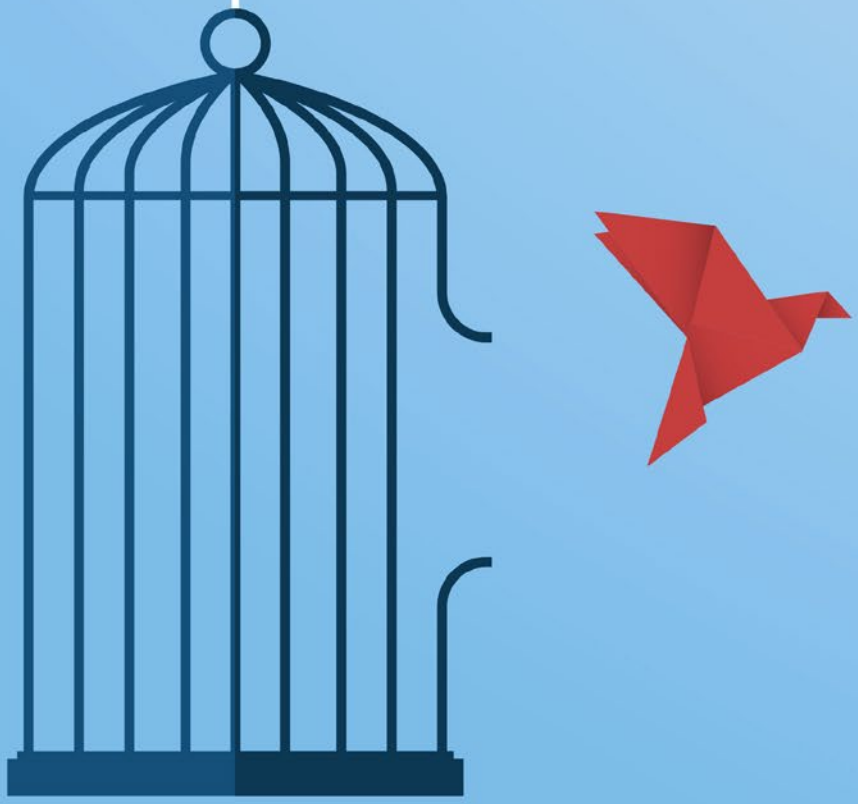
Antitrust Chronicle

SEPTEMBER · FALL 2021 · VOLUME 1(2)



Free Isn't Free?

CPI COMPETITION POLICY INTERNATIONAL

TABLE OF CONTENTS

04 **Letter from the Editor**

05 **Summaries**

07 **What's Next?**
Announcements

08 **Competing for Free**
By Dr. Helen Jenkins, Dave Jevons & Dr. Andrew Mell

14 **When "Free" Is Not "Free"**
By Katherine B. Forrest

17 **Monetary Remedies for Zero-Price Privacy Regulation: An Economic Perspective**
By Andrew Stivers

23 **Free Isn't Free: Digital Platform Data Practices and Australia's Unfolding Regulatory Response**
By Jacqueline Downes, William Georgiou & Melissa Camp

31 **Free as Air?**
By Salil K. Mehra

35 **Personal Data as a Price in Market Definition: A Brief Assessment**
By Magali Eben

LETTER FROM THE EDITOR

Dear Readers,

What is a “free” service? Intuitively, and historically, a “free” service would be defined, simply, as one that merely does not require payment at the point of sale.

Yet, new business models, facilitated by the Internet, have upended the notion of “free.” In particular, with regard to user-facing services such as online search, social networking, image and video hosting (along with countless others), users are not obliged to pay for the service in monetary terms.

In today’s economy, companies extract value (sometimes graphically described as the users’ “eyeballs”) by displaying advertising alongside the core service. In addition, they gain access to data on users’ preferences and habits, allowing them to display ever more targeted advertising and content.

Other services are also ostensibly “free,” yet also produce value for the provider company. An “open source” operating system may come at no monetary cost to hardware producers who seek to use it. But it may generate ecosystem and lock-in effects that represent genuine economic value for the software provider (and as a result produce market power).

On the other hand, such free business models can produce genuine innovation and provide valuable services to consumers (who might not otherwise be willing or able to pay for them).

The challenge for antitrust enforcers is to grapple with such novel and innovative market dynamics, while preserving innovation incentives, on the one hand, and preventing any abuse of market power, on the other.

The contributions to this volume explore the details of this dynamic, in its many facets, drawing on the authors’ wealth of experience in jurisdictions around the world.

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

Sincerely,

CPI Team

SUMMARIES

08

Competing for Free

By Dr. Helen Jenkins, Dave Jevons & Dr. Andrew Mell

A feature of many digital platforms is that they offer services to one side of the platform "for free." In some instances, the business model requires the consumer to trade their data and attention in return for "free" services. We consider how providing consumers with a service that is 'free' can provide consumer benefits but also make it harder for potential rivals to contest that market, since it can be very difficult to undercut an incumbent selling goods for "free." Price reductions below zero are sometimes possible, as shown by cashback and bundled offers, but can be more challenging when the payment is in data or attention. In addition, any move away from free, up or down, may require a significant additional transaction cost, which can be a significant barrier to consumer switching in certain situations.

14

When "Free" Is Not "Free"

By Katherine B. Forrest

Consumers on the Internet routinely give away data — information about their habits, preferences, purchasing patterns, contacts and more — in return for "free" access to an abundance of platforms and sites. While this may be an attractive model for some users, most are operating with less than full information. In the digital world, what is "freely" given can actually come with embedded costs. Defining large quantities of user data as a product cognizable under antitrust laws raises questions as to whether such data can confer market power, and what the consumer welfare implications of its use are. In addition to the personal cost to individuals, effective control of the data comes with a community cost: other innovators are barred from using those "free" inputs. This essay assesses the current state of antitrust matters related to the monetization of "free" data and where the landscape might be headed.

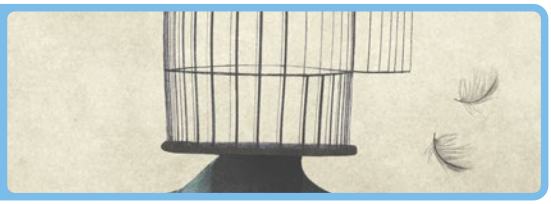
17

Monetary Remedies for Zero-Price Privacy Regulation: An Economic Perspective

By Andrew Stivers

Zero-price goods and services potentially create a problem for regulators interested in crafting monetary remedies that are deterrent, efficient, and inexpensive to implement in that they prevent the use of an easy proxy for injury or gain. Major privacy regulations in the EU and U.S. seem to have focused on deterrence, but in pursuit of cheap, have left any hope of efficiency to the discretion of the enforcers with little guidance on what that would mean. This paper examines regulatory choices for monetary remedies in the context of zero-price privacy and data security practices. The paper lays out the economic framework consistent with a broad range of potential harms, and argue that failing to provide any link or guidance between these remedies and the welfare effects of the practices in question will create opportunity for regulatory capture or improper political influence, and muddy the deterrent signal to potential violators.

23

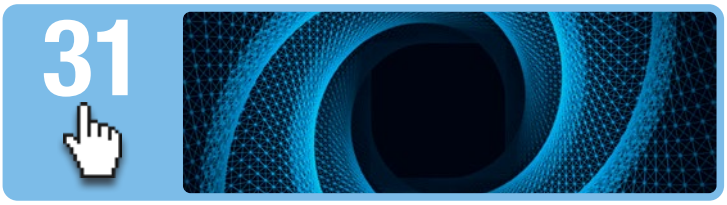


Free Isn't Free: Digital Platform Data Practices and Australia's Unfolding Regulatory Response

By Jacqueline Downes, William Georgiou & Melissa Camp

Since the release of its Digital Platforms Inquiry Final Report in 2019, the ACCC has continued to be active in investigating digital platform market issues in Australia, including the collection and use of consumer data in exchange for the provision of "free" services. The ACCC has initiated a variety of enforcement actions before the courts relating to these services. However, these cases have not to date used Australia's competition law but rather have been brought under consumer laws. This article explores whether current Australian competition laws are sufficient to address data issues or whether it is likely that, like their international counterparts, the ACCC may also move towards an *ex-ante* regulatory regime to govern digital platforms.

SUMMARIES



Free as Air?

By Salil K. Mehra

"Free" once had a simple meaning – something without constraint whatsoever, as in "free as air." At times, some have suggested that antitrust enforcement should not target "free" services – but "free" is Protean in meaning. After all, "there ain't no such thing as a free lunch." "No-monetary-payment" is not the same thing as "free." Making someone else pay is not "free." Finally, receiving something in exchange for the alteration of one's mind is not "free." Firms, products and markets have changed; so too, must competition law. Recent cases against firms that provide users applications without monetary payment, such as Google and Facebook, suggest that competition law enforcers increasingly understand that "free" cannot be a get-out-of-antitrust enforcement card. These cases bear watching to gauge whether and how competition law can evolve as firms, products, and markets have done.

Personal Data as a Price in Market Definition: A Brief Assessment

By Magali Eben

Services offered by Google, Facebook, and their kin are not truly free: users contribute to the monetization of the platform. The question is not whether a market can be defined for zero-price services, but rather how this should be done. This short piece assesses whether personal data can be conceptualized as a price, to enable a substitution analysis for zero-price services. To do so, the piece focuses on the notion of price and its role in quantitative substitution analysis (when consumers react to price changes) in the context of personal data. It makes a reflection on the feasibility of conceptualizing personal data as a price. This would require answering two questions: first, is there a relationship of exchange between the user and the platform; second, can reactions to changes in personal data collection be used to assess substitution. The piece then briefly considers a revised SSNIP test with personal data.

WHAT'S NEXT?

For October 2021, we will feature Chronicles focused on issues related to (1) **Imperfect Competition**; and (2) **Breaking Up Is Hard To Do?**

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 NOVEMBER 2021

For November 2021, we will feature Chronicles focused on issues related to (1) **RegTech**; and (2) **Compliance**.

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.

COMPETING FOR FREE

BY DR. HELEN JENKINS, DAVE JEVONS & DR. ANDREW MELL[1]



1 Oxera, LLP. The views expressed in this article are the authors' own and do not necessarily reflect those of Oxera or its clients.

I. INTRODUCTION

Consumers have been offered a variety of services "for free" for a long time, however the rise of digital technologies which exhibit high fixed costs and low variable costs has increased the prevalence of "free" services, including free internet search; free email; free social networking; free microblogging; and free entertainment. Of course, in economic terms, a free lunch is very rare, and consumers are typically paying for these services through a form of barter with their attention and their data.[2] This is not a new phenomenon: historically consumers have received free radio and television entertainment; free newspapers; and free telephone directories. Just as the modern set of online services are not free; neither were the services received in the past. Consumers then, as now, paid with their attention.

Two-sided markets abound and their business models have always involved operating as a "platform": giving one side of the market a low (or zero) price has always been a good way to increase demand from, and the amount that can be charged to, the other side of the market.[3] While this phenomenon is not new, the way that it might raise barriers to entry and so embed market strength on one side of a market has raised competition concerns and attention from regulators, especially where the acquisition, aggregation and use of data is at the heart of the business model. In part, the additional regulatory attention might be explained by the greater level of data acquisition that digitization has allowed. The Yellow Pages could not keep track of everything that each household searched for. Google and other internet search engines have been able to keep tabs on what users search for, the search links they then click on, and even their other internet browsing habits. Building up this data allows improvement in the algorithms behind Google's search engine, creating a better service for consumers and a competitive advantage over rivals. The data flows also enable Google to improve the relevance of adverts that are shown, and so increase the value advertisers can derive from their product.[4, 5]

Our focus is on what price is actually being paid by consumers for so-called "free services," and the potential competition concerns that this might raise. To that end, the next section examines the attraction of bartering for internet services with data and attention for consumers and firms alike. Section 3 considers the implications for competition of such services being provided to consumers for free. Section 4 concludes.

II. ONLINE TO THE FUTURE AND THE BARTER ECONOMY

Many firms have built businesses online by offering consumers various services at no monetary cost. The benefits of these "free" services for consumers are obvious, consumers can use email, search the internet, or social network for free. The benefits to the companies providing these services are perhaps less immediately obvious, and different in each case, but still relatively well-known in policy discussions. We set out some of the reasons in the next subsection.

A. Why Provide Services for Free?

There are numerous reasons why a firm might let consumers use the services they provide for free. Classic two-sided markets examples are credit cards and dating agencies. If a large number of consumers are using your credit card, then merchants are more likely to agree to accept and pay for your payment product in order to access sales to those consumers. This can mean that consumers get to use the credit card for free, or may even be paid to use it through cashback incentives and so on. Similarly, in heterosexual dating agencies it can mean that men are charged for listing their profile and viewing the profiles of women, while women can list their profile and gain access for free.[6]

A second, reason for bringing consumers onto a platform without charge is in order to monetize their attention. This is another typical two-sided market strategy, sometimes referred to as advertiser-funded platforms. When searching the internet or browsing a social media feed, a consumer is paying attention to what is on the screen, so this is an opportunity to show them other content of interest, for example an advert for something they might want.

---

2 Sometimes goods are genuinely provided for free either by the state or by charities. The state's provision of primary and secondary education in most Western societies and the rise of food banks in the UK since the Financial Crisis would be two examples. However these are not the cases we are examining here.

3 See Rochet, J.C. & Tirole, J., 2003. Platform competition in two-sided markets. *Journal of the European economic association*, 1(4), pp.990-1029.

4 This data collection has also led to privacy concerns beyond the scope of this paper.

5 See Niels, G. & Ralston, H., 2021. Two-sided market definition: some common misunderstandings. *European Competition Journal*, 17(1), pp.118-133 and Hagiu, A. and Wright, J., 2020. Data-enabled learning, network effects and competitive advantage. *working paper*, available here: https://ap5.fas.nus.edu.sg/fass/ecsjkdw/data%20enabled%20learning%20june2020.pdf (accessed September 22, 2021).

6 See Rochet, J.C. & Tirole, J., 2003. Platform competition in two-sided markets. *Journal of the European economic association*, 1(4), pp.990-1029.

This is not a new business model. For a long time, newspapers, radio, and television broadcasting have used the fact of having the attention of their listeners and viewers to present adverts. This advertising could be tailored to some extent since advertisers had a fairly good idea which consumers were paying attention to which newspapers, radio stations and television channels and at what times. Supermarkets even developed ways of keeping track of people's purchases so as to identify who might profitably be offered a discount on which products.[7] What may be "new" is the extent to which the capture of attention can be combined with the granularity and detail of data on consumers to target them with advertisements to which they are likely to respond. In this way each user can be shown a different advert when visiting the site, tailored to what is known about them.

1. Allocative Efficiency

Many of the services provided over the internet involve high fixed costs, but low variable costs. This is what gives many of the platform industries large economies of scale; and why many internet start-ups are initially loss making. The very low variable costs suggest that the marginal cost of an additional consumer or subscriber may well be very near zero. So zero pricing might lead to allocative efficiency in these industries (i.e. price equal to marginal cost).

B. Why Consume Free Services – Surely People Know There's a Catch?

Paying with data and attention, rather than money, tends to reduce "price" transparency. The extensive policy discussions around data will not necessarily have filtered through to consumers. In a dramatic example of consumer inattention to the terms and conditions of "free" services, a few Londoners "traded" their firstborn children for "free" WiFi access.[8]

To the extent that consumers are aware of the "data price" they pay for "free services," it remains an open question as to how much they value their data and their privacy online. Some consumers might take the view that they don't see how being one datapoint among billions will be harmful to their interests and so are happy to trade their data. Other consumers might place a high value on their privacy and go to great lengths to ensure their online privacy.

Similarly, some consumers don't mind their attention being monetized and simply try to ignore intrusive advertising on the websites they visit. Other consumers might mind a great deal and go to the trouble of installing adblocking software to their browser.[9]

Unlike when consumers pay with money, the data component of the price paid by consumers is non-rivalrous. They can pay for their "free" internet search from Google with their data, and then pay for their "free" email account from Microsoft with the same data. This might make the "data price" attractive for some consumers.

The reasoning of some consumers might be rational in that they don't place a particularly high value on keeping their data private, but do value being able to send emails or network with their friends. So they pay what is, to them, the cheaper price for these services, which comes from handing over their data.

While the considerations above may satisfy economists' need for an explanation based on rational agents, there are also well evidenced behavioral explanations for consumer behavior with "free" services. A "free" offer might make consumers believe they are unlikely to regret a purchase as there is no monetary outlay, and so, effectively over-respond to free offers.[10] In the case of the "free" email, internet search and social networking opportunities offered online, consumers may perceive signing up for these services as a no-regret action. They don't have to pay for the services, so if they don't like them, they can simply stop using them and nothing will have been lost, except for the time they took to experiment. However, therein lies the catch — the time it took to experiment was time in which they gave these products their attention, and in so doing, paid for them.

---

7 There are stories about supermarkets' real-world data gathering allowing them to work out that people were pregnant before they even knew. See: https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/?sh=b3e5d6f66686 (accessed September 21, 2021).

8 Security researchers set up a public WiFi access spot in London which offered free WiFi internet connection, but imposed a "Herod clause" which required users to "*to assign their first-born child to us for the duration of eternity.*" Six people signed on to the WiFi and accepted the terms and conditions. See: https://www.theguardian.com/technology/2014/sep/29/londoners-wi-fi-security-herod-clause (accessed September 15, 2021). Of course, inattention is not the only possible explanation for the decision to accept the terms and conditions. People may have seen the clause but reasoned that such a clause would be unenforceable in any court and so continued anyway. Nevertheless, the anecdote provides a powerful illustration of the potential for consumer inattention or nonchalance over the terms and conditions.

9 For an example of such software, see here: https://adblockplus.org/ (accessed September 15, 2021).

10 See Shampanier, K., Mazar, N. & Ariely, D., 2007. Zero as a special price: The true value of free products. *Marketing science*, 26(6), pp.742-757.

1. The Interaction Between Data and Attention Prices

One interesting aspect of this dual pricing system (data and attention) is the complementarity between the two prices. The more data that consumers give in return for their online services, the better will be the advertising targeting to which they are exposed, and so the attention price per advert shown will fall.

To illustrate, suppose a firm finds a way to extract more data, (i.e. the data price increases). Then that would mean that, assuming no change in the number of adverts shown, the attention price would fall as the adverts would be more targeted on things the consumer might want and so less annoying. The adverts might actually be helpful to the consumer as they might tell them about products they did not know were available, but which actually fulfil a need they have.

However, it is unlikely that the platform would hold the number of adverts constant when the attention price falls in this way. One possible response would be to increase the number of adverts until the attention price returned to its previous level.[11]

The potential impact on the attention price consumers pay is an issue that is not discussed in the any of the policy debates over data. It features in neither the calls to reduce the capacity of firms to gather data for privacy or price transparency reasons, nor in the calls for firms to be made to share the data they have gathered with their rivals for competition reasons. Nevertheless, it is something policymakers should be wary of as it may be a driver of unintended consequences.

There are also externalities between consumers when it comes to the interaction between the data and attention prices. The data we share about ourselves informs the advertising that is shown to similar, but more private individuals and so reduces the attention price they will pay. The converse is also true, those otherwise similar to us who go to great lengths to hide their data while using online services deny that data to advertisers and so raise attention prices paid by all similar consumers.

III. COMPETITION ISSUES WHEN CONSUMERS PAY THE DATA PRICE

Perhaps the most important pro-competitive feature of "free" services is that it makes it relatively easy for consumers to multi-home and test the offerings of different platforms. Compare the cost of trying Bing instead of Google as your default search engine with the cost to an Android phone user of "trying out" an iPhone. Anything that encourages multi-homing on the consumer side is likely to be pro-competitive as it makes it easier for consumers to switch to alternative offers and new entrants. This would tend to lower barriers to entry.

On the other hand, pricing services for free undermines a key entry strategy where a new entrant enters the market with a low, loss-making price that undercuts the incumbent. The hope is that this will attract a sufficient number of consumers to switch and try the competing product. If a sufficient number decide that they prefer the entrant's product to the incumbent's, the entrant will attract a large enough loyal customer base that they can then raise prices to profitable levels.

However, if the incumbent is not charging consumers anything it is very difficult to undercut them. When the market price is zero, moving away from that price can be difficult for entrants. A move, either up or down, faces significant transaction costs in the form of time, effort and sometimes data. Those additional transaction costs may exceed the actual price charged for a small price movement away from zero. While it is possible to undercut zero,[12] in practice moving away from a zero price can be challenging, however it may be possible to enter by undercutting the data or attention price.

11 Note this isn't actually the only possible response. On the other side of the market, more targeted adverts may increase the premium advertisers are willing to pay for their adverts to appear on a "cleaner" less "cluttered" page and avoid being drowned out by the visual cacophony of other adverts, especially if those other adverts are equally well targeted.

12 For example, credit card companies offering cash back on purchases might be seen as form of pricing below zero on the consumer side of the payment market.

A. Undercutting the Data Price

If there are consumers who are wary of handing over their data in return for online services, then one entry strategy might be to enter while collecting less data. Maybe supplementing that lower data price with a financial price, or accepting less personalized targeting of advertisements which attempt to monetize the consumer's attention. For example, this has been DuckDuckGo's entry strategy as an internet search engine. While they are funded by advertisements, those advertisements are targeted on the basis of what the consumer has put into the search bar, rather than being based on any personal information about the consumer. DuckDuckGo's Privacy Policy is described very briefly as "*Our privacy policy is simple: we don't collect or share any of your personal information.*"[13]

DuckDuckGo's entry strategy might be seen as a version of entering with a price which undercuts the incumbent. However, in this case, the goal is to enter with a *data price* that undercuts the data price charged by Google. However, such a strategy must be credible. How does one know either that the company is not collecting more data than they purport; or will not raise the data price once they have attracted enough customers? This credibility problem is little different from the standard reputational problem for a firm justifying premium prices through high quality, which has been covered elsewhere.[14]

However, note that a consequence of this entry strategy cutting the data price may be that the attention price paid by consumers rises (unless the number of advertisements were to fall to compensate). Which suggests an alternative entry strategy – cutting the attention price.

B. Undercutting the Attention Price

To an extent this was HBO's strategy when they launched as a cable company in the United States. Part of their unique selling point was that they offered premium content without interruption for advertising for a monetary price. HBO is now experimenting with a price discrimination strategy in their streaming services where viewers can choose a streaming service at a lower price, but where viewing will occasionally be interrupted by advertisements.[15] This could be seen as undercutting on the attention price.

However, this ability to price discriminate on the attention price is also a reason why it might not be a frequent entry strategy. Some incumbent platforms already price discriminate by offering lower *attention* prices in return for charging a monetary fee. Free membership means that one's enjoyment of the platform might be limited in some way, and one sees advertisements on the screen while using the platform; but paid membership opens up additional functionality and eliminates adverts.[16]

It is notable that the premium element of freemium models tends to lower the attention price, but not (visibly) lower the data price. This may indicate that consumers care more about the attention prices they pay than they do about the data prices that they pay. However, that may well be because it is difficult to credibly take lots of data from some users and not take very much data from others. Consumers who are aware of the data price are likely to associate the amount of data taken by a firm with that firm's brand and reputation rather than the brand and reputation of a particular package offered by that firm.

It is tempting to draw conclusions from the fact that the large digital platforms which have brought large numbers of consumers onboard to their two-sided platforms by offering free services have not been undercut (on any price dimension) by entrants. One might infer from this that free services are detrimental to the competitive process. However, such a judgement would be premature without first gaining an understanding of *why* these firms have weathered the challenges from rivals. It might simply be that the alternative free internet search facilities (such as Bing or DuckDuckGo) or social networking sites (such as Google+) have been perceived as inferior substitutes by consumers rather than anything nefarious about free pricing.

13 See https://duckduckgo.com/ (accessed September 21, 2021).

14 See, e.g. Klein, B. & Leffler, K.B., 1981. The role of market forces in assuring contractual performance. *Journal of political Economy*, 89(4), pp.615-641.

15 See https://deadline.com/2021/06/hbo-max-ads-launches-lowest-commercial-load-streaming-1234767796/ (accessed September 21, 2021).

16 This is known as the Freemium business model.

IV. CONCLUSIONS

When it comes to "free" services, the data price has received a lot of attention both from those concerned with competition in these markets and those concerned with privacy. The former group see data as a significant barrier to entry and want to force companies that have found new ways of generating it to share it with their rivals.[17] The latter want to ensure that the data price is appreciated by consumers and to force companies to hold data securely and give consumers opportunities to opt out of data collection.[18]

While regulators may be right to be skeptical about "free" services, there is a need to bear in mind a number of issues to avoid unintended consequences from any intervention. First, while much has been written about the data price consumers pay for "free" services; the attention price is at least as important, as are the complicated inter-relationships between the two prices. Restricting what data firms may gather may lead to an increase in the attention price being paid. By contrast, opening data to other market providers may actually lead to lower attention prices as other service providers can use the same data to target consumers more precisely.[19]

Second, while there may also be concerns over whether zero pricing creates a barrier to entry as it is a difficult price to undercut, this needs to be weighed against the way in which zero pricing also breaks down barriers to multihoming and the social welfare generated from free consumer services which might not exist if they charged even 1 cent due to transaction costs.

Third, it is possible that firms have attempted to undercut zero pricing. For example, Microsoft has attempted to introduce a negative price for internet searches, by offering rewards for people who use Bing for their internet searches in the form of "Microsoft Rewards."[20] The rewards for searching increase if one uses Microsoft's web browser, "Edge" instead of Google's Chrome.[21] This indicates that firms that have broad eco-systems providing different content that might tempt consumers may have an advantage in entering against "free" offers by incumbents.

A healthy skepticism about "free" services over the internet is certainly a good thing from regulators and customers, especially since consumers have shown themselves to be subject to behavioral biases when it comes to zero prices. However, any case for regulatory intervention is complicated by three important features. First, zero pricing typically appears in high fixed cost, low variable cost industries, so the marginal cost might be pretty close to zero, such that transaction costs might make the charging of a monetary price inefficient. Second, we should bear in mind that the business strategy of offering "free" services to consumers in order to bring them on board in a two-sided market is not new and can be welfare enhancing. What is new is the ability to combine capturing consumers' attention which harvesting and analyzing large quantities of data about consumers – while this may raise privacy concerns, it may also lower the attention price that consumers have to pay. Finally, although "free" services might be difficult for rivals to undercut, the market is innovating around this point and finding ways to offer these services at negative prices. Furthermore, free services reduce the cost of multihoming for the consumer which is likely to be procompetitive. These considerations should direct policymakers to be wary of the potential unintended consequences of regulating around "free" offers.

17 See, e.g. Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), COM(2020) 842 final, December 15, 2020, Article 6(i-j).

18 Anecdotally, these opportunities to opt out come with their own "attention price."

19 One should potentially allow a certain amount of time to pass so that a firm that develops a new way

20 See https://www.microsoft.com/en-gb/rewards (accessed September 17, 2021).

21 See https://www.microsoft.com/en-us/rewards/search-and-earn (accessed September 17, 2021).

WHEN "FREE" IS NOT "FREE"

BY KATHERINE B. FORREST[1]

1 Katherine B. Forrest is a partner at Cravath, Swaine & Moore LLP, and a former United States District Judge of the United States District Court for the Southern District of New York.

Little in this world is actually free. A particularly American salivation response is activated when we are informed, or believe, that something we receive, or could acquire, is "free." A coupon for "buy 2 get 1 free" often inspires additional purchases; sales of bulk products at mega supermarkets may result in the acquisition of more mayonnaise jars than any family could consume in a decade. In the digital sphere, the Internet presents itself as a smorgasbord of "free": free information, news, podcasts, social media platforms, YouTube videos on every conceivable topic.

Consumers are not alone in liking "free" — our digital world has created companies with inexhaustible appetites for what we give them for "free." The irony in 2021 is that when as consumers we give tech companies valuable data for "free," that "free" data is assembled, packaged in a variety of forms, and sold back to us. In effect, giving away our data for "free" costs us. Let's look at this more closely.

The most pressing antitrust matters today concern the monetization of "free" data: investigations, enforcement actions and litigations brought against tech companies using data acquired from consumers. A common thread is some form of allegation that a tech company takes that which is "freely" given by users: their digital activity encompassing browsing and search, purchasing patterns, time spent on websites, numbers of emails sent and received to various addresses. According to various complaints scattered about the courts and agencies, aggregation of this data can lead to market power (in a variety of differently conceptualized markets) and potential abuse. This article does not take a position on the merits of these matters. Rather, I want to pause on where we are and where we might be headed.

When the Internet was born, it provided a superhighway to connection and information. It took some time for users to realize that tire tracks of our personal journeys on that highway could never be erased — and in fact, could be harvested into a whole new set of products. The tire tracks of our journeys over the Internet highway attained value when companies understood that most users were creatures of habit, following similar routes: the types of websites previously visited were indicative of where a user, or one with a similar demographic profile, traveled next. The companies that most quickly figured out how to monetize travel patterns were those that controlled the superhighway infrastructure: companies such as Google, Apple, Facebook and others. Large data sets of information about Internet travel patterns are now routinely monetized into targeted sales, and we can more easily see that what we once assumed was "free" has a cost.

In 2021, we are now used to hearing that prior searches are sold to companies who want to pitch products to us; or that our Instagram histories are used to sell us particular clothes, vacations, goods or services. We are all used to seeing and clicking through the pop-up requests to use tracking "cookies." Every click along the Internet superhighway is watched, analyzed and sold.

How should we conceptualize product definition, market power, and consumer welfare in this digital world when inputs are free but the end product may come at a cost?

All people and all companies possess some form of data. Indeed, all living things possess forms of data encoded into their cellular make-up. The antitrust laws are concerned with the particular ability of certain large tech companies to gather, aggregate and analyze data from our journeys on the Internet superhighway. Data obtains value when it comes in large quantities. Large quantities — large data sets — activate a kind of alchemy: patterns resident in data become valuable predictors of monetizable human behavior (put differently: a company that knows where we have been and what we care about can sell us stuff).

Is "data" obtained, for instance, from an Internet search *a product* cognizable under the antitrust laws? Interestingly, granular data derived from only a single person's digital journey may have no value at all; even less valuable is data based on one set of observations for one person, relevant to a single moment in time.

Instead, the value of "free" data is in *patterns* of behavior that can be derived only from some number of observations. Such patterns transform single data points into a data set that can meet the definition of product: a data set is definable, subject to separate demand, and useful for clear, articulable purposes.

Once we have defined freely given data as a potential product when aggregated, the question follows as to whether such data can confer market power. Numerous investigations and lawsuits assume the answer to this question to be in the affirmative. But let's pause on it for a moment because there is a reality of economic theory being extended in the answer: an individual's personal digital history, freely given, can be given again and again and again. Individual data can be collected again and again — as consumers continuously create digital footprints. The key aspect is control of the superhighway — because it is the control of the means of collection that limits access, creating scarcity. The product then — the data — is not, as traditionally considered, what gives direct rise to "market power." Rather, the power, to the extent it exists, is derived from control of the means of aggregation and control of access. In the absence of such control, the inputs (similar to water sourced from a well-fed spring) are endlessly and freely replicable.

With this as essential background, the product at issue with free digital data comes in two pieces: data in gross, and control of access.

Let's assume that data in gross quantities plus control constitute a product of tremendous value: the control leads to scarcity and the scarcity increases the value. The base inputs were freely given by consumers — how do we conceptualize the welfare impact of control of such freely given information?

It has long been accepted that consumer welfare may be enhanced or reduced by what are defined as "free" products. As an initial matter, a "free" product that in fact has a cost is not free. Determining the cost of such a product might well be an individualized inquiry, however. Imagine, for instance, that I am content to accept all tracking cookies, and traverse the digital superhighway frequently and without a care as to who gathers my history as I go. I may in fact enjoy targeted advertising — preferring it over advertising having no bearing on any of my interests. For me (speaking here hypothetically, of course), my freely given data has come with a positive value associated with it. But let's take a second example: perhaps a person even in the same household as the first. This person eschews cookies, engages in private browsing when possible, but uses apps that nonetheless create, retain and monetize records of usage. This individual has freely but carefully given digital information and will similarly be subject to targeted advertising of various sorts that he or she may deem offensive by virtue of its very existence. The transmogrification of this individual's "free" information into advertisements with a personal cost, has led to a feeling of personal invasion, being surveilled, and perhaps even of being taken advantage of. Here, this individual has experienced a diminution in consumer welfare.

Apart from individuals, there are additional community costs that have welfare implications. Returning to our point above about control: when control of the free input is effective, it precludes other innovators from utilizing free inputs to create new end products. One such end product could be a type of sandbox around the freely given digital information, protecting the example of the second individual above from the welfare-reducing costs. New companies able to access the same digital superhighway information could, in effect, create "off-ramps"; in antitrust terms, this would be output expanding.

What is clear from all of this is that in the digital world, what is freely given can actually come with embedded costs, and has diverse consumer welfare implications.

We all like a good deal — as I said at the outset, a good deal activates a salivation response. We are used to understanding some of the more obvious hidden costs in the brick and mortar world (that we have too much mayonnaise, or we really didn't need three pairs of jeans anyway). In the digital world, consumers are operating with less than full information — less information about what is collected and how it is used. Even more fundamentally, we don't fully understand the scope of how digital information is collected, controlled and monetized. Consumer welfare may be enhanced when free conveys a positive value (as the person in the first example), or harmed when the value proposition turns negative.

We will all be watching with great interest the many antitrust matters now underway that will provide guidance as to how to think about new products, market power, and consumer welfare in this world when "free" is really not free at all.

MONETARY REMEDIES FOR ZERO-PRICE PRIVACY REGULATION: AN ECONOMIC PERSPECTIVE

BY ANDREW STIVERS[1]

1 Andrew Stivers is an Associate Director at NERA Economic Consulting, and former Deputy Director for Consumer Protection in the Federal Trade Commission's Bureau of Economics.

For efficiency reasons, economists often argue that monetary remedies for competition or consumer protection law violations should be tied, at least proportionally, to the welfare effects of those violations. Here, efficiency means both accounting for the intended benefits of regulatory activity and attempting to minimize any effects on legitimate activity. A convenient, if incomplete and sometimes misleading, way to proxy for negative welfare effects is with a price premium associated with the practice in question. Zero-price goods and services remove this convenience, as price in the most plausible counterfactuals are also likely to be zero. This potentially creates a problem for regulators interested in crafting monetary remedies that are deterrent, efficient in the above sense, and inexpensive to implement. Major privacy regulations in the EU and U.S. seem to have focused on deterrence, but in pursuit of cheap, have left any hope of efficiency to the discretion of the enforcers with little guidance on what that would mean.

This paper examines regulatory choices for monetary remedies in the context of zero-price privacy and data security practices. The paper lays out the economic framework consistent with a broad range of potential harms, and argues that failing to provide any link or guidance between these remedies and the welfare effects of the practices in question will create opportunity for regulatory capture or improper political influence, muddy the deterrent signal to potential violators.

I. INJURY IN ZERO PRICE GOODS WITH PRIVACY ATTRIBUTES

The tangibility of money changing hands in the context of contested practices has provided an expedient way for courts to proxy for consumer harm in many consumer protection and competition settings. This is convenient because consumers, by purchasing something in the market, have an observable basis for injury – they gave money in exchange for some bundle of attributes – and clear attribution for that injury – they exchanged money and product directly with a specific firm.

However, when consumers do not give money when consuming some product or service, characterizing injury with respect to privacy attributes may require additional work. Establishing the basis for injury in privacy can be especially difficult, as harmful outcomes may be more removed from the data collection itself, thus requiring more work to attribute outcomes – either to the firm's practices or to specific individuals – and to estimate the monetary value of the injury associated with those outcomes. To start, the paper summarizes two general areas where consumer injury might lie when they do not pay money. Glasgow & Stomberg provide a more general discussion of injury and valuation techniques for privacy in the context of antitrust cases.[2]

First, a consumer may make non-money payments, for example in data or attention (which also generates data). Just like with money payments, transfers of data and attention are relatively easy to tie to a transaction and violative privacy practices may induce premia over compliant practices. For example, a false promise of privacy on a social media site may draw a consumer to that site, where they otherwise would not have gone. The data shared and time expended by the consumer and given to the firm could be the basis for injury, as a function of the consumer's value of those assets. Of these two, time has a relatively well-developed literature establishing its value. While there are some complications, time and attention are normal, rival, and (somewhat) excludable goods. Furthermore, while individual valuations of an increment of time varies, in general spending that increment is viewed as costly.[3] As such, there is little dispute in economics about whether misappropriated time is costly to consumers, although this does not appear to be a readily available source of legal remedy.

Harm to consumers from the misappropriation of data – independent of any feedback effects – on the other hand, is much more difficult to assess, much less well-established, and thus much more contentious. Unlike attention, which consumers often guard fiercely and trade parsimoniously in market and nonmarket settings, consumer data is more intermittently protected, and often given – or simply flows – promiscuously. That many consumers have direct preferences over those data flows is not in doubt, and with enough effort, grounded estimates of injury can be made in many cases. Substantial research over the last twenty years has consistently shown positive – if not always consistent – valuations in surveys, experiments and imputed valuation studies.[4] Recent work has validated the idea that consumers have both intrinsic (independent of feedback effects) and reactive value to that flow.[5] However, absent an explicit promise not to collect data as "payment," or an explicit statute prohibiting certain practices, it is not well established that consumers have a general right to dictate the dispersion of the data flowing from them, nor is it clear that they are deprived of something of value just because that flow is captured. Unlike commercial piracy of intellectual property, for example, where there is an implicit but reasonable presumption of loss in licensing fees, it is not clear that individuals can generally monetize

2 Garrett Glasgow & Chris Stomberg "Consumer Welfare and Privacy in Antitrust Cases: An Economic Perspective" *Antitrust*, Vol. 35, No. 1, Fall 2020.

3 Hamermesh, Daniel S. "What's to know about time use?" Journal of Economic Surveys 30, no. 1 (2016): 198-203.

4 Acquisti, Alessandro, Curtis Taylor & Liad Wagman. "The economics of privacy." Journal of Economic Literature 54, no. 2 (2016): 442-92.

5 Lin, Tesary, Valuing Intrinsic and Instrumental Preferences for Privacy (June 29, 2019). Available at https://ssrn.com/abstract=3406412 or http://dx.doi.org/10.2139/ssrn.3406412.

access to their data. As the recent *TransUnion v. Ramirez* U.S. Supreme Court decision suggests, courts struggle with how to assign value to data problems that are real, but are abstracted from concrete, individualized outcomes.[6] Finally, consumers have heterogeneous preferences for privacy that are not necessarily all pointed in the same direction. A data flow that is costly to one consumer – revelation of a credit score for someone with bad credit – could be beneficial to another – revelation of a credit score for someone with good credit. Thus, the mere presence of an increase in data collection associated with particular practices is not necessarily evidence that consumers are made worse off by that practice.

Second, there may be indirect effects that can be linked to the misappropriation or misuse of consumer data. Citron and Solove provide a comprehensive overview of possibly applicable frameworks for injury.[7] Some of these potential injuries are relatively straightforward to value and assign liability for – for example, payment account thefts or credit misappropriation from first party mishandling – but Jin & Stivers, as well as many others, have discussed the difficulties that arise even in these cases.[8] Other realized injuries, including serious, and often attributable, effects from stalking, revenge porn, or serious and unwarranted reputational effects, are difficult to value in a consistent way. This difficulty is even greater when these injuries stem largely from violation of preferences for product attributes for which there is little market data (e.g., a preference that one's publicly accessible data cannot be collected by a particular kind of private party without assent).

Gains to the firm from the contested practices may be an easier to estimate alternative to basing monetary remedies on injury. In some cases, this is based directly on a preference for using gains – in the context of attempting to invoke complete deterrence – but may also appeal to the idea that gains and injury are logically tied together, as they are in legal discussions of equitable remedies.[9] The seeming common sense basis for conflating gains and injury may apply in positive-price fraud settings, where one party is simply stealing the price of a purported good or service from the other. In a business to business context, for example, one party's failure to pay for an IP license to another can be both the injury to the owner of the IP and gains to the non-payer. Equating gains and injury makes less sense in non-fraud settings, where at least some consumers may be willing to pay some positive amount (meaning that the entire price is not injury), and the firm has expended some legitimate effort to provide that valued good (meaning that the entire price is not gain). These costs to the firm and benefit to consumers are not equivalent, meaning that not only is market price an imperfect estimate of either injury or gain, but also that a more perfect estimate of one does also not necessarily yield a better estimate of the other. The presence of persistent, unanticipated welfare effects – as in many privacy cases – further delinks any relationship between a firm revenue and injury.

In the case of zero price products, firm gains from the collecting and processing consumer data often stems from a third-party interaction – e.g. selling access to the consumers' data to someone in a different market – so the value of that third party interaction to the firm may be completely unrelated to consumers' disvalue from the collection. For example, it is hard to articulate a link between the value that some parents place on not having their children's online activities tracked, and the revenue generated from placing tracked ads in front of those children.

6 In that case, records on individuals were, in fact, incorrect. However, for many members of the class, those errors had not left the database, and thus had not seemed to have a concrete effect on the lives of those members. https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf.

7 Citron, Danielle Keats & Solove, Daniel J., Privacy Harms (February 9, 2021). GWU Legal Studies Research Paper No. 2021-11, GWU Law School Public Law Research Paper No. 2021-11, Available at https://ssrn.com/abstract=3782222 or http://dx.doi.org/10.2139/ssrn.3782222.

8 Jin, Ginger Zhe & Stivers, Andrew, Protecting Consumers in Privacy and Data Security: A Perspective of Information Economics (May 22, 2017). Available at https://ssrn.com/abstract=3006172 or http://dx.doi.org/10.2139/ssrn.3006172.

9 See SCOTUS opinion in *Liu v SEC* https://www.supremecourt.gov/opinions/19pdf/18-1501_8n5a.pdf.

II. REGULATORY MONETARY REMEDIES FOR PRIVACY PRACTICES

The difficulties in attribution and estimation of zero price privacy harms make tying monetary remedies to injury relatively unattractive to some policymakers because of the cost and uncertainty in imposing these remedies. However, tying monetary remedies proportionally to injury has attractive efficiency and incentive properties.[10] In the context of very complex networks of consumer data flows, where practices are often difficult to define, penalties that are tied to injury help focus firm incentives on mitigating expected harms when either the firm makes mistakes in following the law or the enforcement agency makes mistakes in applying it.[11] These incentives to reduce injury are lost when tying penalties to firm gains instead of harm.

Alternatively, penalties that are at least as large as the gains associated with the violative practices may be more likely to induce complete deterrence. A simplistic view might then suggest simply setting penalties high enough to ruin any company that was deemed to be in violation. However, in at least some contexts, regulatory language suggests a gentler approach. For example, both case law and statutory guidance for the Federal Trade Commission suggest that fines should not necessarily be higher than a firm can afford.[12] This caution may reflect a concern that both firms and regulators can make mistakes when the regulated practices are complex. To reduce exposure to those mistakes when enforcement is uncertainty, firms may have incentives to over-invest in compliance, meaning that they incur greater expense in meeting the required standards, as penalties rise. In extreme cases, firms may simply choose not to serve a market, rather than risk penalties that are disproportionate to any profit they might expect.

In practice, the most prominent data protection efforts in the U.S. and EU rely on administrative fines/civil penalties that are not linked to whether money changes hands between consumer and firm or to estimates of gain or injury. This means that neither price, nor the existence or effects of a transaction involving the consumer need to influence the monetary remedy. With respect to welfare effects more generally – injury to consumers or gain to the violating firm – only the European Union's General Data Protection Regulation ("GDPR") provides any explicit, overarching reference to market-based welfare effects in assessing fines, and even that is limited to firm gains. The GDPR provides for administrative fines that are "effective, proportionate and dissuasive,"[13] suggesting that the motivation is for deterrence, levied by some consideration toward the costs of severe punishment. The regulation offers a variety of factors that should be considered in setting the fine, including some rough proxies for harm (nature, gravity and duration of infringement, categories of data affected), the culpability and cooperativity of the firm, and:

> "any other aggravating or mitigating factor applicable to the circumstances of the case, *such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement*." [emphasis added][14]

More famously, it allows maximum administrative fines keyed to the overall size and wealth of the company – up to 2 percent of global revenue (or EUR 10,000,000, whichever is higher) for more technical violations and up to 4 percent (or EUR 20,000,000) for practices that are more fundamental to the spirit of the rule. These limits appear not to be binding in practices, for example, Google's fine from 2019 amounted to something in the range of hundredths of a percent of global revenue ($57 million vs. $160 billion).[15]

In the U.S., the Federal Trade Commission has had some success bringing consumer data cases under its general Section 5 deception and unfairness authority that parallel at least some of the rights given by the EU and the states. Where privacy was clearly a salient attribute being sold for a positive price, the Commission has been able to obtain redress. For example, the Commission obtained $100,000,000 in equitable relief from Lifelock, Inc., where the Commission alleged that the data protective services sold by the company were deceptively advertised.[16] The Commission also obtained an $8,750,000 (reduced to roughly 10 percent for ability to pay reasons) judgement for equitable relief against Ashley Madison, a matching service for cheating spouses, where the Commission alleged both deceptive and unfair practices with respect to the

10 See Stigler, George J. "The Optimal Enforcement of Laws," Journal of Political Economy 78 no. 3 (1970) or, for a more recent overview, Polinsky, A. Mitchell & Steven Shavell. "The Economic Theory of Public Enforcement of Law." Journal of Economic Literature 38, no. 1 (2000): 45-76.

11 See, for example, the discussion of incentives in Cooper, James C., & Bruce H. Kobayashi. "An Unreasonable Solution: Rethinking the FTC's Current Approach to Data Security." George Mason Law & Economics Research Paper 20-23 (2020).

12 See 315 U.S.C. 45(m)(1)(C) "ability to pay," and *US v. Reader's Digest Ass'n Inc*, 494 F. Supp. 770 (D. Del 1980) "the defendant's ability to pay."

13 GDPR Article 83 1.

14 GDPR Article 83 2 (a)-(k).

15 See "18 Biggest GDPR Fines of 2020 and 2021 (So Far)" published May 21, 2021. Accessed July 23, 2021. https://www.tessian.com/blog/biggest-gdpr-fines-2020/. TIM data Statistica EUROPE IDATE DigWorld; 2016. H&M data Statistica Annual Report 2020. Google data Alphabet Annul Report 2020.

16 See case summary and documents at https://www.ftc.gov/enforcement/cases-proceedings/072-3069-x100023/lifelock-inc-corporation.

privacy of user data.[17] However, application of this authority to gain equitable relief to cases where privacy as less obviously being paid for – either because of saliency or because of a zero price – seems to have been less successful. More recently, even this limited authority for equitable monetary remedy was removed by the U.S. Supreme Court's ruling against the Commission in *AMG v. FTC*.[18]

Even before that ruling, the Commission had been increasingly aggressive in using rule or order violations to trigger civil penalties. Most notably, it extracted $5 billion from Facebook for alleged violations of a 2012 FTC order relating to how it presented privacy controls to its users.[19] This judgement came after widespread coverage of Cambridge Analytica's ability to capture user data (including "friends of friends" data) without permission. The Commission took $170 million from Google/YouTube for alleged COPPA (Children's Online Privacy and Protection Act) violations. In that case YouTube was accused of capturing data from users that it should have known were likely to be children without getting parental assent, or providing any of the other COPPA requirements. For COPPA and order violations the Commission can extract up to about $43,000 per violation. Statutory guidance allowing civil penalties for violations does not mention either injury or ill-gotten gains, although there may be case law that supports consideration of injury in some contexts.[20] The Commission has not given any public accounting of its penalty calculations for these cases, so again, the deterrent signal is not clear.

Three states within the U.S. have passed comprehensive data protection statutes, California, Virginia, and Colorado. Notably, the U.S. variants provide substantially less guidance than GDPR or even U.S. federal authorities with respect to penalties. The California Consumer Privacy Act allows the state to pursue maximum civil penalties per violation of $2500 for unintentional and $7500 for intentional (or related to a minor).[21] The only guidance given is for the state to consider "good faith" on the part of the business.[22] The Colorado Privacy Act does not specify civil penalty amounts that the state can impose. However, the Colorado Consumer Protection Act (which applies to at least some of the relevant privacy practices) allows for penalties up to $20,000 per violation ($50,000 against an elderly person), with the total penalty not to exceed $500,000. The Virginia Consumer Data Protection Act also provides the state with authority to impose civil penalties up to $7,500 per violation.[23] None of the privacy statutes provide any additional guidance on calculating penalty amounts. They are all too new to have provided any useful examples of how they will be used in practice for monetary remedies.

In addition to fines or penalties, some privacy regulations also allow for private right of action. Private rights of action may in many cases serve primarily as avenues for redress. However, in the zero-price privacy space, private rights of action have also provided for recovery of statutory damages, which do not necessarily require any assessment of realized harm. For example, the GDPR allows a private right of action to recover "material, or non-material," damage with minimum statutory damage of EUR 500.[24] The question of exactly what "non-material" means seems not to have been yet resolved, but it at least opens the door to injury with zero-price products with no obvious, realized, and attributable feedback effect to the consumer. California's CCPA also allows for private rights of action and allows minimum statutory damages of between $100 and $750 per consumer per incident or the actual damages, whichever is greater in the context of a data breach. For statutory damages CCPA directs the court to consider a variety of factors, some of which could be taken as very rough proxies for injury.[25] The act also directs courts to consider the wealth of the company. If a business sells consumer data that has been opted out of, consumers can also pursue statutory damages of between $1000 and $3000 per incident, or actual damages, whichever is greater. Neither Colorado nor Virginia allow a private right of action.

17 See case summary and documents at https://www.ftc.gov/enforcement/cases-proceedings/152-3284/ashley-madison.

18 *AMG CAPITAL MANAGEMENT, LLC, ET AL. v. FEDERAL TRADE COMMISSION* https://www.supremecourt.gov/opinions/20pdf/19-508_l6gn.pdf.

19 See https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

20 15 U.S.C sec. 45(m)(1)(C). "In determining the amount of such a civil penalty, the court shall take into account the degree of culpability, any history of prior such conduct, ability to pay, effect on ability to continue to do business, and such other matters as justice may require." See also "Statement of Commissioner Noah Joshua Phillips, *FTC v. HyperBeard, Inc., et al* Matter No. 1923109" June 4, 2020, citing *U.S. v. Dish Network, L.L.C.*, No. 17-3111, slip op. at 16 (7th Cir. Mar. 26, 2020). See also *US v. Reader's Digest Ass'n Inc*, 494 F. Supp. 770 (D. Del 1980).

21 TITLE 1.81.5. California Consumer Privacy Act of 2018, 1798.199.90

22 TITLE 1.81.5. California Consumer Privacy Act of 2018, 1798.155.

23 Code of Virginia Title 59.1 Chapter 53 Section 59.1-584.

24 GDPR Article 832 para.1 "Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered."

25 Title 1.81.5 California Consumer Privacy Act of 2018, 1798.150 (a)(2) "In assessing the amount of statutory damages, the court shall consider any one or more of the relevant circumstances presented by any of the parties to the case, including, but not limited to, the nature and seriousness of the misconduct, the number of violations, the persistence of the misconduct, the length of time over which the misconduct occurred, the willfulness of the defendant's misconduct, and the defendant's assets, liabilities, and net worth."

For private cases brought under federal regulation in the U.S., the Supreme Court has recently increased the barrier to recovering damages when alleged injury is more difficult to tie to the practices and the individual.[26] Where statutory damages are allowed, independent of realized harm, the incentive effect of the firm is similar to civil penalties – the firm will need to assess whether the increased cost of ensuring against errors – its own, enforcers and the courts – weighs against the value of entering the market.

All these approaches of regulation bearing on privacy and consumer data sidestep the actual welfare effects of violations of the statutes. That is, they key to neither ill-gotten gains, nor to realized injury. Even the private rights of action, including federal, have called for statutory damages, with realized damages as backup. As discussed below, there are real difficulties in assigning and assessing injury with respect to privacy in general, and zero price products in particular, so this is not a surprising direction for civil penalties to take. However, as this paper argues, this may be a problem for the usual reasons.

III. DISCUSSION

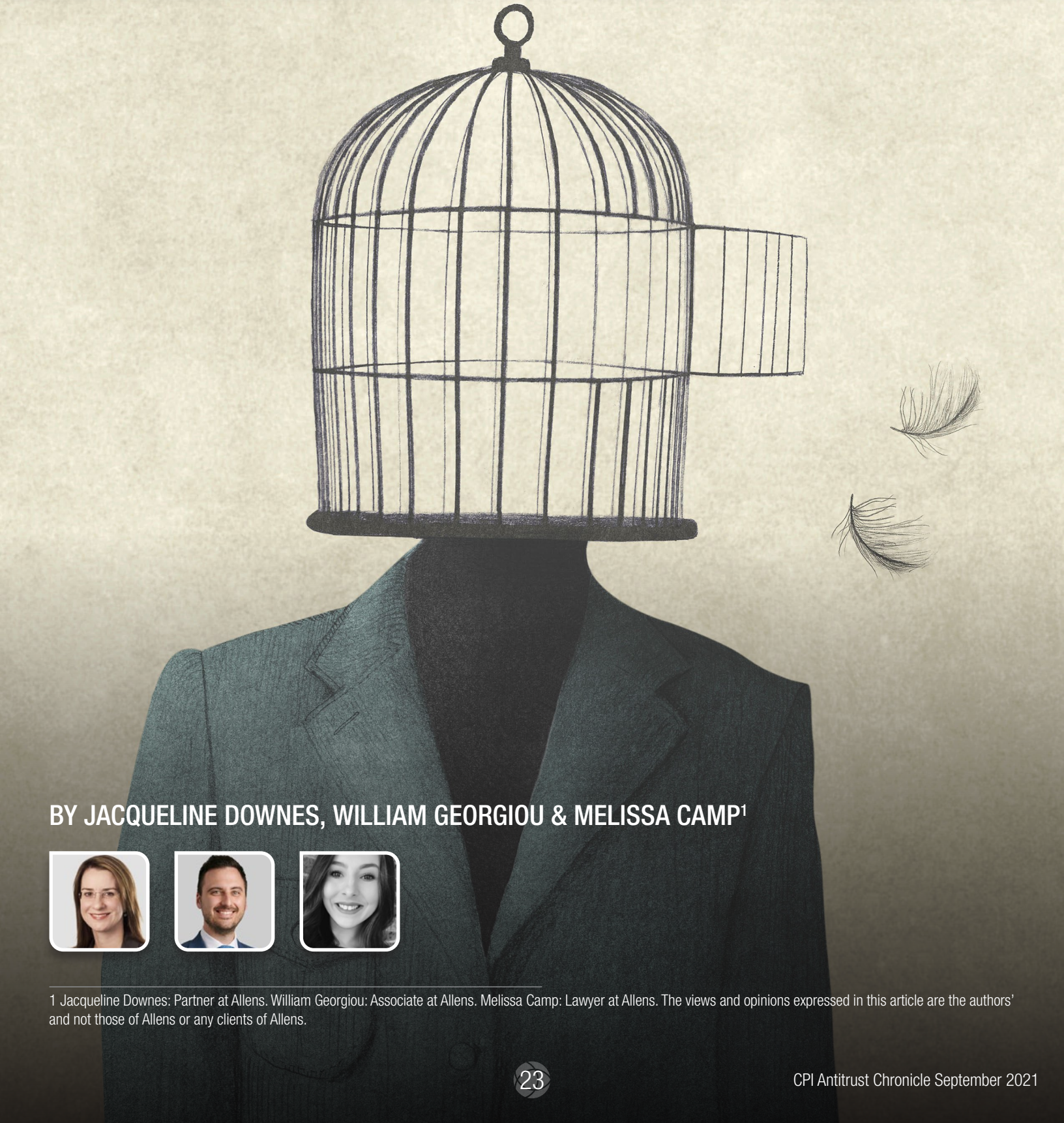
The above discussion suggests that for monetary remedies on zero price privacy practices, regulators have elevated deterrence and relatively easy implementation over proportionality and efficiency. In application, the actual assessed fines could be influenced by welfare considerations, but enforcers have little guidance in how to implement proportionality, or why it might be important. Without that guidance, and without details of how enforcers calculate and apply penalties, regulators are left with several possible problems. First, lack of transparency or guidance means that penalties are more at risk of inconsistency, which could be driven by a variety of unwanted influences, including from unrelated political disfavor or regulatory capture. Second, without a process for evaluating data on harms or gains that could help reduce the cost to legitimate operations without significantly reducing deterrence, the first issue is likely exacerbated. Lastly, the deterrent signal of civil penalties that are not clearly tied to injury or gains are more difficult for potential future violators to read. While some observers may see the increased uncertainty as more likely to induce complete deterrence, this is not without cost, as discussed above. In addition, it is not clear that the penalties that are assessed can be interpreted as encouraging complete deterrence. For example, the $170 million penalty given to YouTube in its COPPA case could be viewed as small (less than 1 percent) relative to YouTube's $20 billion ad revenue from 2020, but the public does not know its relationship to the profit or revenue generated by the specific practices at issue, nor to any estimate of injury associated with those practices. Because of this, observers cannot necessarily interpret the magnitude of the compliance costs and risks associated with providing COPPA-related data services and products.

At a minimum, more explicit regulatory guidance on appropriate deterrence and efficiency related inputs to penalties would help improve the deterrence signal to potential violators and reduce inconsistency – whether driven by lack of inputs or by improper influences. But, ideally, welfare considerations would be built into the construction of monetary remedies directly, so that these penalties have the greatest chance of appropriate deterrence while being less disruptive to legitimate activity. While regulators may be concerned that binding penalties to welfare considerations will make the costs of implementing penalties prohibitive, given the difficulties discussed above, there are possible solutions. For example, regulators may be able to use reasonable presumptions about injury or gains based on available data that would be rebuttable by sound empirical analysis.

As a final note, it is important to remember that because society is still at the very beginning of this revolution in data flows, we do not have a good understanding of where it is going to take us, either in outcomes or in preferences over those outcomes, as markets, society and individuals adapt. As noted above, there is plenty of research suggesting that consumers care about their data flows, but also plenty that suggests consumer knowledge and decision making, much less regulatory expertise, are not yet mature. As consumers and policy makers gain experience, and more data is collected and analyzed on risks, preferences, and values over consumer data flows, it may be possible to better calibrate monetary remedies for efficiency. Tying regulation generally, and monetary remedies in particular to empirical estimations of injury would help make current regulation more flexible, and robust to that evolution.

26 *TRANSUNION LLC v. RAMIREZ:* https://www.supremecourt.gov/opinions/20pdf/20-297_4g25.pdf.

FREE ISN'T FREE: DIGITAL PLATFORM DATA PRACTICES AND AUSTRALIA'S UNFOLDING REGULATORY RESPONSE



BY JACQUELINE DOWNES, WILLIAM GEORGIOU & MELISSA CAMP[1]

1 Jacqueline Downes: Partner at Allens. William Georgiou: Associate at Allens. Melissa Camp: Lawyer at Allens. The views and opinions expressed in this article are the authors' and not those of Allens or any clients of Allens.

Consumers often exchange their personal data for "free" access to a digital service on one side of the market while the relevant digital platform sells that data (including after combining it with the consumer's data across other services) to customers on the other side of the market. This multi-sided exchange has led to a variety of benefits. These include increased digital participation, economies of scale and innovations and efficiencies. However, such services are arguably not "free" in reality: because consumers effectively trade their attention and data for access to content and services. In recent years the accumulation of vast amounts of data by digital platforms through this exchange has created challenges for governments and regulators: the accumulation of this data has allowed platforms to cement incumbency through network effects. Given the strong network effects present in such markets, there are concerns that there may be little room for alternative platform operators to supply consumers services that increase privacy or enhanced control over the way data is obtained, used, combined or sold.

With that context in mind, this article:

- Discusses the potential competition and consumer (i.e. privacy) risks presented by the "free" model and associated data collection practices, including those identified by Australia's competition regulator, the Australian Competition and Consumer Commission ("ACCC");
- Discusses how these potential competition and consumer risks are being managed in Australia, including via continued ACCC inquiries and enforcement actions (specifically via the use of Australia's consumer protection law rather than its competition law);
- Discusses the international trend towards *ex ante* regulation of digital platforms, including in Europe, the UK and the U.S.; and
- Opines on whether the ACCC is also likely to consider the effectiveness of an *ex ante* regime in Australia.

I. THE RISKS WITH "FREE"

While some digital platforms collect subscription or membership fees for a paid version of their services, such as YouTube Premium and LinkedIn Premium, many platforms provide valuable services to consumers at zero financial cost.[2] Indeed, many important digital services are offered to customers for no monetary cost.

Use of these services has facilitated social, educational and workplace participation, especially throughout the COVID-19 pandemic. These services allow knowledge, ideas, and creativity to be shared instantaneously worldwide. The business model opens up markets in a way that was not previously possible by driving down barriers to user access, thereby encouraging wide-spread uptake. In turn, a digital platform gains access to enormous quantities of consumer data which can be leveraged in the supply of advertising or other services to subsidise the "free" service or the platform's ecosystem more broadly.[3] In this respect, price is charged asymmetrically across the two markets making it difficult to gauge the actual price paid by consumers when utilising digital platform services.

Despite the transformational impact that these free digital services have had, concern continues to grow internationally regarding the risks to competition and consumer outcomes that the accumulation of data, and the expansion of data gathering and combination practices, by digital platforms (including via free services) is having.

Recognising these risks, in 2017, the ACCC commenced the Digital Platforms Inquiry, which was the first of its kind globally to scrutinise competition and consumer issues in digital markets. Since the release of its Digital Platforms Inquiry Final Report ("DPI Final Report") in 2019, the ACCC has continued to be active in investigating digital platform market issues in Australia. The ACCC established a specialist Digital Platforms unit.

In response to the ACCC's DPI Final Report and its various recommendations to consider strengthening Australia's competition, consumer and privacy laws, the Australian Government directed the ACCC to undertake an inquiry into digital advertising services. It also directed the ACCC to conduct a broader inquiry across a range of specific digital platform topics as part of an ongoing "Digital Platform Services Inquiry 2020-2025" ("DPSI").

2 ACCC, "Digital Platforms Inquiry Final Report," (July 26, 2019) p 376. Available at https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report ("DPI Final Report").

3 *Ibid.* p 376.

As part of the DPSI the ACCC consults on and produces bi-annual public reports to the Australian Government in respect of competition and consumer issues across digital markets of its choosing. For example, the first report of the DPSI considered online private messaging, search and social media services.[4] The second report considered mobile app marketplaces.[5] Following its consultation on an issues paper in March 2021, the ACCC is now preparing a third report on the issue of whether a choice screen for web browser services and search engines is necessary in Australia.[6] The ACCC also recently closed consultation in respect of what will be its fourth report which will investigate general online marketplaces (eg, Amazon, eBay, Kogan and Catch).[7]

II. THE POTENTIAL COMPETITION RISKS

The ACCC has found across its various digital inquiries that access to large amounts of user data can entrench a strong market position by creating significant barriers to entry and expansion.[8] A key finding in the DPI Final Report was that cross-side network effects operate to benefit both consumers and advertisers on either side of the digital platform. A positive feedback loop may therefore result and drive scale.[9] This feedback loop may compound network effects and raise barriers to entry and expansion, as consumers are less likely to switch to a new platform which provides worse quality or less tailored services as a result of a smaller aggregated data pool. This entrenches the position of a first mover platform.

Given this feedback loop, the ACCC identified as a potential trend the expansion of Google and Facebook into adjacent markets.[10] Expanding a data driven business into new areas from which additional user data can be collected makes commercial sense. Given the successes of the "free" model noted above, it also makes sense that data driven businesses continue to offer services for free to promote rapid user uptake. As explained by the ACCC:

> Businesses and, specifically, digital platforms can increase the amount of first party data collected by increasing the services provided to users. For example, Google now provides over 60 different online services that provide Google with over 60 different sources of first-party user data that may be combined and associated with a single user account.[11]

The ACCC has raised concerns that the expansion of online platforms into other markets provides additional opportunities to collect data and creates an ecosystem of products and services that interoperate, which may have the effect of raising costs for rivals, creating barriers to entry and allowing anticompetitive tying or bundling.[12] While it is not unlawful to use market power to move into adjacent markets and offer new services, it is unlawful to do so where the leveraging of power (e.g. data in one market) results in a substantial lessening of competition.[13]

---

4 ACCC, 'Digital Platform Services Inquiry Interim report September 2020' (October 23, 2020). Available at https://www.accc.gov.au/publications/serial-publications/digital-platform-services-inquiry-2020-2025/digital-platform-services-inquiry-september-2020-interim-report.

5 ACCC, 'Digital platform services inquiry Interim report No. 2 – App marketplaces March 2021' (April 28, 2021). Available at https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025/march-2021-interim-report.

6 ACCC, 'Digital Platform Services Inquiry – September 2021 Report on market dynamics and consumer choice screens in search services and web browsers Issues Paper March 2021' (11 March 2021). Available at https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025/september-2021-interim-report.

7 ACCC, 'Digital Platform Services Inquiry – March 2022 Report on general online retail marketplaces Issues Paper July 2021' (July 22, 2021). Available at https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platform-services-inquiry-2020-2025/march-2022-interim-report.

8 ACCC Chair, Rod Sims, speech at Global Competition Review Webinar, 'Platforms' dominance of apps market needs to be addressed' (August 19, 2021). Available at https://www.accc.gov.au/speech/platforms-dominance-of-apps-market-needs-to-be-addressed. ("GCR Speech").

9 DPI Final Report, p 67.

10 *Ibid.* pp 529 – 534.

11 *Ibid.* p 379.

12 ACCC, 'Digital Platform Services Inquiry Interim Report September 2020' (September 2020) pp 82 – 85. Available at https://www.accc.gov.au/system/files/ACCC%20Digital%20Platforms%20Service%20Inquiry%20-%20September%202020%20interim%20report.pdf.

13 Competition and Consumer Act 2010 (Cth) s 46.

III. THE POTENTIAL PRIVACY RISKS

Data driven platforms are incentivised to expand the amount of data collected and combined, including by increasing user uptake (such as by offering services for free), expanding into new services, obtaining larger data sets within services and aggregating pools of data. This is because the value of these platforms' services on the other side of the market (e.g. advertising) increases as they do so. These incentives have a number of privacy implications. The ACCC's observations on the privacy implications of digital platforms' data practices include the following:

- Many digital platforms can collect a large amount and variety of data on a user's activities beyond what the user actively provides while they are using the digital platform's services. Digital platforms often have broad discretions in how they use and disclose this data;[14]
- Many consumers do not understand which data is actually collected and how it is used. Often they are unable to opt out of data collection, meaning they must forgo use of that service altogether if they wish to avoid providing access to their data;[15]
- In a consumer survey commissioned by the ACCC, more than three in four digital platform users surveyed (77 percent) considered the tracking of their online behaviour to be a misuse of their personal information if it is used to create profiles or enable targeted advertising;[16]
- Presenting consumers with services marketed as "free" in the form of a clickwrap agreement can exploit behavioural biases that lead consumers to provide their consent to a transaction without informing themselves of the content of the terms and conditions and without due regard to these other potential costs of providing their user data;[17]
- Given the value provided by user data to the business models of digital platforms, including for product development and targeted advertising, digital platforms are not incentivised to encourage consumers to opt-out of their collection, use or disclosure of user data. Digital platforms are however incentivised to convey an impression that they offer consumers significant control over the collection, use and disclosure of their user data;[18] and
- Digital platforms emphasise to users that they may control privacy settings. These options can however give users an impression of granular control over the sharing of their data without actually providing options for less data collection.[19]

It seems unlikely that a heavily data driven business would voluntarily scale back data collection practices to offer greater user privacy. This may be because, for example, in the case of search:

> [C]harging even only a penny for the use of Google's engine may turn away many users, which then reduces the value of ad placement and of keywords. So the economic incentives are for Google, for example, to decrease its price on the side of users in order to increase the value of the products it sells to advertisers, and so increase the price on the advertisers' side.[20]

14 DPI Final Report, p 374.

15 GCR Speech.

16 DPI Final Report, p 389.

17 *Ibid.* p 395.

18 *Ibid.* p 423.

19 *Ibid.* p 425.

20 See G. Roger, 'Digital Platform Inquiry submission as a comment' (January 31, 2019) p 11. Available at https://www.accc.gov.au/system/files/Guillaume%20Roger%20%28January%202019%29.PDF.

IV. HOW ARE POTENTIAL COMPETITION AND CONSUMER RISKS BEING MANAGED IN AUSTRALIA?

> *In respect of the competition and privacy issues identified above, the ACCC has brought a variety of enforcement cases. Reflecting on such cases brought by the ACCC, Mr Sims stated that "these enforcement actions are about holding powerful digital platform businesses accountable for their representations to consumers and ensuring consumers are fully aware of the price they pay, through their data, for the supposedly free services they receive."*[21]

However, while the ACCC has indicated it is investigating ant-competitive conduct, to date competition law cases regarding digital platform issues have only been brought by private litigants. For example:

- In May 2018, Unlockd instituted proceedings in Australia, alleging Google misused its market power when it threatened to block its app, "Unlockd Rewards,"[22] from accessing the Google Play Store and AdMob. Unlockd alleged Google's conduct had the substantial purpose, effect or likely effect of substantially lessening competition in markets for the publication of advertisements on Android mobile devices; mobile devices; and/or online. Justice Moshinsky found that Unlockd had a prima facie case to be tried, and granted an interim injunction against Google. Unlockd however went into voluntary administration (citing Google's conduct as the cause) and ultimately discontinued the proceedings;[23]

- In April 2019, start-up Dialogue Consulting instituted proceedings against Facebook (and Instagram) in Australia, alleging Facebook misused its market power when it deactivated Dialogue's platform access for alleged breaches of platform guidelines. Dialogue provides a service that automatically logs in and out of Facebook and Instagram accounts and allows users to schedule posts. Dialogue's claim alleges that Instagram was refusing Dialogue access to its platform in an attempt to steer users towards Instagram's own products. This case is ongoing;[24]

- In November 2020, Epic Games instituted proceedings against Apple in Australia, alleging that Apple engaged in anticompetitive conduct, including by requiring that iOS (Apple's mobile device operating system) app developers only distribute iOS apps through Apple's "App Store," and that certain iOS developers only use Apple's in-app payment processing system and pay a 30 percent commission for all sales of in-app content. Epic Games brought similar proceedings against Google in March 2021. These cases are ongoing and follow similar ongoing cases instituted by Epic Games overseas.

The ACCC did challenge Google in the context of the ACCC's public review of Google's (then) proposed acquisition of Fitbit. On June 18, 2020, the ACCC expressed preliminary competition concerns with the transaction, including that it would substantially lessen competition in the supply of data-dependent health services or the supply of certain ad tech services in Australia that rely on the collection and analysis of large amounts of individual data (and in particular those services which enable targeting of online display advertising to consumer segments).[25] The ACCC rejected a behavioural undertaking proposed by Google. Google proposed that it would not, among other things, use health data for advertising (the EC however accepted a similar undertaking). Google completed the transaction on January 14, 2021 before the ACCC finished its merger investigation. The ACCC noted that the matter had become an enforcement investigation of a completed merger.[26]

Against the backdrop of exclusively private competition law litigation against digital platform issues, the ACCC has commented that it considers Australia's competition laws are insufficient to deal with digital platforms leveraging or misusing their market power (including

---

21 ACCC Chair, Rod Sims, speech at Australia-Israel Chamber of Commerce, 'The ACCC's Digital Platforms Inquiry and the need for competition, consumer protection and regulatory responses (August 6, 2020). Available at https://www.accc.gov.au/speech/the-acccs-digital-platforms-inquiry-and-the-need-for-competition-consumer-protection-and-regulatory-responses.

22 Unlockd's mobile app allowed consumers to, among other things, obtain discounts on their telecoms services by watching ads when they unlock their phone screen.

23 ABC, "Unlockd advertising start-up blames Google as it goes into voluntary administration" (June 13, 2018). Available at https://www.abc.net.au/news/2018-06-13/unlockd-enters-voluntary-administration-blames-google/9863596.

24 *Dialogue Consulting Pty Ltd v Instagram, Inc* [2020] FCA 1846 (Application filed April 2019).

25 ACCC, Statement of Issues in Google/Fitbit, p 3. Available at https://www.accc.gov.au/system/files/public-registers/documents/Google%20Fitbit%20-%20Statement%20of%20Issues%20-%2018%20June%202020.pdf.

26 See ACCC, *Google LLC proposed acquisition of Fitbit Inc,* public register. Available at https://www.accc.gov.au/public-registers/mergers-registers/public-informal-merger-reviews/google-llc-proposed-acquisition-of-fitbit-inc.

into adjacent markets) and issues that arise from a lack of transparency of these platforms' data practices.[27] Speaking at a recent Global Competition Review webinar (the "GCR Speech"), Mr Sims noted that the reason competition law is often inadequate to address competitive concerns associated with digital platforms because of "*the necessary narrowness of the cases [brought to court], and the length of time taken to investigate and enforce competition law.*"[28] The length of time taken to investigate and enforce contraventions of the competition law in particular has significant consequences in digital markets where dominant digital platforms can rapidly leverage consumer data to expand into adjacent markets.

In this context, the ACCC has instead relied on Australia's consumer protection framework. For example:

In April 2021, the Federal Court handed down its judgment in *Australian Competition and Consumer Commission v Google LLC (No 2)*.[29] This case was the first in the world to probe Google's approach to the collection of users' location data. In this case, the Court commented that a user who read all of the available information provided by Google would probably not have been misled by its practices.[30] However, the Court ultimately found that most consumers will not carefully read the contents of privacy policies.[31] It also found that the choice architecture used by Google on the mobile screen display, including presenting consumers with default settings switched to "on" and "off," would have misled consumers into thinking that their location data would not be collected in certain situations.[32]

On 27 July 2020, the ACCC instituted proceedings against Google, alleging that Google misled consumers.[33] Following Google's acquisition of DoubleClick in 2008, Google stated in its privacy policy up to 2015 that it "*will not combine DoubleClick cookie information with personally identifiable information unless we have your opt-in consent.*"[34] Despite this, in 2016 Google changed its privacy policy to allow for the combination of these sets of data,[35] and prompted consumers to agree to this change with a pop-up notification displaying the text "I agree." The ACCC argues that the "I agree" notification was misleading because consumers could not have properly understood the changes it was making or how their data would be used, and so did not – and could not – give informed consent. In this case the ACCC also alleges that through combining the datasets, Google improved the profitability of its advertising business because this combined data is particularly valuable for advertisers who are seeking to target particular audiences – this allegation however was not paired with a competition law argument.

On December 16, 2020, the ACCC instituted proceedings against Facebook, alleging that Facebook misled consumers.[36] The ACCC alleges that Facebook made representations to consumers that its Onavo Protect app would keep users' personal activity data private, protected and secret, and that it would not use the data for any purpose other than providing Onavo Protects products. The ACCC also alleges however that Onavo Protect collected, aggregated and used significant amounts of users' personal activity data for Facebook's commercial benefit. This included details about Onavo Protect users' internet and app activity, including records of every app the consumer accessed on their device and the number of seconds each day they spent using those apps.

While these cases may result in more transparent data collection and use statements being made to consumers by digital platforms, they do not address the potential underlying competition and privacy risks noted above. The incentives to expand data collection, use and aggregation practices continue to exist. While the use of the consumer law achieves better disclosure of these practices by the digital platforms, it does not prevent the practices from occurring.

---

27 DPI Final Report, pp 138 – 139.

28 ACCC, Rod Sims, 'Platforms' dominance of apps market needs to be addressed' (August 19, 2020) (*GCR Speech*). Available at https://www.accc.gov.au/speech/platforms-dominance-of-apps-market-needs-to-be-addressed.

29 *Australian Competition and Consumer Commission v Google LLC (No 2)* [2021] FCA 367

30 *Ibid.* [227].

31 *Ibid.* [338].

32 *Ibid.* [326], [330].

33 ACCC, "ACCC alleges Google misled consumers about expanded use of personal data" (July 27, 2020) ("*ACCC Google/DoubleClick*"). Available at https://www.accc.gov.au/media-release/correction-accc-alleges-google-misled-consumers-about-expanded-use-of-personal-data.

34 See e.g. Google, Privacy Policy (August 19, 2015). Available at https://policies.google.com/privacy/archive/20150819?hl=en-US.

35 Google, Privacy Policy (June 28, 2016). Available at https://policies.google.com/privacy/archive/20160628?hl=en-US.

36 ACCC, "ACCC alleges Facebook misled consumers when promoting app to protect users data" (December 16, 2020). Available at https://www.accc.gov.au/media-release/accc-alleges-facebook-misled-consumers-when-promoting-app-to-protect-users-data.

V. THE TREND TOWARDS AN *EX ANTE* REGIME

Recognising the difficulty in using traditional competition law and policy to regulate digital platforms, numerous international jurisdictions are moving to introduce *ex ante* regulatory regimes in digital markets. The European Union is considering the proposed Digital Markets Act ("DMA") which, if passed, will establish a targeted *ex ante* regulatory regime that provides certain designated core digital platform services with a clear framework of "dos and don'ts." In relation to data specifically, the DMA introduces the following measures for designated digital platforms:

- Do: provide effective portability of data generated by a business or a consumer to that business or consumer,[37] and provide businesses access to high-quality, continuous, and real-time access to aggregated and non-aggregated data generated by that business on the relevant digital platform.[38]

- Don't: combine personal data sourced from multiple different services offered by the digital platform,[39] or use non-public generated by a business on its platform to compete with those businesses.[40]

More recently, the UK Government has released a consultation paper outlining its proposal to introduce its own *ex ante* regulatory regime for digital markets.[41] The consultation paper proposes to empower the UK Competition and Markets Authority's Digital Markets Unit to implement "codes of conduct" and "pro-competitive interventions" against platforms with "Strategic Market Status." Interventions may include "*measures to overcome network effects and barriers to entry/expansion through mandating interoperability, third-party access to data, or certain separation measures.*"[42]

Germany's legislature amended Germany's competition laws, introducing specific *ex ante* competition rules for digital platforms that have paramount significance for competition across markets.[43] First, Germany's Bundeskartellamt can declare that a company is active on multi-sided or platform markets and that it has paramount significance for competition across markets. Second, the Bundeskartellamt may also issue a prohibition order. This order prohibits a range of conduct by a declared platform, including: self-preferencing, impeding downstream/upstream competitors, impeding potential competitors, using competitively sensitive data to create barriers to entry and refusing interoperability or data portability.[44]

The US House Judiciary Committee has also passed a six-bill reform package which is aimed at increasing regulation of digital platforms. The legislative package includes the *American Choice and Innovation Online Act* bill. It seeks to establish an *ex ante* regulatory regime similar to that proposed in the EU,[45] with similar interoperability and access requirements and prohibitions on the combination and use of personal data in the competitive process.[46]

In his GCR Speech, Mr Sims referred to these (and other) international regulatory developments and said they "*… could bring greater transparency, competition and fairness to digital markets*." He also said:

---

37 Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (December 2020) Art 6(h) ("DMA"). Available at https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN.

38 *Ibid*. Art 6(l).

39 *Ibid*. Art 5(a).

40 *Ibid*. Art 6(a).

41 UK Government, Consultation Paper "A new pro-competition regime for digital markets" (July 2021). Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1003913/Digital_Competition_Consultation_v2.pdf.

42 *Ibid*. paragraph 104.

43 Tenth Act Amending the Act against Restraints of Competition for Competition Law 4.0 (ARC-Digital Competition Act), approved by the German Bundestag on 14 January 2021 and coming into force GWB Digitization Act or 10th Amendment to the German Act against Restraints of Competition. ARC Amendments

44 See s 19a(2), Acts against Restraints of Competition (Competition Act – GWB) s 19a(2), available here.

45 *American Choice and Innovation Act* available at https://cicilline.house.gov/sites/cicilline.house.gov/files/documents/American%20Innovation%20and%20Choice%20Online%20Act%20-%20Bill%20Text.pdf. The other bills are: *Platform Competition and Opportunity Act*; *Ending Platforms Monopolies Act*; *Augmenting Compatibility and Competition by Enabling Service Switching Act*; *State Antitrust Enforcement Venue Act*; and *Merger Filing Fee Modernization Act*.

46 DMA, Art 6(a).

In Australia, our own work at the ACCC must be tailored to match our own issues and concerns. But although the finer details of our approaches may vary, competition authorities must align our approaches as much as possible.

This will include alignment around up-front regulation and rules, as well as enforcement and merger control.

The competitiveness, and the level and type of innovation in our economy, requires this.

It is clear from these comments and Mr Sims' responses during the Q&A portion of the GCR webinar that the ACCC is keeping a close eye on these developments. Mr Sims called for work to be done in multilateral (e.g. the ICN and OECD) and also bilateral forums to compare and synthesize each regulatory approach to work towards this alignment.

VI. WHAT IS NEXT FOR AUSTRALIA

The ACCC signalled in the DPI Final Report that it would revisit the introduction of data portability and interoperability requirements in the future if it considered requirements would be beneficial in addressing issues of market power and competitive entry or switching.[47] The ACCC recognised that "*aside from addressing issues of market power, portability of data held by digital platforms may deliver significant benefits to current and potential future markets including through innovation and the development of new services.*"[48] The ACCC is likely to pursue this line of inquiry further through its DPSI and may potentially broaden the scope of the measures it considered necessary to address issues of market power and deliver benefits to the competitive process.

Further, considering the international trend towards *ex ante* regulation of digital platforms, it is likely that the ACCC will follow its international counterparts and consider recommending some form of *ex ante* regulation. In his recent GCR Speech, Mr Sims commented that, to address the global impact of dominant digital platforms, competition authorities globally must work to align their approaches as much as possible.[49] Mr Sims also announced, in an opening address to the Law Council of Australia that focused on the ACCC's 'conversation starters' for merger reform in Australia, that the ACCC would consult in early 2022 via the DPSI on whether digital platform specific merger rules are needed, their particular design (if needed) and whether they "[N]eed to sit alongside wider sector specific rules to govern the conduct of digital platforms in order to address the competition and consumer concerns present in digital platform markets.".[50] In the interim, we anticipate the ACCC will continue to rely on the consumer law to tackle the competition and privacy risks arising in digital markets, issues which often relate to "free" services.

47 DPI Final Report, p 30.

48 *Ibid.*

49 GCR Speech.

50 ACCC, Rod Sims, "Protecting and promoting competition in Australia," Competition and Consumer Workshop 2021 - Law Council of Australia (August 27, 2020). Available at https://www.accc.gov.au/speech/protecting-and-promoting-competition-in-australia.

FREE AS AIR?

BY SALIL K. MEHRA[1]

1 Charles Klein Professor of Law and Government, Temple University, Philadelphia, USA, smehra@temple.edu. All errors and omissions are mine.

"Free as air; that's what they say – 'free as air.' Now they bring me my air in an iron barrel."
– Evelyn Waugh, Brideshead Revisited

The "rule of threes" recognizes that a person can survive three weeks without food, three days without water, but only three minutes without air.[2] At the end of Evelyn Waugh's *Brideshead Revisited*, a nobleman who has lived a dissolute life fairly free from the constraints of money or social norms gets his comedown in the shape of respiratory reliance on costly machinery. COVID-19 has forced us to consider the freedom, in several senses, of our very breath.

It has long been said that "there ain't no such thing as a free lunch."[3] While the word "free" has several related meanings, they have in common the notion of being unconstrained, whether by a financial cost, physical bond, or legal or other restraint. Though popularized by the science fiction writer Robert Heinlein, the "free lunch" is believed to refer originally to the practice in 19th century American saloons of providing their customers with a "free lunch" consisting of a buffet of well-salted food likely to provoke further drinking. Free drinks were sometimes provided as well for youth, since, as the Brewers' Association proclaimed, "[a] few cents on free drinks for boys was a good investment; the money would be amply recovered as these youths became habitual drinkers!" However, the free lunch was often monitored by the tavern's bouncer to discourage too much eating[4] – an early example by which a high-consumption user might, literally, find himself "throttled."[5]

No payment now, but we *will* get you later is not anyone's definition of "free." Nor do many consider to be "free" a good or service provided at no charge if you buy another product – you cannot successfully respond to a "buy one, get one free" offer by saying, "I'll take only the free one, thanks!" In a similar vein, "free" should not limit antitrust, to the extent that free lunches are not a thing. "Free" goods and services often involve several kinds of "payment." First, and perhaps most familiarly, individuals trade personal data that benefits the seller for these "free" products – so not at all free, just "no-monetary-payment" required. Second, individuals receive "no-monetary-payment" products but thereby "lock in" other individuals, who "pay" instead. Finally, "free" products that trigger dopamine or other behavioral responses may alter individuals' brains to their detriment, as 19th century saloon owners knew. Just as we might take the air we freely breathe for granted, until it suddenly turns potentially COVID-19 infective, we might consider that so-called "free" services may only be such at that instant, with possibly expensive consequences.

I. NO-MONETARY-PAYMENT IS NOT NECESSARILY "FREE"

The law, especially that of contracts, has long recognized that not having to pay money is not the same thing as "free." If you provide a pharmaceutical company data on your body's reactions in a drug trial, its promise to give you a supply of its products in exchange is not a gift.[6] This is unsurprising; you have provided the company a benefit, at its request.[7] Despite that, it is not rare to read someone arguing that antitrust action against services that platforms provide to consumers without payment must be misguided – a trope that goes back to the turn-of-the-century *Microsoft* litigation.[8] Indeed, the respected antitrust economist Hal Varian has recently argued, in connection with the Department of Justice's ongoing action against Google, that the latter is no monopolist, despite an 80 percent market share in search, on the grounds that it offers a high-quality service to consumers "for free."[9]

2 Colin Towell, *Essential Survival Skills,* p.154 (Penguin, 2011).

3 Mark Edward Lender & James Kirby Martin, *Drinking in America: A History,* p.104 (Free Press, 1982).

4 *Id.*

5 "Throttling" has been used metaphorically to refer to ISPs' constraining the use of those customers who, in the ISPs' view, excessively use "unlimited" data. See, e.g. Jon Brodkin, *Verizon Throttled Fire Department's "Unlimited" Data during Calif. Wildfire,* Ars Technica, Aug. 21, 2018 (reporting allegations in lawsuit against Verizon), *at* https://arstechnica.com/tech-policy/2018/08/verizon-throttled-fire-departments-unlimited-data-during-calif-wildfire/.

6 *Dahl v. HEM Pharmaceuticals*, 7 F.3d 1399 (9th Cirl 1993) (pointing out precedents for this view going back to *Hamer* v. *Sidway* (N.Y. 1891)).

7 See Restatement (Second) of Contracts (American Law Institute, 1981), Section 71.

8 See, e.g. Joe Kennedy, *The Myth of Data Monopoly: Why Antitrust Concerns About Data Are Overblown*, Info. Tech. & Innovation Found. 1, 25 (2017), http://www2.itif.org/2017-data-competition.pdf [https://perma.cc/5QH8-V5TK] (arguing against antitrust action because "many data-rich companies offer free or low-cost services that are extremely valuable to billions of people, most of whom have a pretty good idea of what data they are providing companies and how it might be used."); J. Gregory Sidak, *Do Free Mobile Apps Harm Consumers?,* 52 San Diego L. Rev. 619, 625 (2015) (answering the title negatively).

9 "Google Case is a Chance to Reframe Antitrust Debate," Financial Times, Oct. 21, 2020 (describing Varian's argument).

To some extent, serious antitrust discussion has long treated the "for free" argument as hollow. This idea was rebuffed by the district court in *U.S. v. Microsoft* more than 20 years ago,[10] based on the intuition that a firm cannot make money giving things away for free, so there must be some "catch"—"in other words, there ain't no such thing as a free lunch." More recently, social media and other Internet-based platforms have promoted a deeper understanding of no-payment services. Most prominently, Professor John Newman has provided in-depth examination of what he calls, not free, but "zero-price" markets, and introduced a taxonomy of consumer-facing costs to watch out for. In particular, he emphasizes a focus on costs to consumers that provide market signals as a keystone for antitrust enforcement.[11]

Fortunately, it appears that version of "free" in which users "pay" producers benefits in non-monetary ways has been rejected as grounds for an "antitrust-free zone." First, the European Commission's Directorate-General for Competition, and now the U.S. antitrust authorities, have focused their attention on Facebook and Google, both of which offer consumers myriad services without monetary payment. This energized scrutiny extends to the critical area of merger review – witness the FTC's challenge of Facebook's proposed acquisition of Giphy.[12] While the endgame of this revitalized enforcement awaits us, it seems as though the no-monetary-cost version of "free" may be done as a get-out-of-antitrust-enforcement card.

II. MAKING SOMEONE ELSE PAY IS NOT "FREE"

Another model of "free" is to offer goods and services without payment to a consumer in a way that extracts costs from someone else. The classic textbook – if quite gender-normative – example in economics is a local bar ladies' night when "discounted or even "free" (in the sense of no monetary payment) drinks are offered to female customers."[13] Putting aside the ways in which the female customers may have to "pay" for cheap or free drinks by fending off unwanted attention,[14] the reality is that, as the textbooks suggest, the bar profits by the increased volume of sales to male customers seeking to socialize with the female customers drawn in by the discount.

But cross-subsidization with no-monetary charge products exists beyond nightlife. For example, while the COVID-19 vaccines may have been provided in the U.S. without monetary charge, vaccination is rapidly becoming a requirement to attend or teach at colleges, and to hold one's job in many workplaces. Because many students, professors and workers who have been vaccinated do not wish to share the air they breathe with unvaccinated people, as the proportion who are vaccinated grow, it makes it easier for administrators and managers to impose vaccine requirements. As a result, the "free" vaccine has the effect of locking-in or imposing costs – such as unemployment – on others.

Contract law has long recognized that the fact that a third party pays for something does not make it gratuitous. Indeed, the concept of exchange is not limited to two parties making an offer and an acceptance, including the enforcement of a promise based on consideration provided by someone other than the promisee.[15] Similarly, antitrust law should engage more deeply with "no-monetary-payment" services. The U.S. Federal Trade Commission's complaint against Facebook in particular is a step in the right direction, recognizing the lock-in effects that so-called "free" services can generate so others effectively pay. Certainly, the Internet has encouraged the proliferation and increased economic importance of such business models, and there is nothing to suggest that they will disappear anytime soon.

10 87 F. Supp. 2d. 30, 50 (D.D.C. 2000) (concluding that "the fact that Microsoft ostensibly priced Internet Explorer at zero does not detract from the conclusion that consumers were forced to pay, one way or another, for the browser along with Windows").

11 John Mark Newman, *Antitrust in Zero-Price Markets: Foundations,* 164 U. Pa. L. Rev. 149 (2015).

12 David McLaughlin, "Facebook's Stealth M&A Puts Focus on Deals Under Antitrust Radar," *Bloomberg,* Aug. 23, 2021, https://www.bloomberg.com/news/articles/2021-08-23/facebook-s-stealth-m-a-puts-focus-on-deals-under-antitrust-radar.

13 Geoffrey G. Parker, Marshall w. Van Alstyne, Sangeet Paul Choudary, *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work For You* (Norton, 2016), Chapter 2; James D. Gwartney, et al., *Microeconomics: Private and Public Choice* (Cengage, 2016), pp. 200-203.

14 This seems to have become a recurring source of pained comedy in pop music. See Lily Allen, *Knock 'Em Out* (2006); Meghan Trainor, *No* (2015).

15 See Restatement (Second) of Contracts, Section 71(4) (American Law Institute, 1981) (stating that "[t]he performance or return promise [given as consideration making a promise enforceable] . . . may be given by the promisee or by some other person").

III. ALTERING BRAINS IS NOT "FREE"

An additional example of "free" is to offer goods and services without monetary payment in order to get consumers "hooked" – a model well-known not just to 19th century saloon keepers, but also to other sellers of addictive substances.[16] That said, the concept of a good, usually typified by heroin or cocaine, whose consumption increases the consumer's demand for more of that good, despite the law of diminishing marginal utility, has been taught in microeconomics for years.[17] While the boundaries of such goods have traditionally been set by legislatures rather than antitrust enforcers, technological advances may require more attention from the latter.

In particular, the ability of technology firms to trigger consumers' dopamine responses in an addictive way via apps may require competition law attention. In fact, antitrust scholars have long considered whether the consumer welfare standard should deem increased output of tobacco a positive thing for consumers, considering the product's addictive qualities and negative effects on user health.[18] That said, antitrust enforcers do continue to regulate conduct and mergers that may reduce the output of addictive products, notwithstanding their adverse health effects.[19]

The Internet, smartphone and video gaming technology has opened the door to no-monetary-charge services that the user can enjoy with little effort, but whose consumption may have literal mind-altering effects. This discussion has already commenced, and is likely to continue.[20] In a similar manner to antitrust and tobacco, Professors Niels Rosenquist, Fiona Scott Morton & Samuel Weinstein have pointed out that "robust medical evidence" is starting to show that digital platforms can be addictive and "harmful to users' mental health."

As a result, where more use actually injures the consumer, the increased output of some addictive digital platforms may not be a reliable proxy for positive effects on consumer welfare. Such services are certainly not "free" just because no money is paid by the user; contract law has long understood that non-monetary detriment can ground an exchange. Antitrust commentators have an unfortunate tendency to wave away such problems as best dealt with other areas of law, or by Congress. While that may be true for some issues, the Federal Trade Commission's long history with consumer protection and deception may make it particular suited to considering how antitrust law should handle mergers and conduct involving firms that sell mind-altering, no-money-payment products, and, if necessary, leading efforts to reshape antitrust accordingly.

IV. CONCLUSION

Contract law has understood for centuries that lack of a monetary payment does not make something free; antitrust law recognized this as far back as the *Microsoft* browser case. When a customer provides the seller benefits in non-monetary ways, or their action forces someone else to pay, or they suffer psychological change, a transaction cannot reasonably be called "free." The Internet and the changes it has spawned have raise the importance of no-monetary-payment services that are, in these ways, not "free." Just as the air we breathe can have costs we did not anticipate before COVID-19 first appeared in Wuhan, underestimating the antitrust implications of no-charge services is undermining consumers' faith in our law and our markets. To breathe free again requires an appropriate response.

16 See *infra* n.3 and accompanying text; Ray Fisman & Michael Luca, *Did Free Pens Cause the Opioid Crisis?* The Atlantic, Jan./Feb. 2019 (suggesting that free pens, meats and Christmas trees as gifts to physicians from Perdue Pharma representatives hawking OxyContin elicited a psychological response of gratitude in those physicians, who were then more likely to prescribe an addictive medication to their patients), *at https://www.theatlantic.com/magazine/archive/2019/01/did-free-pens-cause-the-opioid-crisis/576394/.*

17 Kenyon A. Knopf, *A Lexicon of Economics* (Academic, 2014), p.80 (defining "diminishing marginal utility" as a "'law' in the marginal utility of consumption [that] states that as an individual consumes more and more of a good in a given time period, the satisfaction derived from each additional unit will be less than the satisfaction from the preceding unit," but stating that "[a] major exception to the law is an addictive drug such as heroin, cocaine or 'crack.'").

18 See Daniel Crane, *Harmful Output in the Antitrust Domain: Lesson from the Tobacco Industry,* 39 Ga. L. Rev. 321 (2005); Barak Y. Orbach, The Antitrust Consumer Welfare Paradox, 7 J. Comp. L. & Econ. 133, 152 (2010) (questioning whether increased output of tobacco, with its harmful effects, does in fact benefit consumers, and if it does not, how the consumer welfare standard should be altered).

19 See, e.g. Complaint, *U.S. v. Anheuser-Busch InBev SA/NV and Grupo Modelo S.A.B. de C.V.* (Jan. 31, 2013) (challenging merger in beer industry).

20 Niels J. Rosenquist, Fiona M. Scott Morton & Samuel Weinstein, *Addictive Technology and Its Implications for Antitrust Enforcement,* Mar. 22, 2021.

PERSONAL DATA AS A PRICE IN MARKET DEFINITION: A BRIEF ASSESSMENT

BY MAGALI EBEN[1]

1 Magali Eben is Lecturer in Competition Law at the University of Glasgow, and co-director of the UK chapter of ASCOLA. No conflict of interest to declare, in accordance with the ASCOLA declaration of ethics.

I. INTRODUCTION

Nowadays, all but the staunchest sceptics acknowledge that the services offered by Google, Facebook, and their kin are not truly free. As Vestager put it, "there ain't no such thing as a free search."[2] The users contribute to the monetization of the platform through the attention and/or data they provide. We have come a long way since a U.S. court, now rather famously, declared that antitrust law "does not concern itself with competition in the provision of free services."[3] If there is a relationship of an economic nature between the user of a platform and the platform provider, it should be possible, at least in principle, to define a market. The question, then, is not whether a market can be defined for zero-price services, but rather how this should be done. In this short piece, I assess whether personal data can be conceptualized as a price, to enable a substitution analysis for zero-price services.

II. PRICE, CONSIDERATION, AND SUBSTITUTION

What is a "price"? A "price" indicates that something is given up to receive something else – something equally or more valuable – in return. In principle, a buyer parts with a specific amount of money only because they value the product they receive in exchange the same or more than those euros or dollars. Similarly, the seller parts with the product because, to them, its value is the same or less than the amount of money the buyer is willing to pay. Through the price, the buyer and seller enter into a transaction based on mutual exchange. The price – the thing the buyer gives up – is a form of consideration.

Yet "money" is not the only thing which could fulfil this role. Any good (including coffee beans, stones, salt, cacao, tobacco, cattle…) could function as a medium of exchange if certain conditions are met. Two important conditions are the acceptability and value of the medium:[4] the buyer consciously and intentionally provides a good as payment which the seller is willing to accept as such, and which both the seller and the buyer agree has value.[5] When any kind of medium of exchange changes ownership like this, a price is paid. The regular establishment of this exchange relationship could be sufficient to indicate the existence of demand and supply, and thus of the existence of a market in a general sense, regardless of the exact form consideration takes and the exact medium which is exchanged.

Knowing there is a market is all good and well, of course, but in antitrust cases we also need to know exactly *how to delineate it*. Indeed, the term "market" has acquired a very particular meaning in competition law, referring to "the boundaries of competition between firms."[6] An antitrust market is defined around the competitive constraints the firm and product under investigation faces. The most common constraints included in the market are the ones exercised by substitute products.[7] Although qualitative analysis (based on product characteristics and functionalities) is routinely used to identify demand substitutes, price can play an important role in quantitative analysis of demand substitution.

A question many will recognize is whether customers would switch to other products in response to a hypothetical, small but significant increase in price (the so-called "SSNIP test"). Prices not only represent the point where a seller and a buyer's valuation of a product intersect, but they can also indicate that product's significance in relation to other goods and services. Hayek called them "numerical indexes," embodying the preferences of economic participants across a variety of products.[8] In a world of limited wealth, the reaction of consumers to price changes – particularly whether they buy more or less of that product and correspondingly more or less of another product – can be evidence that the consumers value certain products more than others. It might also, given the right circumstances, be an indication of a competitive relationship between products.

Thus, what is important to delineate a market is not merely whether there is a price, regardless of the form of the medium of exchange, but whether consumers react to changes in this price in a way which reveals which products they consider to be substitutes.

---

2 Statement by Commissioner Vestager on Commission decision to fine Google €4.34 billion for illegal practices regarding Android mobile devices to strengthen dominance of Google's search engine (18 July 2018) available at https://ec.europa.eu/commission/presscorner/detail/en/STATEMENT_18_4584.

3 *Kinderstart.com, LLC v. Google, Inc.,* No. C 06-2057 JF (RS), 2007 WL 831806 (N.D. Ca. Mar. 16, 2007) para 5.

4 Eben, M. 'Market Definition and Free Online Services: The Prospect of Personal Data as Price' (2018) 14(2) I/S Journal of Law and Policy for the Information Society 242.

5 For those interested in a discussion of the concept of "money," I would recommend reading: Glyn Davies, *A History of Money* (revised and updated by Duncan Connors) (4th edition 2016 University of Wales Press); Goetzmann and Rouwenhorst (eds.), *The Origins of Value: The Financial Innovations that Created Modern Capital Markets* (2005 Oxford University Press).

6 European Commission, Market Definition Notice (1997) para 2.

7 European Commission, Market Definition Notice (1997) para 13.

8 Hayek, F. "The Use of Knowledge in Society," (1945) 35(4) The American Economic Review 525.

III. PERSONAL DATA AS A PRICE

Data may not truly be the "currency" of the 21st Century, but that does not mean it cannot be a price. If users of an online service value their data and provide it in exchange for access to a service, the personal data is a price in the sense described above. Through the "payment" of data, users find themselves in an economic relationship with the providers of the service.

Furthermore, their "purchasing" actions can reveal the extent to which this service fulfils their wants compared to available alternatives. If their consumption patterns change with the amount of personal data they are expected to disclose, it would be possible to get a sense of which services they consider to be substitutes for one another. They might "spend" less personal data on one service, and instead opt for another service, voting not just with their feet, but with their data. Personal data would be the price they pay, and the reactions to changes in data collection could be used to measure demand substitutability.

To determine the feasibility of using personal data to define relevant markets, two questions need to be answered. First, is there a relationship of exchange between the user and the platform? Second, can reactions to changes in personal data collection be used to assess substitution?

The first question to be answered is whether a relationship of exchange exists between users and the platform, based on the personal data they disclose. In the EU and U.S., a consensus seems to be emerging that personal data functions as a medium of exchange. In its *Google* decisions, the European Commission recognized that search services, which are offered free of monetary charge, constitute economic activities, and require the definition of a market. The users may not pay "monetary consideration," but provide the data which contributes to the monetization of the service, thus entering into a contractual relationship with the company.[9] In the recently dismissed FTC complaint against Facebook, the FTC and U.S. federal district judge reflected on the social network's relationship with its users. They are not charged a monetary price, it was argued, but "exchange their time, attention, and personal data, rather than money, for access to Facebook."[10]

Although this seems convincing in principle, the public record does not evidence a thorough assessment of whether the conditions for such an exchange relationship are actually satisfied. For a good of any kind to operate as medium of exchange, it is important that it holds value to both the buyer and the seller and that is accepted as a medium of exchange. In a 2018 paper, I assessed the likelihood that personal data (more specifically, "tradeable personal data") would fulfil these conditions from the perspective of the user.[11] I tentatively concluded that they could be fulfilled in the future. I provided indications that, even though knowledge of the ins and outs of data collection was not perfect, consumer awareness of data collection practices in general seemed to be on the rise, and that consumers increasingly considered themselves to be engaged in an exchange of data for services. Moreover, I anticipated that the advent of personal data management services and increased consent obligations on companies might further boost this awareness.[12] Three years later, it is not entirely obvious whether much has changed.

First, the evidence on consumer awareness remains mixed. A recent study by Akman signals that consumer awareness of the "free" character of services offered by companies such as Google and Facebook, and the source of funding of these services, was mixed. Her results showed that 25-26 percent of respondents believed (erroneously) that their data was collected and *sold* by Google and Facebook, whereas 42-43 percent knew that the platform was funded by advertising, although the paper does not specify how many realize that data *is* collected to enable targeted advertising.[13] Akman's questions focused on the (erroneous) understanding by consumers of the monetization practices of the platforms they use, rather than on their awareness that data is collected. As such, it does not really tell us whether users consciously and purposefully agree to data collection, in the understanding that they will receive services if they do so. They need to be capable of a deliberate choice to disclose data in return for a benefit. This requires that they know they are disclosing data, but it does not mean they need to know the ins and outs of the company's business model or know the exact way their data is used to generate revenue. Ascertaining whether this is the case will require further study of consumer behavior.

---

9 Case AT.39740 *Google Search (Shopping)*, European Commission Decision of 27 June 2017, paras 152, 158, 320; Case T.40099 *Google Android*, European Commission Decision of 28 July 2018, para 326.

10 United States District Court for the District of Columbia, *Federal Trade Commission v. Facebook*, Civil Action No. 20-3590 (JEB), Memorandum Opinion, available at https://storage.courtlistener.com/recap/gov.uscourts.dcd.224921/gov.uscourts.dcd.224921.73.0.pdf, 6.

11 Eben, *supra* n.4.

12 Eben, *supra* n.4, 253.

13 Akman, P. "A Web of Paradoxes: Empirical Evidence on Online Platform Users and Implications for Competition and Regulation in Digital Markets," (March 2021) working paper available on SSRN: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3835280, 20.

Second, we could do with more information on whether consumers value their data in this context. Making a deliberate choice to disclose data also implies that the users of a service value the data they share. Whereas money's value is derived in part from the fact that it is (kept in) limited supply, it can be questioned whether this is true for personal data. Money is valuable because the same euro cannot ordinarily be spent twice: if you buy an expensive house, you won't be able to buy (as many) expensive cars. Data, on the other hand, is often called "non-rivalrous." The same information can be shared with multiple persons. Its value to users cannot, in principle, lie in the fact that it can only be given up once. Rather, its value is derived from its privacy implications, and the costs which can be incurred as a result of the use of the data by other entities.[14]

Although personal information could be shared with multiple entities, disclosing it does come at a cost, and may be difficult to undo. Even though data "could be spent twice," once "spent" it is not that easy to take back. Disclosed data reduces the privacy of the data subjects, and can come with monetary costs, as the products offered to consumers later on may be more expensive as more information is available on their willingness to pay. These associated costs could be a good reason for users to value their data, but the research on whether they actually do so has produced mixed results.

In addition to the privacy implications and monetary costs, consumers may also value their data because they know that it is used by companies to generate revenue and thus has value to those companies. In the 2018 paper, I identified companies which are enabling consumers to receive compensation for their data, enabling them to control the data they disclose and directly monetize it. I argued that that these might make it more likely, over time, that consumers will start recognizing the economic value of their data in its own right. Nonetheless, the popularity of these companies is unclear. Although by the end of 2019 two of the companies mentioned in the paper, Datacoup and People.IO, had stopped operating in their original form, a UK company called "gener8" has since made headlines,[15] joining CitizenMe[16] and others in giving consumers the ability to earn money for their personal information.

It is worth noting that it is not necessary at this stage for users to be able to attribute an exact value to their data. Although the evidence so far seems mixed, if users value their data in general, and can sufficiently identify the data categories collected by a company, this should be sufficient to establish a relationship of exchange between the user and the platform.

Although this seems convincing in theory, it is important to be conscious of the obstacles to consumer autonomy in their relationship to data. Whether users are sufficiently aware that and which data is collected is still heavily dependent on the companies themselves. Companies may have incentives to reduce users' awareness of the data being collected on them, which would in turn reduce the likelihood that users consciously and willingly enter into an exchange of their data for the service. It is worth noting, for example, that the Google Play Store used to provide a list of all data permissions an app collects and require users to allow these permissions *before* an app could be installed. Now, these permissions are listed in the "about" section of an app, so that users accept them implicitly rather than expressly. Moreover, the GDPR's[17] consent and transparency requirements may not be sufficient to ensure that users are fully informed of the different categories of data they disclose. This not only may jeopardize the conceptualization of personal data as a medium of exchange, but also render it more difficult for users to choose between services, since they cannot compare them in terms of data collection. This brings us to the second question.

14 Acquisti, A. "The Economics of Privacy," OECD Background Paper 3 (2010) Joint WPISP-WPIE Roundtable on The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines, 11-14.

15 After an impressive appearance on the popular TV show "Dragon's Den" in April 2021.

16 https://www.citizenme.com/.

17 Regulation (EU) 2016/679 (General Data Protection Regulation) OJ L 119, 04.05.2016; cor. OJ L 127, 23.5.2018.

IV. PERSONAL DATA AND SUBSTITUTION ANALYSIS

If consumers exchange their personal data for services, it seems reasonable that their reactions to changes in data collection could be used to assess substitution. By making a choice to disclose their data to a particular service, they indicate their preference for that service over another. If the service were to collect more data, and users would switch to another, it would be reasonable to assume that the latter is a substitute for the former. Yet there are practical challenges to implementing such an analysis.

The test ordinarily used for monetary prices is the SSNIP test, which stands for "Small but Significant Non-transitory Increase in Price," whereby consumers' reactions to a (hypothetical) increase in price are used to identify possible substitutes. The "small but significant" nature of the increase is usually set at 5-10 percent for monetary prices. It is not evident at first glance how much of an increase would be considered "small but significant" if the test were applied to data collection. It is possible that consumers' sensitivity to data collection is different from their tolerance to monetary price hikes. This may seem like a hurdle to implementing data in a quantitative substitution test, but its importance should not be overstated. After all, the 5-10 percent range used in traditional, monetary price situations is itself the result of compromise. It is a range upon which not all scholars agree and whether it is truly "small but significant" is likely to vary from industry to industry.

A more pressing question is what constitutes an increase in data collection. An increase could either consist of an increase in the *quantity* of data collected overall, or it could a qualitative increase by collecting *more valuable* data. Certain categories of data might be more valuable than others because they are more privacy-sensitive or because users attribute a higher monetary value to them (in light of the benefits they could reap, for example, if they monetized them directly through companies like gener8 mentioned above). Research by Kummer and Schulte[18] identified the privacy-sensitivity of certain data permissions on the Google Play Store. This indicates a possibility to identify which data categories are more valuable to consumers, so that an increase could be based on the increase in more valuable data, if the authority chose this method. Potentially, it would be possible to study consumer reactions both to increases in quantity of data collected overall and to increases in more valuable data only, to compare the results of both.

A SSNIP-like test based on personal data is not so far-fetched. To shed light on the money-for-privacy trade-off, Kummer and Schulte compared data permissions and prices for different apps on the Google Play Store. This allowed them to study the choices made by app developers to use more privacy-sensitive data permissions for cheaper or free apps than for apps offered in exchange for money. It also allowed them to reflect on the choices made by users downloading apps, revealing that installation numbers were lower for apps with sensitive permissions. Although this remarkable study indicates that a "SSNIP" test based on personal data might be feasibly implemented, at least in the context of app stores, the study was done before Google changed the way it shows data permissions on its app store. Without visibility of the data categories collected, users would not be aware of increases in data collection and not be able to compare it with the data collected by other services.

Another comparison which may be challenging for users is the identification of "better value" alternatives, if not all services are monetized through personal data. It is possible that a service with similar functionalities is offered for a monetary charge. In that case, users may need to have some ability to compare the value "in data" of the first service with the "monetary" value of the second service. Although the valuations may not need to be exact, it still would require that consumers have some internal or external frame of reference to compare the values of the "prices" charged in order to decide whether, in response to an increase in "data price," it is worth switching to a service with a monetary charge.

A last challenge to note is the so-called "Cellophane Fallacy." This problem is well-known from the traditional context of monetary prices: if the company already exercise significant market power by pricing near or at the monopoly price, an increase in price may lead consumers to switch to products even if these are not substitutes. Some people argue that the data collection by companies such as Facebook is excessive. The intrusive nature of the data gathering policies is due to the market power the companies in question possess. If there were (more) competition less data would be collected (there would be more "privacy protection options" and more "options regarding data gathering and data usage practices" in the words of the U.S. Federal Trade Commission[19]). If this is true, there may be a risk of a personal data-form of the Cellophane Fallacy. If the company is already in a monopoly position, it may already be charging the monopoly "data" price beyond which the collection would cease being profitable. If this is the case – and assuming users are (made) aware of the exact data they disclose – an increase in collection (by increasing the quantity of data collected or by collecting more privacy-sensitive data) might lead them to cease using the service. If they then use another service, it cannot be concluded that it is a substitute.

18 Kummer, M. and Schulte, P. "When Private Information Settles the Bill: Money and Privacy in Google's Market for Smartphone Applications," (2019) 65(8) Management Science 1. See also citations in this paper.

19 United States District Court for the District of Columbia, *Federal Trade Commission v. Facebook*, FTC Complaint for Injunctive and Other Equitable Relief, available at https://www.ftc.gov/system/files/documents/cases/051_2021.01.21_revised_partially_redacted_complaint.pdf, para 163.

V. CONCLUSION

Online services are not "free" to use: even when no money changes hands, users do incur other costs such as the personal data they disclose. In both the EU and U.S. competition authorities have come to see the relationship between online platforms and their users as one of exchange, in which users disclose data which contributes to the monetization of the service. The notion that personal data is a price leads to the question whether reactions to data increases could be used in the identification of demand substitutes. The answer seems to be that although this is possible in principle, there are still some hurdles to overcome. The most important questions to resolve concern users: how aware are they of the categories of data collected and could companies and regulators in any way contribute to improving their knowledge; do they value data and accept that they exchange it for access to services; are they able to compare services even if some charge data and others charge money. If satisfactory answers can be provided to these questions, it seems likely that solutions can be developed for the practical challenges in designing a data-based SSNIP test. As Peeperkorn and Verouden put it, "the most important aspect of the SSNIP test is its conceptual side, not its quantitative side."[20] There may be hurdles to a substitution analysis based on personal data, but these might be addressed by combining different versions of the hypothetical scenario (with different levels and types of increases) and employing a variety of methods. Over time, with trial and error, a consistent practice could develop. The SSNIP test is not the "end all and be all" of market definition, but it can provide systematism to a complicated exercise. This is sorely needed in the area of zero-price services.

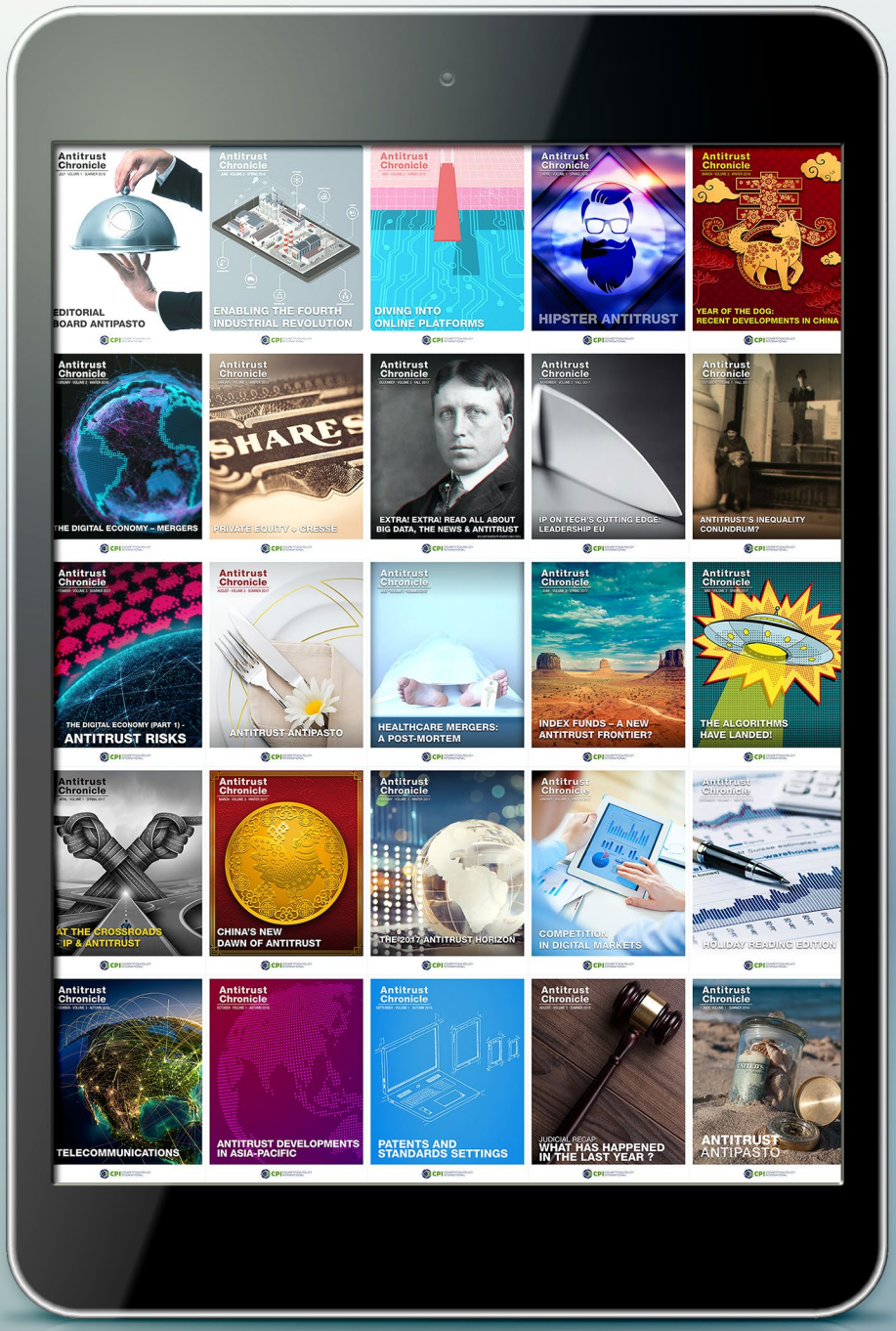
20 Peeperkorn, L. & Verouden, V. "The Economics of Competition," In: Faull, J. & Nikpay, A. *The EU Law of Competition* (3rd ed. 2014 Oxford University Press) §1.151.

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