designed to provide users with the choice to share data; a choice that does not discriminate those that choose not to share data. The GDPR aims to move platforms from a regime that provides the platform with full control over users' data, to a regime that enables users to join a platform and enjoy, at least part of, its services without being required to give their consent to share specific data.

This paper examines the above research question using a theoretical model. We find that whether a regime that gives the platform control or a regime that gives users control over their data is welfare enhancing depends on market conditions such as the type of consumers' heterogeneity, as well as what we refer to as the public benefit of data (on which we elaborate below). We therefore argue that it is not necessarily the case that giving users control over their data is beneficial. Instead, regulating data-driven platforms should be on a one-to-one basis, depending on the dominant platform and market conditions. Below, we describe our theoretical model and findings which identify the market conditions under which it is beneficial to impose a regime that provides users control over their data. We further explain the results and intuition behind them. We conclude with some policy implications.

---

2 See Economides, Nicholas, & Ioannis Lianos. "Restrictions on Privacy and Exploitation in the Digital Economy: A Market Failure Perspective." *Journal of Competition Law and Economics* (forthcoming).

3 See: *The Verge*, Oct 20, 2020. Available at https://www.theverge.com/2020/10/20/21454192/google-monopoly-antitrust-case-lawsuit-filed-us-doj-department-of-justice.

4 See, for example, *The Verge*, Feb 22, 2021. Available at https://www.theverge.com/2021/2/22/22294919/whatsapp-privacy-policy-may-15th-messaging-calls-limited-functionality.

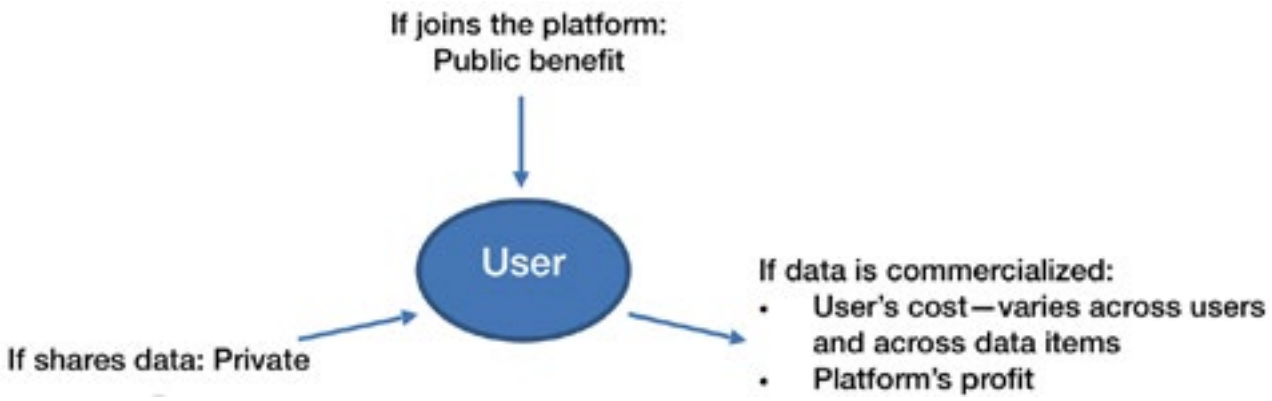
5 See: *The Verge*, Oct 20, 2020. Available at https://www.theverge.com/2020/10/20/21454192/google-monopoly-antitrust-case-lawsuit-filed-us-doj-department-of-justice.

II. THE BENEFITS AND COST OF DATA

Our research considers a game between users and a platform (or competing platforms) that collect and can commercialize users' data. The platform collects multiple *data items*. For example, Waze collects data on location, time, and route that users take; Fitbit collects data on the number of steps its users take and their heart rate; and Facebook collects data on text and photos users upload as well as posts they read, the people and groups they follow, etc. Each data item provides three potential benefits:

1. **Private benefit for users**. For example, if users share data on their number of steps and heart rate with a fitness tracker, the platform can help these users to monitor their training and provide them with recommendations concerning more effective training. Likewise, when a driver uses a navigation app and agrees to let the app track their route, the data collected can help direct the driver to un-congested routes.
2. **Commercial benefits**. The same data provides the platform with *commercial benefit*. The fitness tracker or navigation app, in our example, can sell the user's data to advertisers. Users, however, bear disutility from having their data shared for commercial benefits. This disutility may differ across users. For example, some users are more sensitive to their privacy than others. Moreover, this disutility may differ across data items. For example, users may not care about Waze sharing information about the route they take but suffer disutility from Waze sharing their exact location at a specific point in time. Similarly, users' disutility from Fitbit sharing one's number of daily steps may be lower than that of sharing their heart rate.
3. **Public benefits**. The novel feature of our model is that the data may also benefit all other users that join the platform, regardless of whether they share their data — i.e. provide a *public benefit*. For example, the data collected by a fitness tracker from an individual user can help the fitness tracker provide better training recommendations to all other users. Fitbit's uses its heart rate data to identify episodes of irregular heart rhythm suggestive of atrial fibrillation ("AFib"), the most common form of heart rhythm irregularity. Fitbit intends to use this information to alert users about an irregular heart rhythm so that notified individual would connect with a doctor. Likewise, data collected from a driver can benefit other drivers that consider taking the same route. Other relevant examples are users that provide their location data on a contact-tracing app benefit others who now know they were in proximity of someone who tested positive for COVID-19. Contact tracing apps use one's phone, or other mobile device, to track and alert individual if they'd crossed paths with someone who within a certain window of time tested positive to COVID-19.[6] This third public benefit of data is the most important one for innovation and product improvement, as it implies that data creates positive externalities where users can benefit from other users' data, regardless of whether they share data themselves. Figure 1 below summarizes the different benefits and costs to the user and the platform:

Figure 1: Benefits and Costs of Data



To study who should control users' data, we study three extreme data regimes. In the first regime (hereafter, "regime 1"), the platform has the right to decide which data items to collect and commercialize. Users who want to join the platform must consent to sharing the data items the platform chooses to collect and commercialize. That is, users can only decide whether to join the platform (and agree to its data policy), or stay out. The second regime (hereafter, "regime 2") does not allow the platform to contingent users' participation in the platform with their consent to collect their data. The third regime (hereafter, "regime 3") does not allow the platform to contingent users' participation or data collection on their consent to the commercialization of their data. In this case, in order to incentivize users to allow the platform to commercialize their data, we allow the platform to compensate users for selling their data.

6 Contact tracing apps use one's phone, or other mobile device, to track and alert individual if they'd crossed paths with someone who within a certain window of time tested positive to COVID-19.

We find that the different benefits of data create market inefficiencies. The platform only cares about the commercial benefit, and will thus collect data as to maximize this benefit, subject to the constraint that users agree to join it. Users only care about their own private benefit. If given the opportunity to decide which data to provide the platform, users would only provide data that offers them private benefit, as they enjoy the public benefit regardless of their data contribution. Most ill-considered, however, is the public benefit of data. Although it provides benefits to all on the platform, the public benefit is, at least partially, ignored by both the platform and the users. That is, both parties ignore that while data collected on an individual user may create a disutility for this user, it may benefit the platform's entire user-base. These market inefficiencies raise the question of which regime achieves the best balance between the benefits of data (public, personal, and commercial) and disutility to users, as well as whether competition can mitigate these market inefficiencies. We find that giving users full control over their data is not always welfare enhancing, as it may result in too little data collected for the public benefit.

III. USER OR DATA COVERAGE?

In general, the platform's optimal strategy can take one of three possible outcomes: all data is commercialized but not all users join (i.e. full data coverage but partial user coverage) as some users' disutility from the commercialization of their data is higher than the benefits from joining the platform ; all users join but not all data is commercialized (full user coverage and partial data coverage) as some data items exhibit high commercialization disutility; or partial user and data coverage. As it turns out, our results and intuition crucially depend on whether the market is mostly characterized by data coverage or user coverage, which further depend on whether the market is mostly characterized by users with different disutility from the commercialization of their data (hereafter, "heterogeneous users"), or by data items that differ in the disutility that commercializing them inflicts on users (hereafter, "heterogeneous data items").

Consider first the case of heterogeneous users. In this case, if data does not have any public benefit, regime 1 and regime 2 are identical. When the public benefit of data is positive, in comparison with regime 2 where users control their data, regime 1 that gives the platform control over data has the disadvantage that fewer users join the platform. This is because users that are sensitive to their privacy prefer not join the platform over the possibility of joining and adhering to the platform's strict data sharing policy. At the same time, regime 1 has the advantage that all users who join the platform give all data requested by the platform, which then provides public benefit. That is, there is a tradeoff between the number of users that join the platform and enjoy the public benefit and the amount of data collected which thereby provides public benefit.

We find that when the public benefit per data collected is small, the first effect dominates and since more users join the platform under regime 2, it is welfare enhancing to give users control over their data. As the public benefit of data increases, more users join the platform under regime 1, because they would like to enjoy the public benefit of data. That is, users compare their costs to the sum of the private benefit and the public benefit rather than just to the private benefit (see Figure 1). As a result, the disadvantage of regime 1 decreases while the advantage of regime 1 becomes stronger. Consequently, when the public benefit of data is high, it is welfare enhancing to give the platform control over data. These results highlight the important role the public benefit of data plays when evaluating data regulation.

Interestingly, the opposite conclusion emerges in the case of homogeneous users and heterogeneous data items. In this case, it is welfare enhancing to let the platform control the data when the public benefit of data is low, while giving the users control on their data is welfare enhancing only when the public benefit of data is high. The intuition for this result is that when users are homogeneous, under both regimes 1 and 2 all users join the platform. Recall that under regime 2 users can enjoy the public benefit regardless of whether they share their data. It follows that, under regime 2, the platform can only commercialize data items that provide users with high private benefit, because otherwise users will not agree to share these data items. Yet, under regime 1, the platform can "bundle" data items with low disutility and some data items with high disutility because data items with disutility that is smaller than the private benefit leave positive surplus for users. The platform, then, can force users to agree that the entire "bundle" of data items is commercialized, or they stay out of the platform. That is, relative to regime 2, under regime 1, the platform can collect more data for commercial benefit. As the public benefit of data increases, regime 1 enables the platform to bundle even more data items with high disutility, which makes regime 1 less beneficial to welfare in comparison with regime 2. Notice that this is in contrast to the case of heterogeneous users, where welfare is higher under regime 1 when the public benefit of data is high. Table 1 summarizes the comparison between the two regimes under heterogeneous users and data, and the differences in intuition between the two cases.

Table 1: Comparison Between Heterogeneous Users and Data

Type of Heterogeneity	The main problem with regime 1 (in comparison with 2)	Effect of an increase in the public benefit of data	Result
Heterogeneous Users	Partial user coverage: "Sensitive" users do not join	An increase in the public benefit mitigates this problem because it attracts more users to join	For high public benefit, welfare in regime 1 is higher than in regime 2
Heterogeneous data	Partial data coverage: too much data is commercialized: the platform "bundles" data	An increase in public benefit exacerbates this problem because the platform can bundle more costly data items	For high public benefit, welfare in regime 1 is lower than in regime 2

We also examine the case where the market exhibits both heterogeneities together — i.e. users differ in their disutility from the commercialization of their data and data items differ in the disutility their commercialization imposes. We find that, if the public benefit of data is small, the platform focuses on user coverage. Once the user market is fully covered, the platform turns its focus to commercializing more data items. That is, with both heterogeneities, if the public benefit of data is low, welfare dynamics follows the dynamics in the "heterogenous users" case. As the public benefit of data increases, all users join the platform and welfare dynamics follows the dynamics in our heterogenous data case.

IV. COMPETITION

To study whether competition motivates platforms to adopt the welfare maximizing data regime as well as whether regulating data collection can facilitate entry, we extend our analysis to competition between two platforms: an incumbent platform that benefits from a "focality" advantage — users expect other users to join the incumbent. The second platform is an entrant that suffers from a non-focal position, yet can offer a better base quality due to innovative new features. Our results show that competition does not necessarily motivate platforms to give users control over their data. Furthermore, competition does not necessarily motivate either platform to choose the welfare-maximizing regime. Nevertheless, the entrant has stronger incentives than the incumbent to give users control over data and may choose to do so when doing this enables it to overcome its non-focal position. Specifically, an entrant may choose to give users control over their data as a tool to differentiate itself and strengthen its market position.

V. COMPENSATING USERS FOR THEIR DATA

Finally, we analyze the third regime which in essence provides users with all the control over their data: the platform needs to ask users for their consent to collect and to commercialize the data. A user may agree to collecting the data for private and public benefit, yet require monetary compensation in order to agree to have the data commercialize. While one would expect such a regime to lead to the first best, we find that this regime is not always welfare enhancing. While under this regime all users join and share data for public and private benefits, since the platform needs to pay users for agreeing to share data for commercial benefit, the platform may choose to collect too little data.

The advantage of requiring the platform to compensate users for their data is that the platform internalizes users' disutility from the commercialization of their data. Under heterogeneous data, this leads to the first best. Under heterogeneous users, however, since the platform cannot discriminate across users — i.e. pay more to users with higher disutility — the platform under-collects data for commercial benefit. In this case, this regime may underperform the first two regimes that we consider, especially when the commercial and public benefits of data are high.

VI. POLICY IMPLICATIONS

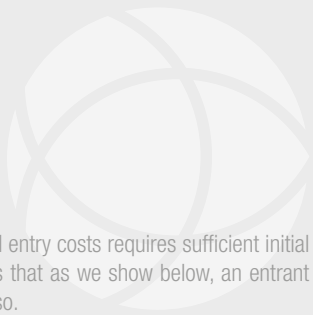
Our results suggest that whether the EU's firmer approach to data regulation as compared to the U.S. enhances welfare, depends on the magnitude of the public benefit of data and the type of heterogeneity in the market. More generally, our paper provides specific conclusions on how to regulate dominant data-driven platforms. When data have significant public benefits and the market is characterized by heterogeneous users, such that users that are relatively sensitive to privacy prefer to stay out, the regulator should not intervene in the platform's data policy. In this case, regulation will result in fewer users giving data for public benefit and may eventually reduce consumer surplus as well as social welfare.

When the market is characterized by mostly homogeneous users and is almost fully covered, regulation that requires the dominant platform to give users control over data can enhance social welfare.[7]

We focus on platforms that do not have high fixed entry costs into a new market. Naturally, a new platform that needs to cover its fixed entry costs requires sufficient initial profits. Hence, regulating the data policy of such new platforms may deter entry. Another argument against regulating a new platform is that as we show below, an entrant platform may independently choose to give users control over data in order to gain a foothold in the market, if the incumbent does not do so.

Lastly, we want to emphasize that the question of who should control our data is also – perhaps foremost – an ethical question of social morality. Is it ethical to allow a platform to collect our personal data items? The moral aspects of this question are important but are beyond the scope of our theoretical model. The goal of our research is to contribute to the debate on data regulation by highlighting some economic forces, specifically, with regards to the public benefit of data. Our results and potential policy implications cannot be placed in isolation from a discussion on the moral aspects of privacy and data protection.

In a somewhat related moral debate in Israel, the question is whether to allow public authorities share information concerning the identity of civilians that did not receive the COVID vaccine. Such data may have valuable public benefit in fighting COVID, yet may violate civilians' privacy rights.



7 We focus on platforms that do not have high fixed entry costs into a new market. Naturally, a new platform that needs to cover its fixed entry costs requires sufficient initial profits. Hence, regulating the data policy of such new platforms may deter entry. Another argument against regulating a new platform is that as we show below, an entrant platform may independently choose to give users control over data in order to gain a foothold in the market, if the incumbent does not do so.

MINIMIZING PRIVACY RISKS IN REGULATING DIGITAL PLATFORMS: INTEROPERABILITY IN THE EU DMA

BY MIKOŁAJ BARCZENTEWICZ[1]

1 Senior Scholar, International Centre for Law and Economics; Senior Lecturer and Research Director, University of Surrey Law and Technology Hub; Fellow, Stanford Law School. This paper is based on my working paper *Privacy and Security Implications of Regulation of Digital Services in the EU and in the US*, Stanford–Vienna Transatlantic Technology Law Forum, TTLF Working Papers No. 84 (2022).

I. INTRODUCTION

It is notoriously difficult to use the law to *strengthen* information privacy and security, even where that is the explicit goal of legislation. Thus, perhaps the least we should expect of the law is not to unintentionally weaken the level of privacy and security. Unfortunately, pursuing even seemingly unrelated policy aims may sometimes yield that negative effect. Here, I analyze some of the provisions included in the proposed EU Digital Markets Act ("DMA").[2] The DMA purports to benefit consumers and improve the competitiveness of digital markets. It is likely to have negative and unaddressed consequences, however, in terms of information privacy and security.

For brevity, I chose to focus on one regulatory solution: interoperability mandates in the DMA. I conclude that only one of those obligations — on the interoperability of messaging services — is accompanied by a potentially adequate safeguard: a requirement that any third-party service must offer at least the same level of user security as the original service. This is a very demanding standard, which may render the interoperability provision a dead letter for the foreseeable future, but which nonetheless offers welcome benefits from the consumer perspective. The remaining obligations that I analyze are accompanied either by no safeguards, or by insufficient safeguards.

II. INTEROPERABILITY

Interoperability[3] increasingly is put forward as a potential solution to some of the problems associated with digital services generally, and with large online platforms, in particular.[4] For example, interoperability might allow third-party developers to offer different "flavors" of social-media news feeds, with varying approaches to content ranking and moderation. Were this approach to take hold, it might render the specific content-moderation decisions made by Facebook or other platforms less central to the user experience. Facebook users could choose alternative content moderators, delivering the kind of news feed that those users desire or expect.[5]

The concept of interoperability is popular not only among thought leaders, but also among legislators. The DMA includes interoperability mandates, as do federal bills introduced in the United States by Rep. Mary Gay Scanlon,[6] Rep. David Cicilline,[7] and Sen. Amy Klobuchar.[8]

A. Privacy and Security Risks of Interoperability

At the most basic level, in the context of digital services, interoperability refers to the capacity to exchange information between computer systems. Email is an example of an interoperable standard that most of us use today. It is telling, however, that supporters of interoperability mandates point to services like email as their model examples. Email (more precisely, the SMTP protocol) originally was designed in a notoriously insecure way.[9] It is a perfect illustration of the opposite of privacy-by-design.[10] As originally conceived, email offered roughly the

2 *Proposal for a Regulation of the European Parliament and of the Council on Contestable and Fair Markets in the Digital Sector* ("Digital Markets Act"). Most recent publicly available version from 11 May 2022 is available at https://www.consilium.europa.eu/media/56086/st08722-xx22.pdf.

3 This section builds on my previous short text *The Digital Markets Act Shouldn't Mandate Radical Interoperability*, Truth on the Market (19 May 2021) https://truthonthemarket.com/2021/05/19/the-digital-markets-act-shouldnt-mandate-radical-interoperability.

4 Stephen Wolfram, *Testifying at the Senate About A.I.-Selected Content on the Internet*, Stephen Wolfram's Writings (25 Jun. 2019) https://writings.stephenwolfram.com/2019/06/testifying-at-the-senate-about-a-i-selected-content-on-the-internet/; Mike Masnick, *Protocols, Not Platforms: A Technological Approach to Free Speech*, Knight First Amendment Institute (21 Aug. 2019) https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech; Daphne Keller, *If Lawmakers Don't Like Platforms' Speech Rules, Here's What They Can Do About It. Spoiler: The Options Aren't Great,* Techdirt (9 Sep. 2020) https://www.techdirt.com/articles/20200901/13524045226/if-lawmakers-dont-like-platforms-speech-rules-heres-what-they-can-do-about-it-spoiler-options-arent-great.shtml; Francis Fukuyama, *Making the Internet Safe for Democracy*, 32 J. Democr. 37 (2021) https://www.journalofdemocracy.org/articles/making-the-internet-safe-for-democracy.

5 Of course, this may have its own negative consequences in strengthening "filter bubbles" and fueling polarization.

6 H.R. 3849, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/3849.

7 H.R. 3816, 117th Congress (2021-2022), https://www.congress.gov/bill/117th-congress/house-bill/3816.

8 S. 2992, 117th Congress (2021-2022). https://www.congress.gov/bill/117th-congress/senate-bill/2992.

9 See. e.g. Durumeric et al, *Neither Snow Nor Rain Nor MITM… An Empirical Analysis of Email Delivery*, Security Proceedings of the 2015 Internet Measurement Conference (2015).

10 See Article 25 of the Regulation (EU) 2016/679 (General Data Protection Regulation).

same levels of privacy and security as a postcard message sent without an envelope that passes through many hands before reaching the addressee. Even today, email continues to be a source of security concerns due to its prioritization of interoperability.[11]

Using currently available technology to provide alternative interfaces or moderation services for social-media platforms, third-party developers would have to be able to access much of the platform content potentially available to a user. This would include not just content produced by users who explicitly agree to share their data with third parties, but also content — e.g. posts, comments, likes — created by others who may have strong objections to such sharing. It does not require much imagination to see how, without adequate safeguards, mandating this kind of information exchange would inevitably result in something akin to the 2018 Cambridge Analytica data scandal.[12]

Imposing a legal duty on digital service providers to make their core services interoperable with any third party creates, as noted by Cory Doctorow and Benedict Cyphers, at least three categories of risks:

1. Data sharing and mining via new APIs;
2. New opportunities for phishing and sock puppetry in a federated ecosystem; and
3. More friction for platforms trying to maintain a secure system.[13]

1. Friction in Ensuring Security

Bearing in mind Doctorow & Cyphers' last point, a crude interoperability mandate could make it much more difficult for service providers to keep up with the fast-evolving threat landscape. For example, it may seem a good idea to require service providers to submit all changes to their interoperability standards (interfaces) for external review, possibly by a public authority. This could potentially help to ensure that service providers do not "break" interoperability or discriminate against some third-party services that would want to benefit from it. However, imposing such a requirement would introduce delay in responding to new threats, potentially putting user data at risk. When it can take just seconds to exfiltrate millions of user profiles, delaying security patches by weeks or even days through regulation is unacceptable.

2. "Phishing and Sock Puppetry"

True interoperability of digital services would mean a two-way exchange of information. For online platforms like social networks, this would mean that, e.g. a Facebook user could interact with users of other interoperable platforms as if they were also Facebook users (exchange direct messages, see their posts, add comments and so on). Doctorow & Cyphers recognized that this would mean that any identity controls (e.g. Facebook's requirement to use real names) could easily be undermined if criminals or state actors run or control their own interoperable platforms. Those in control of such a platform could appear to users of other platforms as their friends in an attempt to hack them (e.g. phishing through direct messages). Such deception already happens on major online platforms, but those platforms are legally free to adopt measures to counteract it. A broad interoperability mandate would disallow service providers from vetting other providers and from imposing their own identity requirements (e.g. requiring the use of real names).

Those risks are well-illustrated by how often users are victimized through one of the most widely used interoperable protocols: telephony and, in particular, telephone numbers.[14] Due to design choices in interoperability of telephony systems, which entirely sidelined security concerns, it is often trivial for any malicious actor to "spoof" the number that appears in a call recipient's "caller ID" feature. They may thus to appear to a victim as if they are calling from, e.g. the victim's bank. Having created an insecure-by-design system that facilitated widespread consumer harm, regulators are slowly and, to date, ineffectively playing catch-up.[15]

11 See, e.g. Sydney Li, A Technical Deep Dive into STARTTLS Everywhere, Electronic Frontier Foundation (25 Jun. 2018) https://www.eff.org/deeplinks/2018/06/technical-deep-dive-starttls-everywhere.

12 On the Cambridge Analytica scandal, see, e.g. *Investigation into Data Analytics for Political Purposes*, UK Information Commissioner, https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes.

13 Cory Doctorow & Benedict Cyphers, *Privacy Without Monopoly: Data Protection and Interoperability*, Electronic Frontier Foundation (12 Feb. 2021) https://www.eff.org/wp/interoperability-and-privacy.

14 See e.g. Jovi Umawing, More than a Quarter of Americans Fell for Robocall Scam Calls on Past Year, Malwarebytes (1 Jun. 2022) https://blog.malwarebytes.com/reports/2022/06/more-than-a-quarter-of-americans-fell-for-robocall-scam-calls-in-past-year.

15 *Ibid.*

3. General Data-sharing Risks

Effective interoperability requires sharing of sensitive data among different service providers through new two-way real-time interfaces ("APIs"). Doctorow & Cyphers put forth a plan endorsing broad interoperability mandates,[16] but admirably, they acknowledge the important security and privacy tradeoffs such a mandate would impose. Promoters of the bills analyzed herein frequently do not account for such costs. It is therefore worth analyzing these harms from the perspective of proponents of interoperability mandates. Doctorow & Cyphers are open about the scale of the risk: "[w]ithout new legal safeguards to protect the privacy of user data, this kind of interoperable ecosystem could make Cambridge Analytica-style attacks more common."[17]

The Cambridge Analytica incident illustrates the risks well. The personal data that Cambridge Analytica ultimately used was collected through a Facebook app created by an academic researcher.[18] The app was used by 270,000 people, who expressly granted permission for the app to access their account information, including information about their Facebook contacts. This is how the app's author collected data on more than 50 million Facebook users.

A potential future Cambridge Analytica could benefit from a poorly drafted interoperability mandate. Today, Facebook can and does stop third-party developers who try to exfiltrate data from the platform in violation of the company's terms. Some even believe that Facebook does so too vigorously.[19] But under an interoperability mandate, Facebook may be prevented from vetting and denying access to third parties if a user clicks "yes" in a consent popup. And users may habitually click "yes" in consent popups, irrespective of any "dark patterns" that would nudge them to authorize the desired action ("popup fatigue").[20] This is understandable: users may simply want to access the desired functionality (e.g. to play a game) and may not be willing to invest sufficient time and effort to parse the consequences of what, exactly, they are authorizing.

Thus, one risk is that users will authorize interoperability to an extent that may later surprise them, even if the third-party service providers provide all necessary information in an accessible and intelligible form. It may just be that users will only start caring about the consequences of their choices once they materialize, not before they make a choice.

It is, however, unrealistic to expect all third-party service providers to obey the rules, including rules stipulating that one should act in accordance with unstated user expectations. Some third-party providers may act in good faith when they push the boundaries of what is permitted, due to the (potentially erroneous) belief that users are better served in some particular way. But some will intentionally engage in illegal — even criminal — activity.[21] Such actors may come from foreign jurisdictions (outside of the EU and the United States), which could render *ex post* enforcement of legal rules against them particularly difficult.

B. How can the Risks be Addressed?

What could be done to make interoperability reasonably safe? There are several constraints that an acceptable solution should address.

1. Constraints

First, solutions should be targeted at users of digital services as the really exist, without assuming away some common but inconvenient characteristics. In particular, solutions should not assume unrealistic levels of user interest or technical acumen. As discussed above, users may not

16 *Supra* note 13.

17 *Supra* note 13, at 28.

18 See also Kurt Wagner, *Here's How Facebook Allowed Cambridge Analytica to Get Data for 50 Million Users*, Vox (17 May 2018) https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data.

19 Mitch Stolz & Andrew Crocker, *Once Again, Facebook Is Using Privacy As A Sword To Kill Independent Innovation*, Electronic Frontier Foundation (20 Nov. 2020) https://www.eff.org/deeplinks/2020/11/once-again-facebook-using-privacy-sword-kill-independent-innovation.

20 See, e.g. Cristian Bravo-Lillo et al., *Harder to Ignore? Revisiting Pop-Up Fatigue and Approaches to Prevent It*, Proceedings of the 10th Symposium On Usable Privacy and Security (2014); Anthony Vance et al., *Tuning Out Security Warnings: A Longitudinal Examination of Habituation Through fMRI, Eye Tracking, and Field Experiments*, 42 Management Information Systems Quarterly (MISQ) 355 (2018).

21 As the Organisation for Economic Co-operation and Development (OECD) noted: "Even where individuals and organisations agree on and consent to specific terms for data sharing and data re-use, including the purposes for which the data should be re-used, there remains a significant level of risk that a third party may intentionally or unintentionally use the data differently." *Enhancing Access to and Sharing of Data. Reconciling Risks and Benefits for Data Re-use Across Societies*, Organisation for Economic Co-operation and Development (2019), chapter 4, Risks and challenges of data access and sharing." https://www.oecd-ilibrary.org/sites/15c62f9c-en/index.html?itemId=/content/component/15c62f9c-en.

demonstrate concern about privacy and security settings *until* some negative consequences materialize from authorized interoperability. It is telling that mandate proponents tend to invoke as models for interoperability those digital services that are used by exceptionally motivated and informed users, which also tend to be small-scale (e.g. Mastodon) or have unacceptably poor usability for most of today's Internet users (e.g. Usenet).[22]

Second, solutions must address the issue of effective enforcement. Doctorow & Cyphers argued that there is a "need for better privacy law" to make interoperability safe.[23] Somewhat surprisingly, however, Doctorow wrote soon after that "the existence of the GDPR *solves* the thorniest problem involved in interop and privacy."[24] But problems can be solved by legislation only if such legal rules are followed; this requires addressing the problem of procedures and enforcement.

The current EU framework and enforcement of privacy law offers little confidence that misuses of broadly construed interoperability would be detected and prosecuted, much less that they would be prevented.[25] This is especially true for smaller and "judgment-proof" rule-breakers, including those from outside the European Union. In the United States, no such privacy framework exists, as yet, on the federal level; state laws like California's Consumer Privacy Act face enforcement problems similar to the EU GDPR.[26]

When digital service providers are placed under a broad interoperability mandate with non-discrimination provisions (preventing effective vetting of third parties, unilateral denials of access, etc.), the burden placed on law enforcement is mammoth. It could take just one bad actor — perhaps working from Russia or North Korea — to take advantage of interoperability mandates in order to exfiltrate user data or to execute a hacking (e.g. phishing) campaign, causing immense damage. Of course, such foreign bad actors would be in violation of the EU GDPR, but that is unlikely to have any practical significance.

It would not be sufficient to allow (or require) service providers to enforce merely technical filters, such as a requirement to check whether the interoperating third parties' IP addresses are located in jurisdictions with sufficient privacy protections. For motivated bad actors, evading such technical limitations does not pose significant difficulty.

2. The Open Banking Solution

One solution that might potentially address the information privacy and security concerns in interoperability of digital services, without significant technological changes, would be to follow the example of the UK Open Banking regime.[27] As described by the United Kingdom's Competition and Markets Authority:

Open Banking enables consumers and small and medium-sized enterprises ("SMEs") to share their bank and credit card transaction data securely with trusted third parties who are then able to provide them with applications and services which save time and money.[28]

Open Banking was introduced in 2017 and is a heavily regulated interoperability scheme with its own special oversight body — the Open Banking Implementation Entity (OBIE). According to Geoffrey Manne & Sam Bowman, one of the key lessons from Open Banking is that:

---

22 "mastodon" https://github.com/mastodon/mastodon; https://en.wikipedia.org/wiki/Usenet.

23 *Supra* note 13, at 33.

24 Cory Doctorow, *The GDPR, Privacy and Monopoly*, Electronic Frontier Foundation, (11 Jun. 2021) https://www.eff.org/deeplinks/2021/06/gdpr-privacy-and-monopoly.

25 See e.g. *Communication from the Commission to the European Parliament and the Council*, "Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation" COM(2020) 264, 24 Jun. 2020, available at https://ec.europa.eu/info/sites/default/files/1_en_act_part1_v6_1.pdf; *The Long and Winding Road: Two Years of the GDPR: A Cross-Border Data Protection Enforcement Case from a Consumer Perspective*, Bureau Européen des Unions de Consommateurs (5 Aug. 2020) available at https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf.

26 An apparently credible legislative proposal for a U.S. federal privacy statute was released for discussion in June 2022 by a bipartisan group of members of the House of Representatives and of the Senate. See *House and Senate Leaders Release Bipartisan Discussion Draft of Comprehensive Data Privacy Bill*, U.S. House Committee on Energy and Commerce (3 Jun. 2022) https://energycommerce.house.gov/newsroom/press-releases/house-and-senate-leaders-release-bipartisan-discussion-draft-of.

27 On Open Banking, see, e.g. *Open Banking*, Open Banking Implementation Entity, https://www.openbanking.org.uk; Sam Bowman, *Why Data Interoperability Is Harder Than It Looks: the Open Banking Experience*, CPI Antitrust Chronicle (April 2021) available at https://laweconcenter.org/wp-content/uploads/2021/06/CPI-Bowman.pdf; Geoffrey A. Manne & Sam Bowman, *Issue Brief: Data Portability and Interoperability: The Promise and Perils of Data Portability Mandates as a Competition Tool*, International Center for Law & Economics (10 Sep. 2020) https://laweconcenter.org/resource/issue-brief-data-portability-and-interoperability-the-promise-and-perils-of-data-portability-mandates-as-a-competition-tool.

28 *Update on Open Banking*, Competition and Markets Authority (5 Nov. 2021) https://www.gov.uk/government/publications/update-governance-of-open-banking/update-on-open-banking.

Open Banking has been costly and time-consuming to implement. This is despite the fact that the data involved — chiefly transaction history and account balance data — is relatively simple and does not differ between different banks. The main difficulties have been around security, user authentication, and the authorization of new third-party services, and it has taken ongoing monitoring by a new agency set up by the CMA and several re-iterations to get these right, and may require more in the future. For services where the data is more sophisticated and unique to each service, the cost of implementing data portability and/or interoperability may be commensurately higher.[29]

Applying the lessons from Open Banking to digital services could mean that:

1. There would likely be a need for a regulator to set technical standards, oversee the scheme, and possibly to enforce the rules in case of violations.
2. To be able to participate, any potential interoperating party would have to undergo expensive and thorough regulatory vetting (of the kind that financial institutions need to be allowed to operate).

Among the main problems with applying the Open Banking model to digital services is that Open Banking applies to relatively simple and homogenous data (i.e. bank transactions), whereas the digital services offered by the largest providers are much more varied and continuously evolve. Imposing the kinds of detailed technical data standards used in Open Banking would stifle innovation in digital services. Given that some standardization of data formats is likely to be a feature of any interoperability mandate, this may be sufficient reason not to adopt an interoperability mandate, but that issue is beyond the scope of this paper.

Requiring all participating parties to undergo regulatory approval, as in Open Banking, could significantly address the problems of bad actors or of insufficient motivation to follow privacy and security rules. However, some proponents of broad interoperability might object that this would partially defeat the purpose of interoperability mandates, as few small startups would be able to benefit from it. But it must be asked in response whether the risks of opening interoperability to such potentially unreliable providers are worth the potential benefits of their involvement.

C. Mandated Interoperability and Data Flows in the EU Digital Markets Act

The original DMA proposal included several interoperability and data-portability obligations regarding the designated "core platform services" of "gatekeepers" — i.e. the largest online platforms. Those provisions were changed considerably during the legislative process. The most recent version of the DMA, from 11 May 2022, contains, among other provisions:

1) a prohibition on restricting users — "technically or otherwise" — from switching among and subscribing to software and services "accessed using the core platform services of the gatekeeper" (Art 6(6));
2) an obligation for gatekeepers to allow interoperability with their operating system or virtual assistant (Art 6(7)); and
3) an obligation "on interoperability of number-independent interpersonal communications services" (Art 7).

To varying degrees, these provisions attempt to safeguard privacy and security interests, but the first two do so in a clearly inadequate way.

First, the Article 6(6) prohibition on restricting users from using third-party software or services "accessed using the core platform services of the gatekeeper" notably applies to web services (web content) that a user can access through the gatekeeper's web browser (e.g. Safari for iOS).[30] Given that web content is typically not installed in the operating system, but used through a browser (i.e. likely "accessed using a core platform service of the gatekeeper"), earlier "side-loading" provisions (Article 6(4), which is discussed further below) would not apply here.

This leads to what looks like a significant oversight: the gatekeepers appear to be almost completely disabled from protecting their users when they use the Internet through web browsers, one of the most significant channels of privacy and security risks. The Federal Bureau of Investigation ("FBI") has identified "phishing" as one of the three top cybercrime types, based on the number of victim complaints.[31] A successful phishing attack normally involves a user accessing a website that is impersonating a service the user trusts (e.g. an e-mail account or corporate login). Browser developers can prevent some such attacks, e.g. by keeping "block lists" of websites known to be malicious and warning about,

29 *Supra* note 27, Manne & Bowman, at 23.

30 Web browsers are defined as core platform services in Art 2(2) DMA.

31 *Internet Crime (IC3) Report 2020*, Federal Bureau of Investigation (2020) available at https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

or even preventing, access to such sites. An exceptionless prohibition on platforms restricting their users from accessing third-party services, however, would also prohibit this vital cybersecurity practice.

> Under Art 6(4), in case of installed third-party software, the gatekeepers can take:
>
> measures to ensure that third party software applications or software application stores do not endanger the integrity of the hardware or operating system provided by the gatekeeper, provided that such measures go no further than is strictly necessary and proportionate and are duly justified by the gatekeeper.
>
> The gatekeepers can also apply:
>
> measures and settings other than default settings, enabling end users to effectively protect security in relation to third party software applications or software application stores, provided that such measures and settings go no further than is strictly necessary and proportionate and are duly justified by the gatekeeper.

None of those safeguards, insufficient as they are — see the discussion below of Art 6(7) — are present in Art 6(6). Worse still is that the anti-circumvention rule in Art 13(6) applies here, prohibiting gatekeepers from offering "choices to the end-user in a non-neutral manner." That is precisely what a web-browser developer does when warning users of security risks or when blocking access to websites known to be malicious — e.g. to protect users from phishing attacks.

This concern is not addressed by the general provision in Art 8(1) requiring the gatekeepers to ensure "that the implementation" of the measures under the DMA complies with the GDPR, as well as "legislation on cyber security, consumer protection, product safety." The first concerns is that this would not allow the gatekeepers to offer a *higher* standard of user protection than that required by the arguably weak or overly vague existing legislation. Also, given that the DMA's rules (including future delegated legislation) are likely to be more specific — in the sense of constituting *lex specialis* — than EU rules on privacy and security, establishing a coherent legal interpretation that would allow gatekeepers to protect their users is likely to be unnecessarily difficult.

Second, the obligation from Art 6(7) for gatekeepers to allow interoperability with their operating system or virtual assistant only includes the first kind of a safeguard from Art 6(4), concerning the risk of compromising "the integrity of the operating system, virtual assistant or software features provided by the gatekeeper." However, the risks from which service providers aim to protect users today are by no means limited to system "integrity." A user may be a victim of, e.g. a phishing attack that does not explicitly compromise the integrity of the software they used.

Moreover, as in Art 6(4), there is a problem with the "strictly necessary and proportionate" qualification. This standard may be too high and push gatekeepers to offer more lax security to avoid liability for adopting measures that would be judged by EU Commission and the courts as going beyond what is strictly necessary or indispensable.

The relevant recitals from the DMA preamble, instead of aiding in interpretation, add more confusion. The most notorious example is in recital 50, which states that gatekeepers "should be prevented from implementing" measures that are "strictly necessary and proportionate" to effectively protect user security "as a default setting or as pre-installation." What possible justification can there be for prohibiting providers from setting a "strictly necessary" security measure as a default? We can hope that this manifestly bizarre provision will be corrected in the final text, together with the other issues identified above.

Finally, there is the obligation "on interoperability of number-independent interpersonal communications services" from Art 7. Here, the DMA takes a different and much better approach to safeguarding user privacy and security. Art 7(3) states that: "The level of security, including the end-to-end encryption, where applicable, that the gatekeeper provides to its own end users shall be preserved across the interoperable services." There may be some concern that the Commission or the courts will not treat this rule with sufficient seriousness. Ensuring that user security is not compromised by interoperability may take a long time and may require excluding many third-party services that had hoped to benefit from this DMA rule. Nonetheless, EU policymakers should resist watering down the standard of equivalence in security levels, even if it renders Art 7 a dead letter for the foreseeable future.

It is also worth noting that there will be no presumption of user opt-in to any interoperability scheme (Art 7(7)-(8)), which means that third-party service providers will not be able to simply "on-board" all users from a gatekeeper's service without their explicit consent. This is to be commended.

III. CONCLUSIONS

By and large, the DMA betrays a policy preference for privileging uncertain and speculative competition gains at the cost of introducing new and clear dangers to information privacy and security. This is clearly the case in Articles 5 and 6 of the DMA. Proponents of those or even stronger legislative interventions have demonstrated that they are much more concerned, for example, that privacy safeguards are "not abused by Apple and Google to protect their respective app store monopoly in the guise of user security."[32] Given the difficulties in ensuring effective enforcement of privacy protections, however (especially with respect to actors coming from outside of the EU, the United States, and other broadly privacy-respecting jurisdictions), the mentions of privacy and security in Articles 5 and 6 amount to not much more than lip service. It is reasonable to expect a much more detailed vision of concrete safeguards and mechanisms of enforcement from policymakers who are proposing rules that come with entirely predictable and very significant privacy and security risks. One solution worth considering is already to be found in Article 7(3) DMA: the requirement that any third-party service providers offer at least the same level of security as the gatekeepers.

I do not want to suggest that interoperability is undesirable. The argument of this paper was focused on *legally mandated* interoperability. Firms experiment with interoperability all the time; the prevalence of open APIs on the Internet is a testament to this. My aim, however, is to highlight that interoperability is complex and exposes firms and their users to potentially large-scale cyber vulnerabilities. Generalized obligations imposed on firms to open their data or to create service interoperability short-circuit the private ordering processes that seek out the forms of interoperability and sharing that pass a cost-benefit test.

The result will likely be both overinclusive and underinclusive. It would be overinclusive by requiring all firms that are in the regulated class to broadly open their services and data to all interested parties, even where it wouldn't make sense for privacy, security, or other efficiency reasons. It is underinclusive, because the broad mandate will necessarily sap regulated firms' resources and deter them from looking for new innovative uses that *might* make sense, but that are outside of the broad mandate. Thus, the likely result is less security and privacy, more expense, and less innovation.

32 Damien Geradin, *Digital Markets Act (DMA): Where Is the Council Headed to?*, The Platform Law Blog (18 Oct. 2021) https://theplatformlaw.blog/2021/10/18/digital-markets-act-dma-where-is-the-council-headed-to.

COMPETITIVE DYNAMICS OF ONLINE AND BRICK-AND-MORTAR RETAIL PRICES

BY ROSA ABRANTES-METZ & MAME MALONEY[1]

1 Rosa M. Abrantes-Metz is a Principal at the Brattle Group and the Co-Chair of Global Antitrust and Competition. She is a former Adjunct Professor at NYU Stern School of Business (Rosa.Abrantes-Metz@brattle.com). Mame Maloney is a Senior Associate at the Brattle Group (Mame.Maloney@Brattle.com).

I. EXECUTIVE SUMMARY

This article summarizes a recent white paper by the authors analyzing the competitive interplay of prices amongst retail channels: offline (brick-and-mortar) and online (such as retailers' websites and online marketplaces).[2]

We find evidence of a close competitive relationship between the two channels, in which prices correspond tightly across channels. We find that prices in one channel are highly responsive to changes in the other channel's prices; in other words, when offline prices increase (or decrease), online prices tend to respond by also increasing (or decreasing). This means that consumers online face similar pricing trends to consumers offline, and the competition between different retailers and across channels is vigorous.

We specifically find that online prices are more responsive to brick-and-mortar prices than the reverse, which is consistent with the technological capacity for online prices to adjust more rapidly than brick-and-mortar price tags. Both brick-and-mortar and online prices react similarly when they are the lower price, and tend to adjust upwards. But their responses are clearly different when they are the higher price: brick-and-mortar prices will tend to stay high, while online prices will be pulled down to lower levels. This is consistent with intense price competition both within and across retail channels.

For the set of products analyzed at the national aggregate level, we also find that both channels experience increases and decreases in dollar sales at the same time and to the same degree. This is consistent with both channels being subject to the same market forces, highly responsive to each other, and are very frequently identical.

Of relevance for competition and regulation, our findings suggest that competition among retail goods is intense, that these respond quickly to each others' prices and that, as a consequence, regulation affecting online commerce is expected to affect prices in brick-and-mortar stores, and *vice versa.*

II. SUMMARY OF RELATED LITERATURE

Academic literature provides various perspectives on whether online and brick-and-mortar prices are similar. Several papers from the early 2000s conclude that consumers face lower prices online than brick-and-mortar due to lower consumer search costs and other informational effects facilitated in an online shopping environment.[3]

More recently, researchers find that prices are frequently identical at the online and brick-and-mortar stores of multi-channel retailers. For example, a 2016 paper by Alberto Cavallo makes use of hand-collected price data and finds that in the U.S., prices for the same goods at the same retailer are identical online and offline 69 percent of the time.[4] In this paper, we also present research based on a set of hand-collected price data and find that prices are identical an even greater percentage of the time (95 percent). The difference between our findings and Cavallo's is likely due to the difference in the set of goods analyzed in the two studies and likely increasing convergence over time, as Cavallo's paper uses data from years before our data sets.

Academic literature also provides varying conclusions regarding the behavior of price movements online and offline. Cavallo's research, cited above, suggests price changes do not typically occur simultaneously in online and brick-and-mortar locations of the same retailer, but does find that prices change with similar frequency and magnitude in both channels.[5] In contrast, other research suggests that online prices change

2 A working paper of the unabridged white paper can be found at https://www.brattle.com/insights-events/publications/competitive-dynamics-of-online-and-brick-and-mortar-retail-prices/. This research was funded by the Computer & Communications Industry Association (https://www.ccianet.org/).

3 See, for example, Brynjolfsson, Erik and Smith, Michael D., (2000), Frictionless Commerce? A Comparison of Internet and Conventional Retailers, Management Science, 46, issue 4, p. 563-585; Clay, Karen B. and Krishnan, Ramayya and Wolff, Eric D., (May 2001), Prices and Price Dispersion on the Web: Evidence from the Online Book Industry, NBER Working Paper No. w8271, Available at SSRN: https://ssrn.com/abstract=268880; Morton, F.S., Zettelmeyer, F. & Silva-Risso, J, (2003), Consumer Information and Discrimination: Does the Internet Affect the Pricing of New Cars to Women and Minorities?. Quantitative Marketing and Economics 1, 65–92. https://doi.org/10.1023/A:1023529910567; Jeffrey R. Brown and Austan Goolsbee, (2002), "Does the Internet Make Markets More Competitive? Evidence from the Life Insurance Industry," Journal of Political Economy, University of Chicago Press, vol. 110(3), pages 481-507; Sengupta, Anirban and Wiggins, Steven N., (November 2006), Airline Pricing, Price Dispersion and Ticket Characteristics on and Off the Internet. NET Institute Working Paper No. 06-07, Available at SSRN: https://ssrn.com/abstract=938609; Lieber & Syverson (2010) "Online vs. Offline Competition"

4 Cavallo, Alberto, and Roberto Rigobon. (2016), The Billion Prices Project: Using Online Prices for Measurement and Research. Journal of Economic Perspectives, 30 (2): 151-78.

5 *Ibid.*

more frequently, but that price changes in brick-and-mortar stores are greater in magnitude.[6] Our research finds that, within the same retailer, medium-term price changes offline and online are typically identical in timing and magnitude, with frequent but short-term deviations in online prices.

III. DATA

We analyze two data sources, which together allow us to study various aspects of cross-channel and intra-channel price dynamics for a variety of goods.

- **Nation-wide aggregate price and volume point-of-sale data via NPD**.[7]
  - For each product, the data shows the weekly total dollar sales and total unit volume combined for all partner retailers nationwide. Thus, each week we observe the weighted average price of units sold, separately for the online and brick-and-mortar channels.
  - The data covers baby/child bed and bath products for 2018-2019.[8]
  - Point-of-sale data, also referred to as "scanner data," is a commonly-used type of data in economic studies of retail prices and competition. Scanner data captures all sales that occur at partner retailers. Scanner data allows the analysis of sales volume, which is not possible with pricing data collected purely by third party observers.

- **Novel dataset of hand-collected price observations from individual retail locations, via Premise**.[9]
  - The data contains both online and brick-and-mortar prices on each day from October 25, 2021 through December 2, 2021, for five grocery staples[10] from 18 retail locations in the Los Angeles metropolitan area.[11]
  - Together, these price observations comprise a month-long set of paired online-offline data observations perfectly controlling for retailer and geography. In total, the data has observations for 3,477 unique combinations of retail location, product, and date, of which 2,605 have price observations for both online and brick-and-mortar channels.

We acknowledge that our data covers a limited scope of products and time window, and in particular our hand-collected data is limited to specific retailers and geographical locations. Thus, further research using additional products, retailers, and cities would be desirable to address the generalization of our results to additional products. However, we also note that the research in our paper makes use of two datasets covering two different sets of products and geographies, both providing consistent evidence that online and offline retail channels are subject to the same market forces, behave very similarly to each other, and are highly responsive to each other. Therefore, our research is supportive of intense competition between these two channels.

6 Gorodnichenko, Yuriy, & Oleksandr Talavera, (2017), Price Setting in Online Markets: Basic Facts, International Comparisons, and Cross-Border Integration. American Economic Review, 107 (1): 249-82.

7 NPD obtains its data from a range of partner retailers including mass merchants, specialty retailers, and department stores; the exact list of partner retailers is not released publicly. The NPD data covers hundreds of thousands of retail locations. Retailer- or location-specific data was not available.

8 We selected the most recent two years of data pre-pandemic. Early 2020 saw major (though largely temporary) disruptions to many aspects of the retail process: supply-side issues like global supply chain disruptions, shipping delays, brick-and-mortar retail location closures; and demand-side changes such as lost income and changes in the types of goods consumers wish to buy. Given only two years of data, we would not be able to reliably separate "normal" competitive effects from reactions to these many sources of disruption.

9 The Premise data was collected based on an app through which contributors could gather prices in response to daily posted requests. For redundancy and quality control, multiple daily requests were posted per retail location, product, date, and channel. Contributors were required to submit a photograph (for brick-and-mortar) or screenshot (for online) as supporting evidence for their price observations. Based on these photos and screenshots, invalid prices were removed from the data (for example, if the submitter entered the price for the wrong product or wrong package size). Occasionally, valid price submissions were made for a given retail location, product, date, and channel (whether because no data contributor fulfilled the request on the app, or because the prices submitted were invalid).

10 Specifically: Barilla Spaghetti (1 lb package); Cheerios (one box, 8.9 oz); Gold Medal All-Purpose Flour (2 lb package); Jif Creamy Peanut Butter (16 oz jar); Land O' Lakes Salted Butter (1 lb, 4 sticks / 8 half sticks).

11 The 18 retail locations encompassed five different retailers: Albertsons, Food 4 Less, Target, Vons, and Walmart.

IV. ONLINE AND BRICK-AND-MORTAR PRICE LEVELS ARE CONSISTENT WITH BOTH CHANNELS BEING DRIVEN PRIMARILY BY COMMON COMPETITIVE FORCES AND ARE VERY FREQUENTLY IDENTICAL

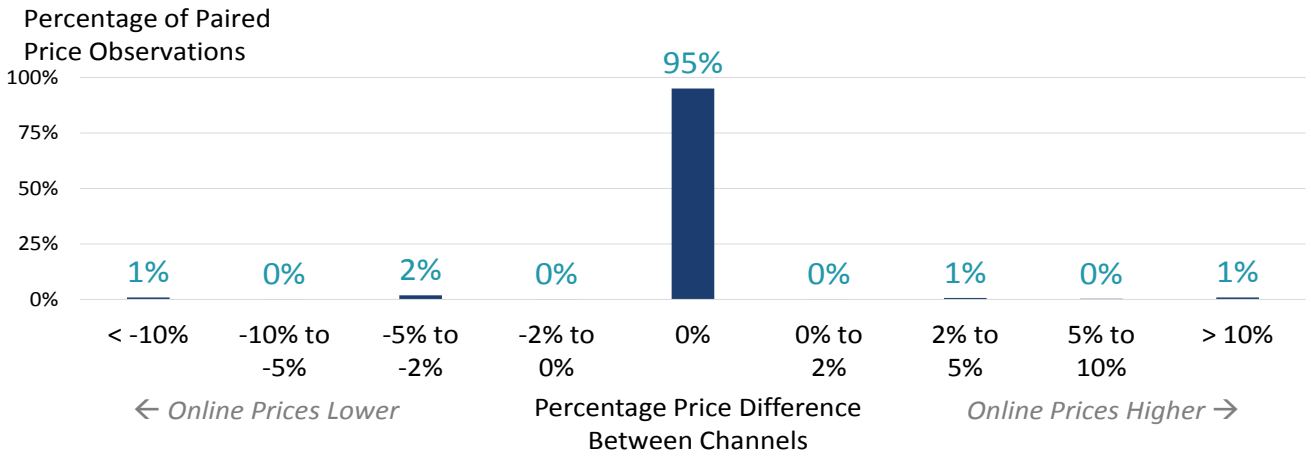
From both data sources, we find strong evidence that online and offline prices correspond closely to one another.

Based on the hand-collected paired grocery price data from Premise – which provide a micro-level view into pricing, explicitly controlling for retailer and geography – we see that online and brick-and-mortar prices are identical to each other the overwhelming majority of the time.

Deviations are the exception rather than the rule and tend to be brief, typically lasting no longer than a day before returning to the prior level. Given the information available to date, we find no evidence that retailers have the ability to set completely different price levels in different channels; on the contrary, online and offline prices appear to be tightly constrained by one another.

Figure 1 below provides a histogram of the percentage differences between online and offline prices. The figure shows that for 95 percent of paired price observations (i.e. corresponding to the same product, retailer, location, and date) online and brick-and-mortar prices are identical. For the remaining 5 percent of observations where online and offline prices differ, online prices are higher roughly half of the time. We find no evidence that online prices routinely over-price or under-price the brick-and-mortar channel. Instead, in the rare cases that prices deviate, online prices are very slightly more likely to be lower than higher.

Figure 1: Distribution of the Percentage Differences between Online and Brick-and-Mortar Prices for the same product, retailer, location, and date



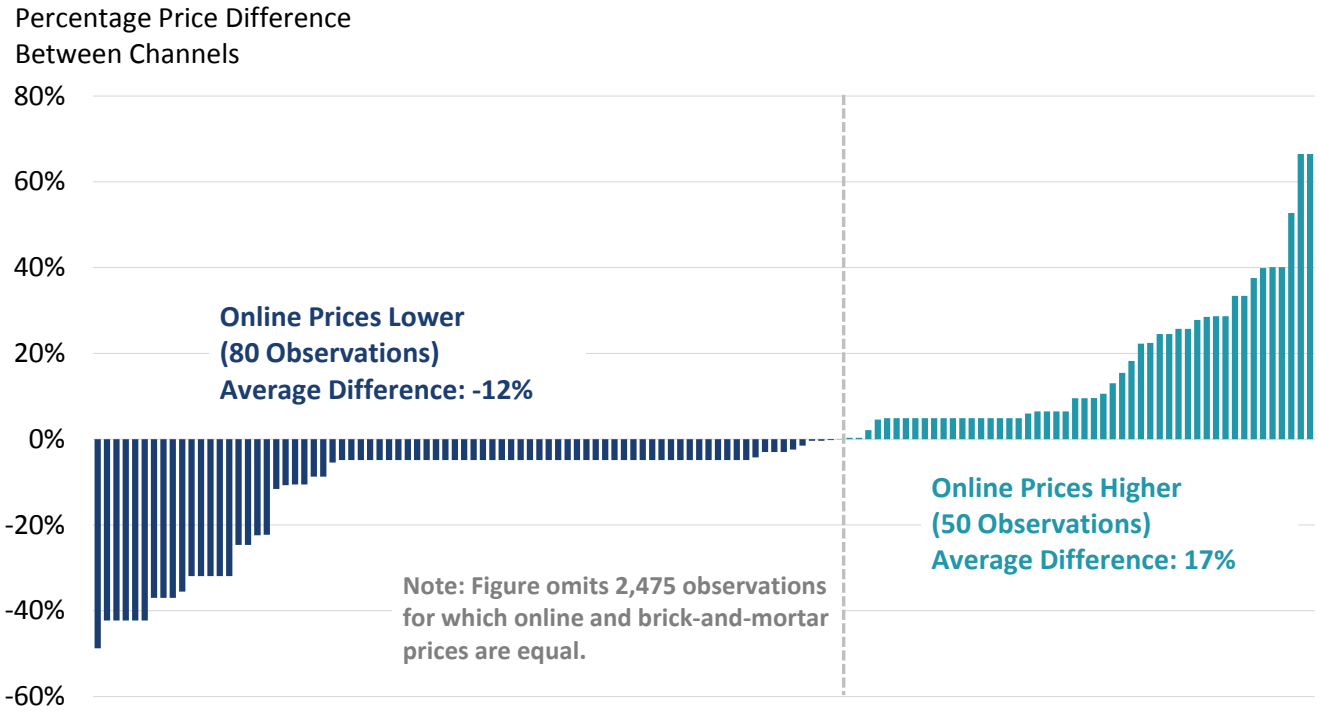
Source: Premise.

Percentage price difference between channels is calculated as ([Online Price] – [Brick-and-Mortar Price]) / (Average of Online and Brick-and-Mortar Prices).

We next focus on the 5 percent of paired price observations for which online and brick-and-mortar prices differ. While these represent a minority of price observations, this allows us to more clearly zoom in on the magnitude of price differences when they are present.

Figure 2 below shows the data for 130 paired price observations for which online and brick-and-mortar prices differ. Each bar in the figure corresponds to a single retail location, product, and date. The height of the bar indicates the percentage difference between online and brick-and-mortar prices, and the bars are sorted from smallest to largest. The dark blue (negative) bars correspond to the 80 observations for which online prices are lower, showing an average difference of 12 percent between the channels. The teal (positive) bars correspond to the 50 observations for which online prices are higher, showing an average difference of 17 percent between the channels.

Figure 2: Percentage Price Difference Between Channels, isolating retail location, products, and dates for which online and brick-and-mortar prices differ



Source: Premise.

Percentage price difference between channels is calculated as ([Online Price] – [Brick-and-Mortar Price]) / (Average of Online and Brick-and-Mortar Prices).

The chart above shows that for the rare instances in which prices differ between channels, we find that online prices are more frequently lower. We further find that the average price discrepancy between channels is larger when online prices are higher as compared to when they are lower.

As another way of looking at this data, we separately examine each of the 18 retail locations, for each of the five products. We test whether online and offline prices are always identical on all days covered by our data, or whether there is ever a difference between online and offline prices. In the instances in which we see a difference, we characterize which channel's prices deviate away from the typical price level[12] prevailing for that product at that retail location.

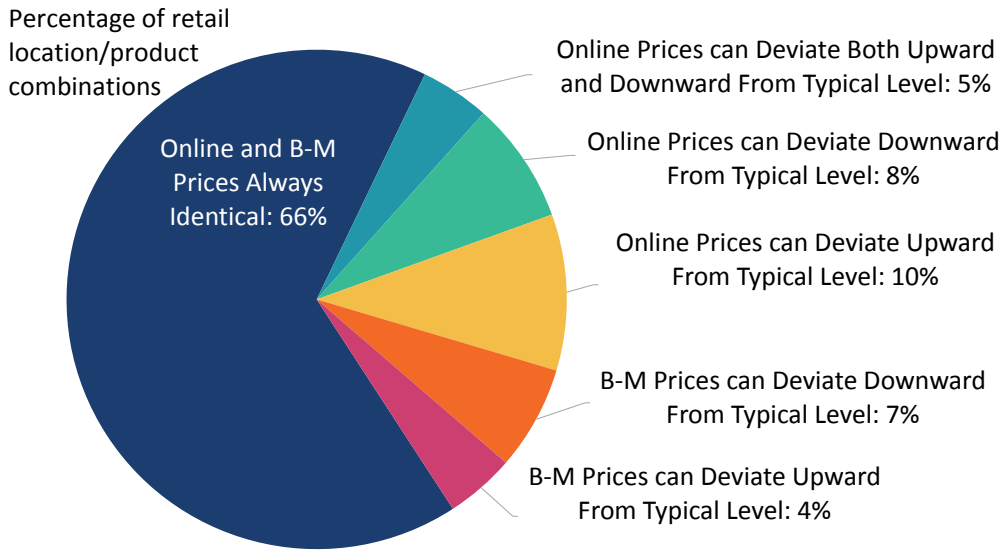
Figure 3 below summarizes our results. We find that for all products, the majority of retail locations always see the same price online and offline during the period of observation. That is, during the period of study, consumers visiting the retail location in-person would see the same prices for the five products as customers shopping on that retailer's website.

The remainder of retail locations have at least one day during the period of study for which prices online and offline can differ. For these, we observe no consistent pattern suggesting one channel's ability to deviate permanently from the other: both channels can deviate from the typical price level, sometimes upwards, sometimes downwards. These deviations are not persistent, and prices tend to come together again quickly.

Finally, to contextualize these findings, recall from Figure 1 above that even when prices between the online and offline channels differ, the magnitude of the difference is quite small.

12 We define the "typical price level" as the mode price during a rolling five-day period centered on the day in question.

Figure 3: Percentage of Products and Retail Locations For Which Online and Offline Prices are Always Identical, or Exhibit Differences, for the period 10/25/21 – 12/2/21



Source: Premise

The national aggregate data from NPD provides additional evidence of persistent similarity in prices between the online and brick-and-mortar channels. Because of the national aggregate nature of the NPD data, we expect to find some degree of difference between prices online and offline.[13] Despite this limitation of the data, we still see a close correspondence between prices online and brick-and-mortar in the NPD data. Typically, online and offline prices fall within +/-5 percent of each other.

V. ANALYSIS OF PRICE MOVEMENTS INDICATES NEITHER CHANNEL HAS THE ABILITY TO RAISE AND SUSTAIN HIGHER PRICES THAN THE OTHER CHANNEL IN THE LONGER TERM

Based on the hand-collected pricing data, we analyze the price movements we observe in both channels, demonstrating that although prices between both channels remain tightly inter-locked, the overall pricing pattern is far from static.
We observe the following patterns in price movements within the hand-collected grocery pricing data:

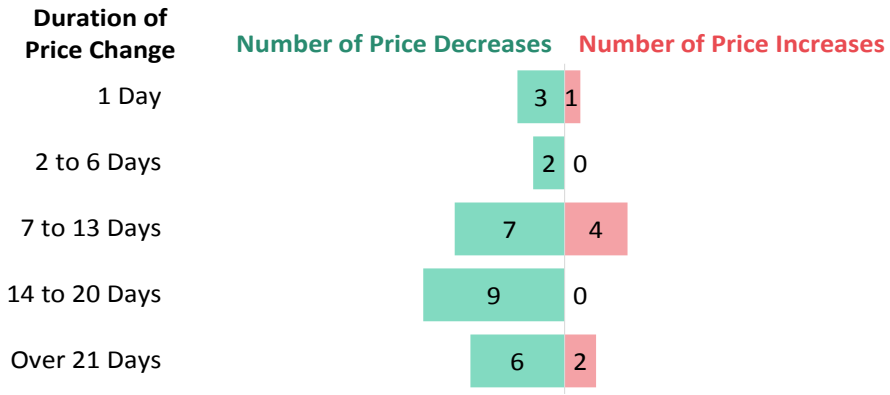
- **Promotional sales and discounts typically begin and end on the same day in both channels for a given retail location**. We find no evidence of persistent or widespread differences in the timing of price changes online and offline. This suggests that a given retailer decides what price to use for a particular product and geographical location, and simultaneously implements this price across channels.
- **Online prices rarely deviate away from brick-and-mortar prices, and when they do, deviations are both upwards and downwards**. This is consistent with the fact that changing prices in a brick-and-mortar store involves a relatively more costly physical effort, whereas online prices can be updated more quickly and easily.
- **Different customers shopping at the same retailer online can see different prices on the same day**. This is consistent with the practice of "A/B testing" whereby a retailer's online channel performs an experiment to test the effect of a price change and help achieve the profit-maximizing price.[14] A subset of customers is shown an alternate price, and quantities purchased can then be compared against the customers who are shown the original price. This pattern of price movement is consistent with very short-term information gathering which helps retailers rapidly respond to changes in demand. The price quickly shifts back to its baseline level, consistent with the online channel being competitively constrained by brick-and-mortar prices.

13 Because the NPD data aggregates together all sales at all partner retailers, we are unable to distinguish price variation by channel from any other reasons prices might differ (e.g. regional variation across different geographical locations, different pricing by different retailers, location-specific promotional pricing). As a simplified example to illustrate this point, suppose we are studying the price of rubber duckies. Suppose also that during the first week of July, only one rubber ducky is sold nationwide, at a boutique in Manhattan. In the second week of July, again only one rubber ducky is sold, this time at a discount retailer in Ohio. Based on the information reflected in our data, it would look like the price of rubber duckies fell substantially week-over-week, even if the prices at each of the two retailers remained constant.

14 For a discussion of A/B testing, see, e.g. Gallo, Amy. "A Refresher on A/B Testing." Harvard Business Review (June 28, 2017). Available at https://hbr.org/2017/06/a-refresher-on-ab-testing.

Figure 4 below summarizes the number and duration of brick-and-mortar price changes. Overall, we observe 34 price change events in the brick-and-mortar data, between October 25 and December 2, 2021. The majority of these (79 percent) are price decreases. Very few price changes last less than a week (only 6 total), due to the costly nature of posting new prices in brick-and-mortar stores. Most price changes last one or two weeks. We also see some examples of effectively permanent changes: 6 price decreases, and 2 price increases, lasting over 21 days.

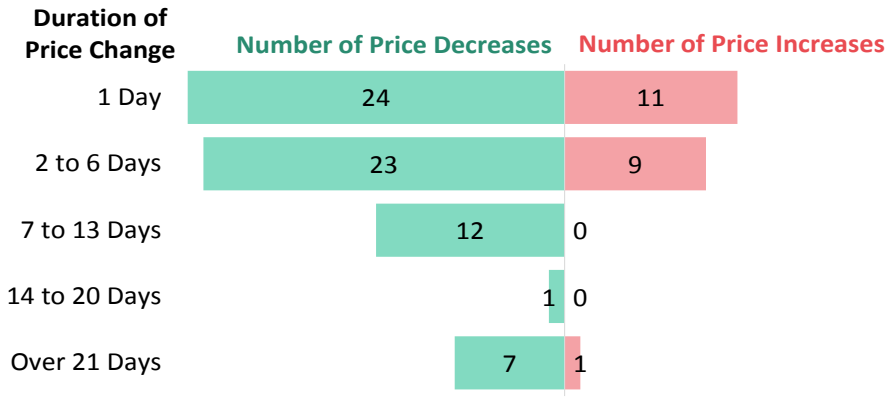
Figure 4: number and duration of brick-and-mortar price changes



Source: Premise

Figure 5 below presents a similar analysis of online price changes. We observe more price changes online (88 total); however, prices still end up the same as the brick-and-mortar price 95 percent of the time (per Figure 1 above). Online price changes frequently last only a single day, consistent with the low cost of adjusting the prices that customers see online. The majority of price changes are decreases (76 percent). We see do see some longer-term changes in online prices: 7 price decreases and 1 price increase, which largely align with the same price changes occurring in the brick-and-mortar channel.

Figure 5: number and duration of online price changes



Source: Premise

The patterns above are consistent with the relative costs associated with adjusting prices in each channel. Because online retailers can adjust prices at virtually zero cost, it may be worth adjusting prices only briefly, if this maximizes revenue. This is consistent with the short-term information-gathering price research, or A/B testing, that we discussed above. A price increase would lead to a higher revenue per item, but lower volume sold, and a price decrease would lead to a lower revenue per item, but higher volume sold; both scenarios could lead to higher total revenues depending on consumer demand. If the price change turns out not to have increased revenue, the online retailer can simply move prices back to the previous level. However, because brick-and-mortar retailers have a higher cost associated with posting new prices, a brief price change may not be worth the cost of adjusting prices (and adjusting them back if the price adjustment was detrimental to revenue). Moreover, it is not possible to establish a randomized experimental treatment and control group in a brick-and-mortar setting, as all customers see prices posted on the shelf.

In addition, brick-and-mortar retailers benefit more than online retailers from the "loss-leader" effect whereby lower prices on one product (such as the staple groceries studied in this sample) attract customers to the store, where customers purchase additional goods while under one roof. For example, a customer could come into the store because of a sale on spaghetti, and then also buy spaghetti sauce while they are there, and other groceries as well. In this hypothetical example, the spaghetti would be the "loss leader." The grocery store can benefit from loss leaders because many goods are sold under one roof, and it is costly for customers to compare prices across brick-and-mortar retailers and visit multiple retail locations.

The "loss leader" effect can occur in online retail but may be less pronounced because it is easy for the consumer to shop at multiple stores online. For example, a customer visiting Retailer A's website because of a sale on spaghetti might also find it convenient to purchase other items (such as spaghetti sauce) on Retailer A's website. However, the shopper may also quickly research sauce prices across different stores online and choose to purchase sauce more cheaply from Retailer B's website. Thus the "loss leader" effect may be less pronounced online.

For medium-term price changes lasting over one week, the vast majority (95 percent) of online price movements occur in the downwards direction. In other words, we see no evidence that online retailers have the ability to raise and sustain higher prices in the longer term.

All of the foregoing analyses show that within the Premise data, pricing patterns are consistent with retailers engaging in active pricing research online and finding they are competitively constrained. Even when retailers experiment with raising prices online, the price does not remain higher than brick-and-mortar prices for long, which is consistent with competitive pressure bringing it back to a baseline level. The pricing patterns are generally strong evidence of intense price competition in retail, especially within the consumer packaged goods ("CPG") market that the Premise data draws from.

VI. DOLLAR VOLUME OF BRICKANDMORTAR VERSUS ONLINE SALES ARE CONSISTENT WITH BOTH CHANNELS BEING SUBJECT TO THE SAME MARKET FORCES

The NPD data allows us to observe the proportion of sales occurring online versus brick-and-mortar. We see that in each week, roughly the same dollar volume is transacted online as in brick-and-mortar stores, for the subset of products available in the data. Moreover, this is true both during periods of high dollar sales and periods of low dollar sales. This suggests that the two channels are subject to the same market forces.

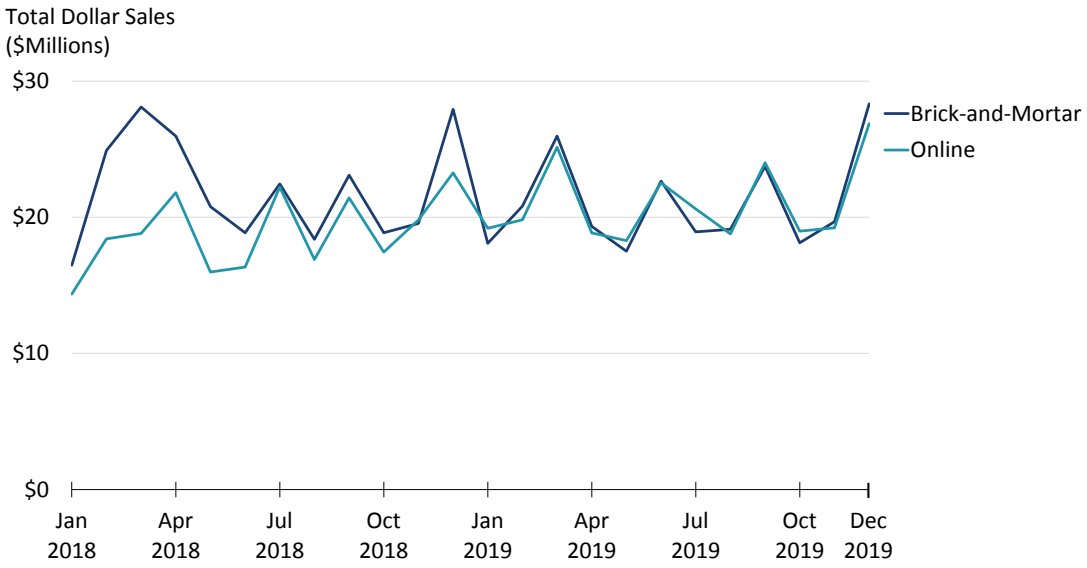
We note that because our national aggregate data is limited to a certain set of products, our findings regarding the proportional market share of e-commerce are not representative of all retail for all products.[15]

Figure 6 plots the total dollar sales in each channel. Some seasonal trends are evident, with both channels seeing a spike in sales approximately every three months (April, July, September, and December of 2018, and March, June, September, and December of 2019).[16] The synchronization of sales volumes between channels is consistent with both channels being subject to the same market conditions. In other words, the same drivers of supply and demand that drive dollar sales appear to affect both online and offline sales similarly. Though not unexpected, the strength of the result is evident.

15 See, e.g. St. Louis Fed data which shows overall e-commerce represented approximately 10 percent of all retail activity during the same time period of 2018-2019. https://fred.stlouisfed.org/series/ECOMPCTSA.

16 As a robustness check (not pictured), we also performed this analysis within each product category. The spikes in sales occur in the majority of product categories. A notable exception was the Bath Toys product category which saw pronounced spikes only in December of 2018 and 2019, coinciding with holiday shopping.

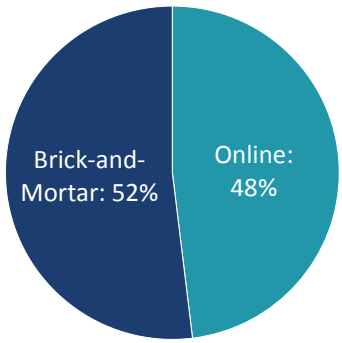
Figure 6: Dollar sales by channel, showing periods of higher and lower sales



Source: NPD

Figure 7 shows the percentage of sales occurring in each channel, as a fraction of the total dollar sales from both channels combined during January 2018 through December 2019. As the pie chart shows, roughly half of sales occur in each channel. Within the set of products studied, neither channel dominates the other.[17]

Figure 7: Percentage of Dollar Sales Occurring online versus brick-and-mortar, January 2018 – December 2019



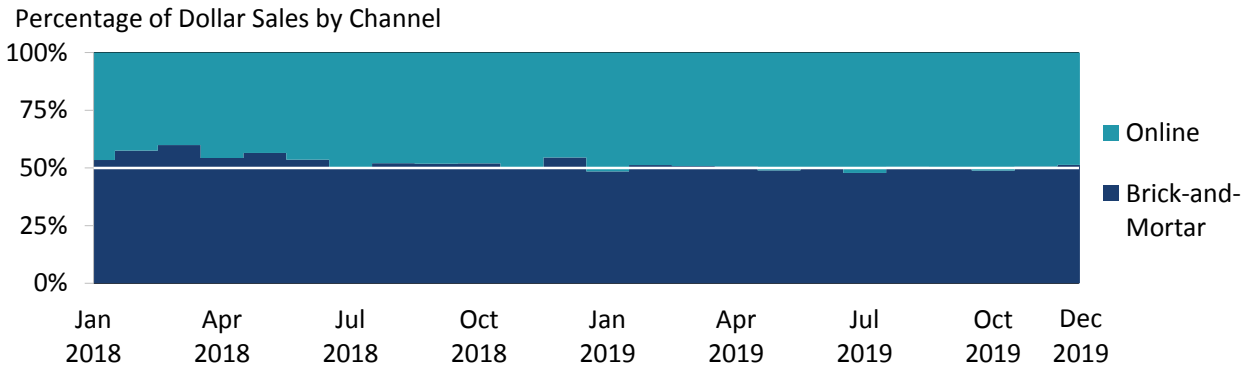
Source: NPD

Figure 8 breaks the pie chart out by month, showing the percentage of total dollar volume each month occurring within each channel. A white horizontal line marks the 50 percent level. The graph shows that the split in volume between channels is stable over time. [18] This is consistent with the idea that online and offline channels are subject to the same market forces, since both channels experience periods of high and low sales volume at the same time and to the same degree.

17 The different product categories saw different proportions of sales conducted online. Bath Toys and Potty Training see the least amount of online sales (~30 percent). Changing Pads has the greatest proportion of online sales (~60 percent).

18 All product categories show a similar stability in the percentage of sales occurring online, with very little month-over-month variation.

Figure 8: Fraction of Dollar Sales Occurring in Each Channel is persistent over time



Source: NPD

VII. CROSS-CHANNEL PRICING DYNAMICS ARE CONSISTENT WITH A DYNAMICALLY COMPETITIVE MARKET

In our final set of analyses, we apply a selection of time-series methodologies to study price dynamics over time in the national aggregate data.

We study the evolution of prices over time by using past price levels to explain the current price levels. For each channel, we simultaneously study both the "own-channel" dynamics (using past online prices to explain current online prices, and past brick-and-mortar prices to explain current brick-and-mortar prices), and the "cross-channel" dynamics (using past online prices to explain current brick-and-mortar prices, and vice versa). This allows us to examine how online prices react to an increase in brick-and-mortar prices and vice versa.

Our key findings are as follows:

- We find that when explaining the variation in brick-and-mortar prices, past values of brick-and-mortar prices have virtually identical explanatory power as past values of online prices. The same is true for explaining online prices. This is consistent with a highly responsive and competitive market between the two channels.
- We further find that online prices move towards brick-and-mortar prices, whether the latter are higher or lower than the former. The data suggests that online retailers are subject to constant competitive pressures and generally respond to competition by matching the lowest price on offer within or across channels.
- The data suggests that online retailers are subject to constant competitive pressures and generally respond to competition by matching the lowest price on offer within or across channels.

To compensate for the noisy nature of the aggregate national data, we apply a time series filter that smooths the data to remove some of the noisiest week-to-week movements. In each of our results, we apply two degrees of smoothing: less filtering which keeps "trend and cycle" movements, and a stronger degree of filtering which keeps "trend" movements only.

Detailed specifications of these analyses, including the time series filter, are presented in the Technical Appendix of the unabridged white paper.[19]

A. Own-Channel and Cross-Channel Explanatory Strength

In our first analysis, we measure to what extent price movements in one channel can be attributed to price movements in the other channel. In other words, we are asking: when prices online vary over time, is this likely due to market forces specific to the online channel, or to market forces that affect both the online and offline channels? Similarly, when brick-and-mortar prices vary from one week to the next, is this likely due to market forces specific to the brick-and-mortar channel, or is it based on market forces affecting both channels? We find that the answer is "both," which is consistent with a very responsive and competitive market that includes both channels.

19 Available at https://www.brattle.com/insights-events/publications/competitive-dynamics-of-online-and-brick-and-mortar-retail-prices/.

In technical terms, this analysis measures the explanatory power of own-channel and cross-channel effects to explain observed price variation.[20] We conduct this analysis for each variation of the filter, and for three time windows (one week prior, 4 weeks prior, and 12 weeks prior).

We find that cross-channel and own-channel prices each explain roughly half of the variation in prices, for both brick-and-mortar and online prices. This holds true even when looking at the trend-and-cycle filter (which allows for more high-frequency noise). Both series are highly responsive to each other, and they are almost equally responsive to cross-channel price movements as they are to own-channel movements. Specifically, when a brick-and-mortar price goes up this week, there is about a 53 percent chance that it is moving in response to a price increase last week from brick-and-mortar, and 47 percent chance that it was due to a price increase for online last week. This is consistent with a very responsive and competitive market that includes both channels.

The pattern is consistent with strong competition both within and across channels. Prices not only respond to variation in prices within the same channel, but also in variation in the other channel. We observe that prices are slightly more responsive to their own price variation than to price variation coming from the other channel.

B. Analysis of Asymmetric Responses

Our second time series analysis quantifies the size and direction of price responses to movements in the same and other channel. In this analysis, we explore the magnitude of own-channel and cross-channel price responses, depending on whether this channel's prices are higher or lower than the other channel's prices. In other words, we look to analyze potential asymmetric responses. Again, the results are consistent with a very competitive setting across channels.

While we do find statistically significant evidence of asymmetry of responses between channels depending which channel's prices are higher or lower, the dollar magnitude of the asymmetry present in the effect size is small. For practical purposes, the behavior of both channels is effectively identical.

Again, we conduct this analysis for each variation of the filter, and for three time windows (one week prior, 4 weeks prior, and 12 weeks prior).

Our "explanatory power" analysis above finds that current prices are about as likely to vary due to past own channel price variation as cross channel price variation. This means that, at any moment in time, price for one channel already reflects price movements from both channels about equally. Therefore, if we want to guess what brick-and-mortar prices will be this week, the best predictor is brick-and-mortar prices from last week, because last week's prices already summarize both channels' prices.[21]

At intervals of two to three months, we find an increased responsiveness to the other channel's prices, for both online and brick-and-mortar. This result holds for both the trend-only filter (which captures low-frequency patterns) and the trend-and-cycle filter (which captures both low-frequency patterns and high-frequency patterns).

We find the following patterns in brick-and-mortar prices:

- When the price level for brick-and-mortar is higher than the online price level, brick-and-mortar prices do ***not*** tend to adjust to meet the lower online prices.
- However, when brick-and-mortar prices are lower than online prices, brick-and-mortar prices ***do*** tend to adjust upward to meet higher online prices.

We find the following patterns in online prices:

- When online are higher than brick-and-mortar prices, online prices tend to be pulled down towards the lower brick-and-mortar prices.
- When online prices are lower than brick-and-mortar prices, online prices tend to be pulled up towards the higher brick-and-mortar prices.
- In summary, both brick-and-mortar and online prices react similarly when they are the lower price, and tend to adjust upwards. But their responses are clearly different when they are the higher price: brick-and-mortar prices will tend to stay high, while online prices will be pulled down to lower levels.

20 Specifically, we are performing a variance decomposition analysis for a set of regression equations; the Technical Appendix provides our model specification and results.

21 While this is always true for both types of filters and at the various time windows, the effect is are stronger at shorter time windows and for the cycle-and-trend filter.

As a general statement, the story that emerges is that online prices move towards brick-and-mortar prices, whether the latter are higher or lower than the former. But while brick-and-mortar prices increase towards online prices when online prices are higher, they will not decrease to the same extent if online prices are lower. This pattern suggests that online retailers are subject to constant competitive pressures and generally respond to competition by matching the lowest price on offer within or across channels. All of our findings are consistent with evidence of competition between online and offline channels.

VIII. CONCLUSION

In this paper, we demonstrate evidence of a dynamic competitive relationship between online and brick-and-mortar channels for retail goods. We find that online prices competitively constrain brick-and-mortar prices, and vice versa. This has implications in policy and regulatory settings, as many regulations targeting one retail channel will likely affect pricing in the other retail channel as well due to intense competition between online and offline retail.

We find that online prices are subject to frequent changes that appear to be related to short-term information gathering and price research. Nonetheless, we find online prices closely adhering to brick-and-mortar prices in the longer term. Thus, we find no evidence that one channel has the ability to systematically raise and sustain higher prices in comparison to the other channel.

Our analyses show several patterns consistent with intense competition between online and offline retail, with both channels responding to the same market forces. This suggests that in the context of antitrust, analyses involving dynamic competition and substitutability for retail goods should incorporate information from both online and brick-and-mortar retail sales.

CONSUMER EXPECTATIONS AND FAIR CONTRACTING FOR DIGITAL PRODUCTS

BY SEAN F. ENNIS[1]

1 Professor Sean F. Ennis, s.ennis@uea.ac.uk. Centre for Competition Policy and Norwich Business School, University of East Anglia, Norwich, Norfolk NR4 7TJ. Please note that I have worked on private matters related to digital companies, as well as for competition authorities. The views presented here represent my personal thoughts on this topic. I thank many colleagues for helpful comments on one or other of these points, including a broad spectrum of economists, and lawyers, and especially Amelia Fletcher, Kai-Uwe Kuhn, Michael Kummer, Bruce Lyons & Bob Sugden. They do not necessarily agree with these views. Any errors are mine alone.

I. INTRODUCTION

This paper focuses on the role of customer expectations in digital markets. For some products, expectations may be crucial in determining consumer adoption of a given supplier of a product. Inaccurate expectations lead them to choose based on an incorrect view of the future features of the product. Decisions made with substantially inaccurate expectations may result in inferior outcomes for consumers, and, to the extent that expectational formation impacts decisions between competing products, could distort competition in ways that are deemed transactionally unfair.[2]

Consumers may select between products today based on their own expectations about both the current and future state of the product. In the active competition for the current set of available customers, enterprises with products whose customers are repeat customers seek to create expectations about the price-quality features of their future product. When products are network products, the creation of these expectations is important on both sides of the market. Examples of products for which future expectations matter include user selection of which digital platform they use, selection of mobile phone platforms, selection of apps and other software that either requires updates or whose operational capacities are based on past use (such as search engines or recommender systems).

This paper makes three points. First, expectations can affect the current and future demand for product. In this sense, expectations may affect the competition between multiple firms offering competing products. Second, firms may find it profitable to create false expectations when there is a lock-in effect for customers. The firm may find it profitable to reduce the quality or raise the price compared to expectations once customers have invested in one product. This profit possibility, if it exists, creates an incentive for firms to encourage "over-optimistic" expectations early on that are not ultimately met. Third, for many products, there are natural adjustment mechanisms (lost demand, loss of firm reputation) that make companies abide by their customers' initial expectations. But these constraints bind most strongly when customers have effective choices to leave in the face of disappointed expectations. For products with network effects, like many digital products, customers may not have such choices, though customers could potentially reduce their consumption and thus discipline providers through reduced consumption.

II. THE ROLE OF EXPECTATIONS IN DEMAND

The role of expectation in influencing consumer choices is well known. In one relevant example, when customers make an investment in a capital good like a car or a photocopier, they recognize that it will have a limited lifespan, reliability differences and will require maintenance during its operational life. A crucial feature of their evaluation of the long-run cost of a good is then its duration of operation and the maintenance costs during that time. That is, the cost evaluated by the customer at the time of purchase is not just the cost of the machine itself but also the cost of maintenance and of renting any alternative machines when the purchased one needs repair.

Examining the market for maintenance services, customers may reasonably look at the prices from alternative suppliers. Suppose they find current options both of obtaining services from the original manufacturer as well as third-party maintenance companies. They may expect they will be able to purchase these third-party maintenance service (and OEM parts would be available to the party) as well as believing that the existence of this third-party option will discipline maintenance service costs from the OEM. The cost of the maintenance services they plan to use will reasonably contribute to customer their expectations about future cost and affect the customer's initial decision over which photocopier to purchase.

Just as in the case of other long-lived capital products, digital products may also find their adoption being influenced by expectations over future characteristics of the product. Even when consumers do not have to pay for a service, they may still be viewed as investing in the service. The characteristics of importance for consumer choice can include quality and price. One major quality characteristic is privacy, but there are many other quality characteristics related to the ability of the product to meet customer needs and desires.

III. MISLED EXPECTATIONS

Suppose that customers are interested both in the current and future characteristics of the product when they choose it. For a firm offering the product, offering a low price or high quality may be either more costly in actual or opportunity costs. As a result, the highest one-period profits, absent competition, might come from providing a high-price or low-quality product, as in a monopoly pricing situation. Nonetheless, firms may be incentivized to offer low-price high-quality combinations, due to the presence of competition or, even with a monopoly, due to the presence of substantial customer variation in their demand or usage of the product in the presence of the high-price low-quality offer.

2 For a further discussion of transactional unfairness, see Lyons, B. & Sugden, R. (2021) "Transactional fairness and pricing practices in consumer markets," CCP Working Paper 21-03. https://ueaeco.github.io/working-papers/papers/ccp/CCP-21-03.pdf.

Looking forwards over multi-periods, the firm may itself recognize that its profits could augment from making customers commit to its product today, with the low-price high-quality offer, and then switch them over to a high-price low-quality offer once the customers have committed. Not all digital products would necessarily have this feature of higher profits from misleading consumers. For those that do, firms will have the incentive to create misleading expectations about the future. These misleading expectations could affect the competitive process and lead customers to commit to the product today, whether a one-sided or multi-sided product.

The existence of expectational distortion strategies is not novel in the digital area. Judge Sporkin in the 1994 in the U.S. v. Microsoft consent decree opinion, noted the existence of "vaporware" allegations against Microsoft. Judge Sporkin defined vaporware as "the public announcement of a computer product before it is ready for market for the sole purpose of causing consumers not to purchase a competitor's product that has been developed and is either currently available for sale or momentarily about to enter the market." Sporkin's memorandum states ""Vaporware" is a practice that is deceitful on its face and everybody in the business community knows it."[3] The announcement of vaporware would affect expectations of users today and could change their purchasing intentions. These announcements could then derail the rollout of alternative products, as users waited for the release they might prefer. In the case of vaporware, that release might never emerge, but competitive damage to competitors would be done.

More generally, distortion of customer expectations has played a key role in judicial interpretation of behaviors related to long-life products. For example, in the Kodak decision, the court recognized that a reversal of a prior policy that had allowed OEM sales to third-party repair companies was effectively a change in expectation, even if not excluded by contract, and could represent a competitive harm and potentially illegal behavior.[4]

The determination of whether an expectation comes from active misleading or simple unplanned adjustment of business behavior after the fact, and without pre-meditation or planning, does not alter the competitive effect from misled expectations, which could be the same in both cases, from the consumer perspective.

One might argue that, given the risks of such "exploitation" from misled expectations, consumers should insist upon contractual protections. But in a situation in which consumers have no ability to deviate from a standard contracts and no effective choice of such a contract with long-run protections from the options present, they may reasonably, in many conditions, base their expectations upon the best current indicator. In such circumstances, the best current indicator is current behavior and announcements of the suppliers.

Consumer cannot be expected to be aware of all the financial calculations and plans or possible plans of companies they deal with, particularly for transactions that have relatively low value. But examples are legion of introductory offers being supported by investors without being properly labelled as introductory offers. Many fintech companies, while competing with traditional banks, have offered their services at zero cost while losing money on an average customer over an extended period. While the rationale of building up a network may result in higher enterprise value, in the long run such a scheme is not sustainable and would require a way to harvest value. In such situations, a proper creation of expectations would warn customers, in large and clear print, that the offer from the company will need to evolve into one with higher payment for services, and provide some estimate of the costs to come. While such clear introductory offer announcements might create more balanced expectations about consumers about their future stream of costs from signing up with and investing in a given service provider, such announcement have been rare or inexistant in most products potentially affected by the type of behavior here, where the product supplier has an incentive to change the deal once customers have locked themselves into it.

If products are repeatedly shown to exhibit "introductory offer" effects, and this is common knowledge among consumers, the introductory offer effects would not be so clearly misleading. Thus, introductory offer effects in a product that is established, and where the effect regularly occurs, such as insurance, may not be on the same level of seriousness as those as products for which customers would have no obvious expectation the effects will exist. For insurance, informed consumers could expect the initial offer received is an introductory offer. Even so, there is an argument that this pattern should be more clearly communicated to consumers, where it occurs, to ensure a balanced competition between products. For some products, such as internet access and telecom services, introductory offers are often clearly labelled and explicitly time limited. But for many products, the potential that offers are introductory is inherently unclear to consumers.

3 Judge Stanley Sporkin's Memorandum Opinion in Civil Action No. 94-1564 further states, in emphasizing the point of unfairness of creating undue expectations, "Microsoft has a dominant position in the operating systems market, from which the Government's expert concedes it would be very hard to dislodge it. Given this fact, Microsoft could unfairly hold onto this position with aggressive preannouncements of new products in the face of the introduction of possibly superior competitive products." Note that Judge Sporkin was subsequently removed from the case after refusing to allow what he considered as too lenient a consent decree.

4 *Eastman Kodak v. Image Technical Services* was decided by the US Supreme Court in 1992 (504 U.S. 451), preventing Kodak from tying its aftermarket services. The court found that if customers were aware of the aftermarket sales restrictions when buying the initial product, they could take into account the life-cycle product cost. To the extent that policies change after purchase, that it is difficult to assess costs or that changing machines after purchase is difficult, concerns could exist. EU cases that have found aftermarket abuse include *Novo Nordisk* (1996), *Digital* (1997), and *IBM Mainframes Maintenance* (2011).

IV. ROLE OF NETWORK EFFECTS

Suppose that we imagine the decision-making and profits of companies as they deal with consumers over two-periods.

In the first period, two competing companies set price-quality levels and recruit consumers. The firm that recruits the most customers in the first period will then experience a tipping effect and have all the customers in the second period. Companies in the first period make statements with implications about their future behavior. These statements can include, for example, direct statements about the future, statements about interoperability, statements about the values of the company and ways that the company's product protects consumers. Companies themselves differ in the extent to which they discount future profits, which can lead them to set different price-quality offers. At the end of the period, all customers move to the winning firm and make their investment. They make an investment to build up knowledge of how to use the product. This investment is not recoverable when moving to the other product.

In the second period, the winning firm from the first period sets a price-quality level. Customers begin by dealing with the company that won the first period tipping battle. This company announces its price-quality level. The customers then find out whether they were led astray by the behavior of the company that was making the best offer in the first period. The difference for the company in this second period is that consumers have now invested into their product, and if the consumers moved away, would have to make, at the minimum, a comparable investment into the product they did not select. We can imagine this would give the tipping winner the power to extract, in the second period, this switching cost. Customers decide whether to continue consuming the same product as won the tipping battle. If so, how much to consume. Customers who leave can return to the product that lost the tipping war.

In this scenario, the key point for determining the first-period decision of consumers is not only the first period price-quality offer but also the consumer's expectation of the second period price-quality offer. The challenge is that predicting the future price-quality offer is difficult. In the absence of clear information, such as a long-term contract, the customer may reasonably determine that the best available mechanism for predicting the subsequent period is each company's behavior in the first period. For example, if one company has a higher quality-adjusted price than the other, the consumer may reasonably conclude that this would also be the company with the higher quality-adjusted price in the second period. There could be good reasons for this assumption, including that the company with the lower price may have lower costs, may have lower discount rates, may have less inclination to take advantage of market power or may have a corporate belief system that would yield better measures of quality (e.g. privacy) than the other company.

Now suppose that the firms are operating a product with network effects in which the value of the selected product is contingent upon the number of consumers. In this case, the analysis changes, in the sense that the cost of switching is no longer limited to that of learning a new product. The cost is multiplied. The functionality of the alternative product, in terms of direct network connections, will be much reduced, so that customers might not any longer have a viable alternative network to use, due to the tipping that happened at the end of the first period. Especially if customers will generally prefer to be on the dominant network, adopting a coordination mechanism that ensures many disappointed customers could move jointly is typically unrealistic. Thus, platforms may have a capacity and incentive to limit the quality or raise price, compared to initial expectations, in ways that would harm consumers. Their capacity to change the offer may be greater than for non-network products.

We here assume that long-term contracting over the price-quality level is not possible. There may be many reasons that such long-term contracting would not be possible. In addition to the classical ones emphasized by Williamson related to uncontractable or costly contracting for all states of the world[5] is the additional reason that if a platform provides future guarantees to both sides, the platform loses its ability to dynamically adjust the contract considering technological changes that are unknown to all and that may affect the bargain needed between the two sides of the platform.

The disciplining effect of lost customers can easily operate in such a way that the company that won the tipping battle is willing to lose a small number of customers who end up with disappointed expectations. Thus, even if some customers are so upset by the quality declines in a product that they leave, the size of this leaving group may be insufficient to discipline a quality reduction from the expected level. This would require that the firm profits from the quality reduction on the remaining customers are greater than the lost profits from customers who leave.

A welfare analysis could usefully compare the scenario in which tipped companies do not meet original customer expectations and one in which there is a standard that implicit expectations must be maintained. Welfare would likely be greater in the presence of a standard that would not allow companies to divert away from expectations initially created. In a world where companies could not mislead initially and

5 Williamson, O. E. (1985). The economic institutions of capitalism: Firms, markets, relational contracting. New York: Free Press.

then divert from their initial status without a strong reason, consumers would make better informed decisions and would likely be better off. Companies would still be able to have introductory offers, which might be necessary to create initial network effects around their products, but when made, such offers would be labelled as introductory. The choice between competing offers early on would be informed. Some ability for platforms to raise price and lower quality from the initial level may be commercially necessary to recover the costs of initial investment and ensure an adequate return. But allowing companies to indiscriminately change the contract from the implicit and initially expected contract will likely lower long-run consumer welfare.

At the same time, a standard expectation of maintaining initial expectations must consider that, to the extent technological evolution makes the initial scenario unrealistic or worse for consumers, then an optimal scenario would allow evolution of the implicit contracts. Moreover, if business plans evolve over time, e.g. due to risk of bankruptcy, a change from initial expectations may also be natural. In absence of these exceptional factors, creating or maintaining false expectations is not a form of corporate behavior that is fair to consumers, can distort competition and would not be encouraged for consumer welfare.

Companies that do not plan to honor their initial contracts, or to treat them as a kind of introductory offer, would provide more truthful and fair indicators to customers if they label their offers as introductory in clear and noticeable ways. For example, if "virtual" banks operating with loss-making business models make it clear that they will have to introduce additional charges in the future, such clarity would be more transparent than a strategy of recruiting customers with zero cost plans and then gradually raising costs in ways that are predictably necessary from the business perspective, but were not expected by consumers. There are many examples of companies in the digital sphere that have created misleading impressions. These actions can include companies that, after establishing a platform product, raise the price to one side of the platform by a factor of as much as four times, or platforms that make announcements that are instrumental in their solidification of tipping but are not later honored, or platforms that begin drip pricing after customers become addicted to a product, or platforms that lower privacy protections to consumers over time.

V. CONCLUSION

The formation of consumer expectations for digital products is crucial for determining early outcomes in competition between platforms. Unfair competition may occur if the competitive outcome is influenced by misled expectations and if the company that won the competition either misled or did not affirmatively correct consumer expectations that were not going to be met. The ability to exploit customers whose expectations have been misled is particularly strong for networks that have tipped, as outside alternatives for dissatisfied consumers may no longer be realistic or viable alternatives for consumers. Greater corporate care to fulfilling consumer expectations would enhance welfare and ensure transactionally fair competitive outcomes for digital products.

CPI COMPETITION POLICY™ INTERNATIONAL

CPI Subscriptions

CPI reaches more than 35,000 readers in over 150 countries every day. Our online library houses over 23,000 papers, articles and interviews.

Visit competitionpolicyinternational.com today to see our available plans and join CPI's global community of antitrust experts.


CPI
COMPETITION POLICY™
INTERNATIONAL