CPI's North America Column Presents:

"Privacy Fixing" After *Texas et al v. Google* and *CMA v. Google (Privacy Sandbox)*: Approaches to Antitrust Considerations of Privacy

By Tim Cowen, Claire Barraclough & Josh Koran[1]

CPI COMPETITION POLICY INTERNATIONAL

January 2021

Executive Summary

Societies have designed antitrust laws to protect consumers from unfair practices (e.g. exclusive dealing, price fixing, abuse of dominance and restraint of trade) by ensuring competition drives business rivals to innovate, thus providing consumers with a greater choice of suppliers to address their needs. This paper discusses the practice of "privacy fixing" and how antitrust laws apply to that activity.

We describe the issue of "Privacy Fixing" as raised in *Texas v. Google* and discuss potential approaches to considerations of privacy as an antitrust issue with reference to the current UK Competition and Markets Authority ("CMA") investigation into Google's Privacy Sandbox[2]. We examine three examples of unfair practices regarding the misuse of data privacy policies that may expose organizations to antitrust liability, namely exclusionary abuse, exploitative abuse, and collusion.

Introduction

Before addressing the recent Google antitrust cases, let us first define the issue of "privacy fixing." Privacy fixing can arise in situations of individual firm action where a dominant organization unilaterally acts to use privacy to exclude rivals from a market or to limit the extent and degree of privacy choice available to its rivals. Alternatively, a number of businesses can agree to restrict or limit consumer choice, either directly by reducing their terms of trade with relation to privacy, or otherwise by jointly limiting competition that might offer people the choice of a differing level of privacy.

In 2017, Benjamin R. Dryden & Shankar Iyer reviewed the issue of privacy fixing and predatory privacy under U.S. law, in an article published in the leading online competition journal "Competition Policy International." As the authors put it "*Protecting privacy may seem so obvious a social good that any comparison with price fixing looks silly."* However, *"the antitrust laws apply to non-price elements of competition like privacy policies. The Supreme Court has made clear that "for antitrust purposes, there is no meaningful distinction between price and non-price components of a transaction."*[3] *F*or these reasons the antitrust rules have been applied "*even to public safety rules by private standards-setting organizations*."[4]

That paper reminds readers that collusion between competitors is "*the supreme evil of antitrust*" and accordingly antitrust law treats classic collusive activity, like price fixing, bid rigging, or customer allocations, as illegal *per se*. This means that these kinds of collusive activities have *"such predictable and pernicious anticompetitive effect, and such limited potential for procompetitive benefit, that they are irrebuttably presumed to violate the law*."

Before continuing it is necessary to define the form of "privacy," which underlies these antitrust concerns. Privacy regulations define "personal data" as information associated with identifiable individuals.[5] This information poses higher privacy risks when it is directly associated with

people's offline identity. Privacy regulations state that organizations can reduce the privacy risks for people by instead associating the same information with only a pseudonymous identifier.[6] A pseudonymous identifier is one where the organization processing the personal data has appropriate technical and operational processes in place to keep the identifier distinct from people's directly-identifiable identity.[7] Dryden & Iyer discussed likely theoretical examples of privacy that could raise antitrust liability and whether it could be *considered per se* illegal, quasi criminal, or subject to a rule of reason analysis under U.S. antitrust.

Now we have real world examples. Two independent antitrust investigations, in the United States and the United Kingdom, now raise the privacy fixing issue. On December 16, 2020, Texas' Attorney General announced that it, along with nine other U.S. States, had filed an antitrust lawsuit against Google.[8] The case is neither the first nor last lawsuit against Google to be announced in the U.S., with *USA v. Google* making headlines in October,[9] partly for the surprising extent of the collaboration it revealed between Google and Apple. Colorado's Attorney General filed another multistate lawsuit on December 17, 2020 covering similar, but not the same, ground. The Texas case focuses on a new aspect, given revelations about collaboration between Google and Facebook and the sharing of WhatsApp data between Google and Facebook.

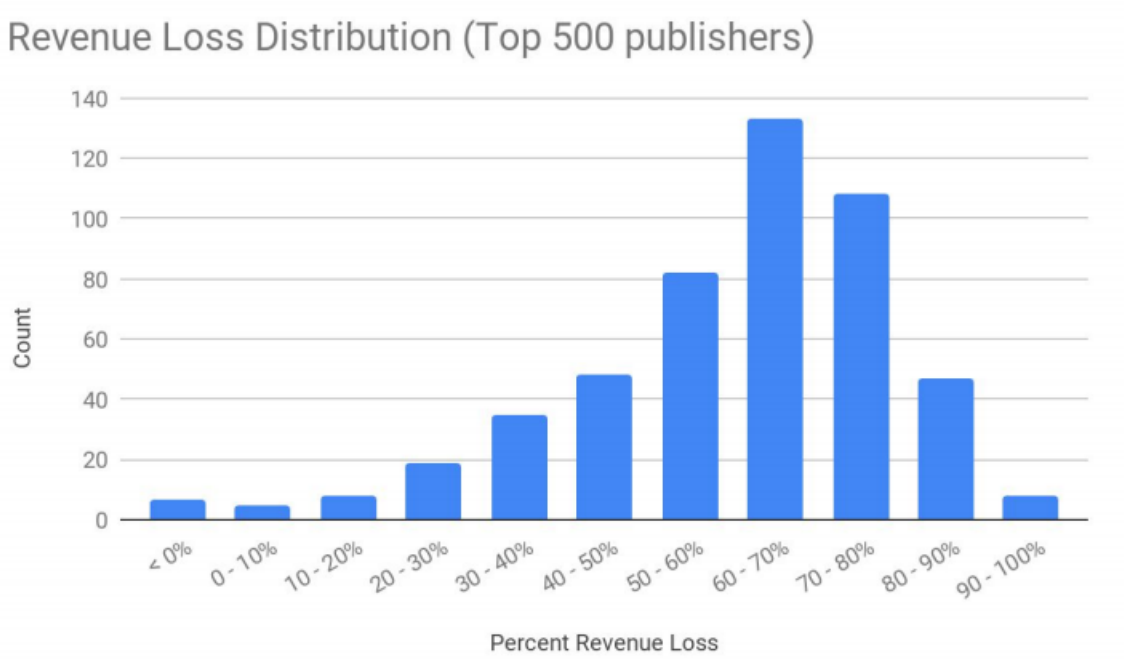
One allegation made against Google in the Texas case is that "it restricts information to foreclose competition and advantage itself." Within this, Texas argues that Google "uses privacy concerns as an excuse to advantage itself over its competitors," even where its "entire business model is to collect comprehensive data about every user in the service of brokering targeted ad sales."[10] The Texas pleading cites evidence from Google's internal documents, including Google's proposal to eliminate third-party cookies from its Chrome browser, which "is justified on privacy grounds, but the effect is to increase information asymmetries between Google and its competitors."[11] The documents available to Texas appear to evidence individual firm action – a kind of exclusionary abuse of dominance by Google vis-à-vis Google's competitors.

Contrary to Google's assertion that its actions protect people's privacy, Texas also refers to the fact that Google "violates users' privacy in other egregious ways when doing so is convenient for Google."[12] Moreover, the complaint goes on to state that "Google actively coordinates with its competitors when it comes to privacy,"[13] raising the further question of whether coordination between competitors in relation to privacy terms or policies could constitute anticompetitive collusion, or even a cartel-esque offence. In respect of this, the complaint states: "Of course, effective competition is concerned about both price and quality, and the fact that Google coordinates with its competitors on the quality metric of privacy – one might call it privacy fixing – underscores Google's selective promotion of privacy concerns only when doing so facilitates its efforts to exclude competition."[14]

On January 8, 2020, the CMA announced a formal investigation of the 23 proposed changes to Google's Chrome and Chromium Browser engine that Google announced on August 22, 2019 under the heading of the "Privacy Sandbox."[15] That investigation is concerned with Google's

unilateral action, the effect of the announcement, and the proposed changes on the market, specifically the negative consequences for publishers, marketers, and others affected relative to the benefits that inure to Google from these changes. The CMA had, during the course of 2019, conducted a wide-ranging Market Investigation which investigated these browser changes among other practices and obtained evidence from many sources. The conclusion of the Market Investigation was to propose new legislation to remedy the situation of dominant gatekeeper platforms' abuse of dominance, which the Government is now working to enact. [16]

One Google document the Market Investigation brought to light discloses the financial impact on publishers of Google's browser changes, which is particularly relevant to the new investigation. That document discloses that if implemented, just 1 of Google's 23 proposed changes would likely lead to catastrophic loss of revenue for publishers and, after the impact of the pandemic, the impact on funding for many web publishers and a plurality of the media in the UK could be devastating. A key graph drawn from Google's publicized research on this topic estimates the impact on publisher revenues from removing interoperable data, which disproportionately impacts smaller players.[17] If Google followed through on its change, they estimate approximately 75 percent of the worlds' largest publishers would lose more than 50 percent of their revenues.



This internal Google document further bolsters the CMA's observations that a 70 percent loss in advertising revenues could be suffered by publishers if the announced browser changes were implemented.[18] The disproportionate impact on smaller publishers is particularly concerning, given these not only represent a large number of minority voices, provide diversity of opinion, and support the plurality of the media, but also because such an impact would threaten future competition from new rivals by raising barriers of entry to the web publishing ecosystem. An

application has now been made to the CMA for interim measures to prevent this from happening and is being considered in the current investigation.[19]

Let us review three antitrust considerations raised by privacy fixing in the Texas case below.

Privacy as a Factor in Competition Cases

Price and non-price factors of competition are the basis on which consumers make purchasing decisions, and are factors that are routinely taken into account by antitrust authorities when examining those decisions and competitive rivalry among firms. Among the non-price factors antitrust regulators routinely consider are reductions in product quality, variety, and service.[20] The United States Supreme Court has also determined that non-price factors deserve protection under antitrust laws.[21] Whether privacy is an important non-price factor will depend on the product in question. In traditional goods and non-digital markets it is, however, hard to see situations where privacy is a key component of many purchasing decisions.[22]

Privacy is more likely to be a component of purchasing decisions in online markets. One early EU case in which this issue arose was Facebook's acquisition of WhatsApp. Users of messaging services were, arguably, attracted to WhatsApp's messaging service and flocked to use its offering in their millions on the basis that it was entirely private and highly secure; and provided groups of people a method for competing with Facebook groups or messenger services and other messaging apps. All were free to the user at the time[23], and one clear competitive differentiator between offerings was privacy, given the lack of privacy protection in Facebook's terms of trade. WhatsApp accumulated 400 million users before being bought by Facebook for over $22 billion. The merger was alleged to be anticompetitive at the time and given Facebook's notorious compliance record on privacy protection, concerns were raised that Facebook was "taking out" a fast-growing competitor and would degrade the privacy protections offered by WhatsApp over time.

The case was the subject of numerous complaints before EU member states and U.S. authorities', and eventually the EU Commission.[24] The Commission in that case accepted that the degradation of privacy policies could affect other aspects of product quality, or amount to an increase in the "price" paid by consumers for the product (e.g. in terms of requiring more personal data to be provided). The precedent was established that:

> "In two-sided markets, where products are offered to users for free and monetised through targeted advertising, personal data can be viewed as the currency paid by the user in return for receiving the 'free' product, or as a dimension of product quality."[25]

After Facebook gave assurances that WhatsApp users' private data could not technically be combined for the use of advertising, the merger was allowed. While it allowed the merger, Facebook's later breach of its undertaking earned it a fine of over $100 million for misleading

the Commission,[26] and the case became notorious when a UK House of Commons Select Committee released documents that showed Facebook senior executives knew they were taking out a rival competitor at the time.[27] Facebook has now announced in January 2021 that it will use personal data gathered in WhatsApp for its advertising, but will not allow third-parties to advertise in this inventory.[28] This undermines one of the three rationales the Commission relied upon in allowing the original merger, namely that "a number of alternative providers would continue to offer targeted advertising after the transaction, and a large amount of internet user data that are valuable for advertising purposes not within Facebook's exclusive control would continue to exist."[29] Moreover, the Commission found that, contrary to Facebook's statements in the 2014 merger review process, the technical possibility of automatically matching Facebook and WhatsApp users' identities already existed in 2014, and that Facebook staff were aware of such a possibility.

Unsurprisingly, the fact that privacy protection can be a major factor in customer's preferences and hence in online competition has been followed in subsequent cases.[30] Whether privacy is important to consumers decision making will depend on the product and market concerned. For example, in *Microsoft/LinkedIn* the Commission considered that data privacy is *"a significant factor of quality"* in the market for Professional Social Networks.[31]

Misapplication of Data Privacy Policies that Cause Exclusionary Abuse

The Dryden & Iyer paper above presents a hypothetical example of a dating app which has decided to match competitor's privacy policy or commitment not to monetize user data for advertising, a decision "motivated by a predatory, monopolistic desire to injure its smaller rivals, rather than a bona fide decision to honor its users' privacy."[32]

In the example they provide, two competitors rely on privacy policy not to improve their service, but instead to reduce competition, given new entrants would not have a scaled user base to support their operations using a direct payment business model. In their example, since advertising revenues can reduce direct cash payments by website visitors, by agreeing to eliminate this revenue model this would raise the prices consumers would need to pay. Essentially, in the example, the dominant dating app is using privacy as a non-price factor of competition to undermine future competition. Such behavior conducted by a dominant supplier that may "create a barrier to entry that inhibits the growth of the new entrants" is likely to be anticompetitive and predatory under U.S. law. The paper cites the leading U.S. antitrust case of *Aspen Skiing Co. v. Aspen Highlands Skiing Corp,* 472 U.S. 585 (1985), where it was found that when a firm "attempt[s] to exclude rivals on some basis other than efficiency, it is fair to characterize its behavior as predatory."[33]

Another example of such behavior, in the digital space, can be found in *Texas v. Google* where it references the attempts by Google to claim that changes to its Chrome browser are privacy protecting, but which are, in reality, exclusionary of advertising rivals. Essentially, platforms such

as Google, which themselves have relied on data monetization to grow, are pulling up the drawbridge behind them. The Texas complaint cites the example of Google's announcement that it will remove third-party cookies from its Chrome browser.[34] That action will limit the ability of competitors to Google's advertising business to access the data needed to optimize the matching of adverts to people across different websites. This negative impact to other publishers is not in dispute, as evidenced in Google's publicized research.[35] It also suggests that the motivation behind the change is designed to reduce competition. The CMA investigation into Privacy Sandbox is assessing how Google's proposed changes would further concentrate more revenues into Google's hands to the detriment of competition.[36]

One potential solution to the issue of exclusionary abuse in the provision of data would be providing access to that data by competitors. The French Autorité de la Concurrence dealt with this issue as long ago as 2014 in the *GDF Suez* case.[37] The measures requested by the complainant included ordering GDF Suez to give competing suppliers of natural gas access to customer data including the customers' names, addresses, telephone numbers, and consumption profiles. Such data were private and protected under the French *Loi Informatique et Libertés* but that did not prevent the Autorité from ordering GDF Suez to grant access to the data, subject to consumers' consent. In line with the recommendations made by CNIL (the French data protection authority), the Autorité required GDF Suez to inform its customers that competitors would be able to request access to their personal data and they had the right to refuse such access. Another solution would have been to provide access to anonymized data, which falls outside the scope of the GDPR, or to pseudonymized data.

The CMA has proposed such a solution in its Market Investigation[38] and it may be forthcoming in the anticipated UK legislation designed to underpin its new Digital Markets Unit. This risk of exclusionary abuse is a just one issue of privacy fixing antitrust authorities should consider in relation to online digital markets.

Misapplication of Data Privacy Policies that Cause Exploitive Abuse

In digital markets, where data is so important for monetization through advertising, there is a tension between companies' incentives to acquire as much personal data as possible about consumers and incentives to respect consumer privacy. Where subject to competitive constraints, one could expect that companies which stray too far one way or the other will suffer. If they gather too much sensitive data that frequently causes privacy harms, consumers who worry about these risks will seek alternatives and switch away from privacy invading firms so the privacy invaders revenues will suffer. However, in the absence of such competitive choice people may find themselves subject to exploitive abuse.

In competitive markets where offerings are vying with each other to provide greater levels of privacy in return for the service supplied, privacy could be a key differentiator in people's choices over which services to use. Thus, when competition exists, much depends on the actions and

choices of end consumers. Some consumers may be willing to share personal data with a trusted supplier in return for specific services; others may not. Different levels of sharing may be offered for different levels of service – and competitive rivalry acts to spur innovation.

Indeed, we have some evidence of digital services that compete in this manner. Duckduckgo is a rival search engine to Google's dominant search service, which differentiates itself by not collecting an individual's prior search activity to personalize search results. Both search services have access to the same website data, but essentially compete on privacy. A second example is Brave Browser that offers its users that it alone will collect their personal data and monetize publisher properties without sharing any non-aggregated personal data with marketers. Given this browser is a white-label version of Google's dominant Chrome browser, Brave essentially is using data sharing with marketers as the principle differentiator. Neither of these alternatives have attracted significant users, which suggests that a majority of people are perhaps not concerned with the exchange of non-sensitive personal data for cost-free access to web services. However, the market context is one of a market that has been dominated and distorted for many years and is not fully competitive. On any analysis, combinations of price and privacy protections are possible, are likely to be better made and reflect consumers real choices in competitive markets than in markets controlled by advertising-funded monopolies. In markets that are funded by advertising, without the constraint imposed by competition, there is an incentive on the monopolist to harvest more sensitive private data if by doing so it can achieve greater numbers of sales and increase profits, even at the expense of consumer privacy.

One leading commentator, Dina Srinivasan, has highlighted this issue in relation to Facebook in both a *New York Times* article,[39] and a longer academic paper.[40] She cites Facebook, when it was a start-up, committing to consumers that it did not and would not use cookies "to collect private information from any user,"[41] essentially using privacy as a competitive differentiator. Over time Facebook rowed back on the plan. Facebook now gathers a considerable amount of consumer data, including through third party cookies across the internet.[42] Since the early 2000s, Facebook has seen its competition diminish, either through the demise of rivals such as MySpace or Bebo, or through acquisition of nascent competitors, including Instagram in 2012 and WhatsApp in 2014. In "2014, Google announced that it would fold its social network Orkut. Emboldened by the decline of market threats, Facebook revoked its users' ability to vote on changes to its privacy policies and then (almost simultaneously with Google's exit from the social media market) changed its privacy pact with users."[43] As competition dwindled, by agreement or otherwise, Facebook began collecting more consumer data. As Srinivasan puts it, "the price of using Facebook has stayed the same over the years (it's free to join and use), but the cost of using it, calculated in terms of the amount of data that users now must provide, is an order of magnitude above what it was when Facebook faced real competition."[44]

Google also changed its stance over the collection of personal data after it acquired DoubleClick. Unlike most digital advertising which marketers evaluate through analysis of consumer behavior after measuring exposure across multiple digital properties, marketers value Search advertising

by the immediate click event on a single property (a search engine). For this reason, prior to Google's expansion into other forms of digital advertising that followed its DoubleClick acquisition, Google differentiated its offering by not collecting and storing personal data associated with its search solutions. In 2007, Google's VP of product management for advertising was quoted as stating Google was not stitching together a user's various online actions in one profile.[45] This executive stated, "Nothing is stored, nothing is remembered. It all happens within that session."[46] After the DoubleClick acquisition, this same executive announced Google would store user web interactions in a profile to optimize the matching of content to people based on their past actions:

> "At Google, we believe that ads are a valuable source of information — one that can connect people to the advertisers offering products, services and ideas that interest them. By making ads more relevant, and improving the connection between advertisers and our users, we can create more value for everyone. Users get more useful ads, and these more relevant ads generate higher returns for advertisers and publishers. Advertising is the lifeblood of the digital economy: it helps support the content and services we all enjoy for free online today, including much of our news, search, email, video and social networks.... We think we can make online advertising even more relevant and useful by using additional information about the websites people visit. Today we are launching "interest-based" advertising as a beta test on our partner sites and on YouTube. These ads will associate categories of interest — say sports, gardening, cars, pets — with your browser, based on the types of sites you visit and the pages you view. We may then use those interest categories to show you more relevant text and display ads."[47]

The CMA has recently found that most consumers, when surveyed, indicate that they are concerned about their privacy online.[48] It can be inferred, therefore, that consumers would, in a competitive market, switch from Facebook, but to what? In a paradigm where there is not, in most cases, a realistic alternative, as competition in social media is limited, consumers are not currently being protected by market forces.

Of course, given that a defining property of social networks is that they depend on the sensitive personal data of identity, a more competitive market might provide people choice to have their cost-free access subsidized via advertising, but ensure that their digital activity is not linked by the social network to their identity via this advertising.

The CMA itself has put forward a proposal that would both address user needs for protection of privacy and identity and allow advertisers with a pseudonymous ID sufficient for allowing ads to be tailored and relevant, and enable the online marketing and advertising industry to measure the performance of ads across multiple websites.

"Privacy-Fixing" Under EU as well as U.S. Competition Law

The examples above reference the issue of privacy in competitive offerings and the issues that have come up in mergers, collusion and unilateral behavior. Both the Texas complaint and the Dyden & Iyer paper explicitly discuss the concept of "privacy fixing," as a non-price factor that can remove consumer choice either directly by reducing privacy, or by limiting competition. The U.S. Supreme Court has held that even companies acting unilaterally "to forsake short-term profits to achieve an anticompetitive end" is against the public interest.[49]

The Texas case also reveals that Google may have agreed with Facebook to give it an advantage in advertising markets and between them the parties have taken steps to limit the data that they share with other players.

Under EU and UK law, if competitors were to agree to reduce or limit the level of protection for users' personal data in their terms or quality of competing offerings, as with an agreement to limit their prices, their conduct would be prohibited in the EU as an anticompetitive agreement within the prohibition of Article 101 of the Treaty on the Functioning of the European Union ("TFEU"), and in the UK under Chapter I of the Competition Act 1998. Such an agreement would be similar to an agreement to reduce or limit the quality of the parties' products. For instance, in the *Belgian Association of Pharmacists* case, an agreement to restrict suppliers from producing products of a different, inferior, standard (thus limiting the variety of products supplied) has been found to infringe Article 101(1).[50]

Thus, privacy fixing is an important non-price factor that organizations should consider, along with factors of controlling price, supply, quality, service, and reductions in innovation, to avoid potential liability from activities that may expose them to potential antitrust violations. Similarly, the exchange of information between competitors about planned changes to their privacy policies may violate competition law if it would remove the uncertainty as to their future conduct and, thereby, eliminate the risk of independent competitive conduct on a market.[51]

Coordination Between Online Ad-funded Platforms

Texas v. Google refers to agreements between Google and Facebook that came to light since the House of Commons DCMS select committee investigations of Facebook, which released documents showing that Facebook trades with others and accumulates data from other online businesses on a non-reciprocal basis.

The Texas complaint now goes further and alleges that Google and Facebook not only discussed privacy, but also signed an exclusive agreement in 2015 under which Facebook shared WhatsApp data with Google.[52] The timing of that 2015 agreement is remarkable in light of the *Facebook/ WhatsApp* acquisition since Facebook notified the acquisition in 2014 and informed the EU Commission that it would be unable to establish reliable automated matching between Facebook users' accounts and WhatsApp users' account data. It stated this both in the

notification form during 2014 and in a reply to a request of information from the Commission. However, in August 2016, WhatsApp announced updates to its terms of service and privacy policy, including the possibility of linking WhatsApp users' phone numbers with Facebook users' identities. All the while it now appears that Facebook perhaps not only had access to that information but had agreed to provide information to Google. This is not an issue on which the record is entirely conclusive, but it could be expected to be a matter of some interest to a curious authority.

Google and Facebook both offer very limited privacy protections in their end user contracts. Rather than relying on pseudonymous identifiers (that most of their smaller rivals rely on), both companies offer marketers content targeting based on matches of this directly-identifiable data. There is presently no evidence of any direct agreement between them to take such an approach, but the Texas case refers to evidence that in their dealings with each other they share user data so obtained to their mutual benefit. The extent of their coordination may become clearer as the Texas case progresses.

Collusion in Collective Agreements and Standards-making Involving Data Privacy Policies

The concern about competitors meeting and discussing prices goes back centuries. As the well-known quotation goes:

> "People of the same trade seldom meet together, even for merriment and diversion, but the conversation ends in a conspiracy against the public, or in some contrivance to raise prices."

Adam Smith eloquently stated the above in The Wealth of Nations Book 1 Chapter X. it is often repeated as the reason that antitrust authorities maintain vigilance over gatherings between competitors. A few examples of agreements and collaboration that involve privacy issue are provided below.

In Dryden & Iyer's dating app example, two competing dating apps hypothetically agree to forego monetization revenue in order to create a barrier to entry preventing new competitors from entering the market at sufficient scale to benefit from network effects in the markets they operate in.

As described above, privacy fixing can, like price fixing, be collusive activity which restricts competition among products and firms and would be condemned by antitrust laws on both sides of the Atlantic. Companies making agreements or arrangements with each other about information sharing, can similarly be guilty of illegal collusion to achieve anticompetitive outcomes.[53] In *Associated Press v. United States, 326 U.S. 1 (1945)*, the U.S. Supreme Court held that prohibitions on newspaper members of the Associated Press against sharing real-time events was an antitrust violation of the Sherman Act, even though the Associated Press had not achieved a complete monopoly.

Another potential method of privacy-fixing posited by Dryden & Iyer is collusion through an industry body, standards body, or trade body. Indeed, they argue that "the most likely target for a privacy fixing or predatory privacy claim might well be a standards-setting organization or trade association that tries to adopt a best privacy practice or a rule of ethics for an entire industry."[54]

Standards bodies, sit within a kind of safe harbor from an antitrust perspective, generally regarded as beneficial or enabling different but complimentary activities to interoperate provided that the standards created are competitively neutral. If such bodies are used for collusion and are not involved in standards-creation or the standards are not competitively neutral, there could well be a breach of the antitrust laws.[55]

Google has, for example, stated publicly that its proposed changes to its browser, labelled the Privacy Sandbox, are being discussed in W3C groups.[56] These proposals are arguably intended to allow Google to collect and process people's personal data, on terms that it determines, but restrict or limit the accuracy and timeliness of the data provided to all of its advertising rivals. By impairing the interoperable data that smaller publishers rely on, Google inherently forces publishers and advertisers to become even more reliant on its own technology.

Cursory investigation reveals that such discussions are not taking place within standards-making groups of the W3C, but rather in business groups that do not have any standard-making capacity. Facilitation of exclusionary and anticompetitive abuse, as alleged by *Texas v. Google* via such a medium, is potentially made worse by the fact that the discussion involves all the major players in the industry.

While Facebook/Google coordination appears in the Texas case, Google/Apple coordination is at the center of *USA v. Google*. That case highlights cross-platform coordination between Apple and Google to an extent that has not previously been appreciated. It is well known that Google has been the exclusive provider of default search on all Apple devices for many years.[57] It is also well known that Apple has been pursuing a walled-garden strategy of "there's an app for that" – within its enclosure for many years. According to *USA v. Google*, Google has a bigger walled garden, containing more apps, and 90 percent of apps on Android are downloaded through Google Play.[58] Although denied by Google, *USA v. Google* refers to emails and evidence that appear to show that Google and Apple jointly pursue profit maximization to their mutual benefit:

> "120. Apple's RSA incentivizes Apple to push more and more search traffic to Google and accommodate Google's strategy of denying scale to rivals. For example, in 2018, Apple's and Google's CEOs met to discuss how the companies could work together to drive search revenue growth. After the 2018 meeting, a senior Apple employee wrote to a Google counterpart: "Our vision is that we work as if we are one company."[59]

The sentiment echoes the statements made by companies operating within more traditional cartels.[60] Nevertheless, the fact that senior execs have met and discussed a range of topics and that one employee thinks the vision should be to work together as one company may not in itself

be sufficient to support a claim for any anticompetitive collusion. If Google's strategy is similar to Apple's, and now Google is adopting browser changes to "encourage" publishers to become apps on its walled garden, that may not involve collusion or collaboration with Apple; it might simply be that they have independently worked out that reducing rival publishers' access to interoperable data makes walled gardens more attractive to marketers, and that app stores provide more control over the market for web content and services.

Whether or not there is a coordinated strategy between Apple and Google, or Google is merely following Apple's lead in making browser changes, may be a matter of further investigation in the DOJ case, and the Texas case, or if they are consolidated.[61]

This use of collusion in collective agreements or standards making is a third example of "privacy fixing" that the antitrust authorities should consider in relation on online digital markets.

Conclusions

As is clear from the above review, the antitrust considerations related to the misuse of data privacy policies are potentially very significant. As ever, much depends on the facts and the markets in question, and on the extent and degree of choice available to end users.

Antitrust regulation is built upon the notion that consumers ought to have sovereign choice in competitive markets, given this choice drives rivals to innovate to better meet those consumers' differing needs. Societies are harmed when organizations conduct practices that significantly undermine these market forces, even when such organizations offer some countervailing benefit. Given the idea of consumer sovereignty is central to the operation of most antitrust laws, whether by individual monopolistic action or by agreement, the usurping of consumer choice is and should always be a concern for the authorities. In this article we have referred to three examples: exclusionary abuse, exploitative abuse, and collusion. All usurp consumer choice.

As digital markets are more and more important to society, maybe it is now time to add privacy to the list of other factors, such as prices, that are not a matter for legitimate discussion among competitors.

[1] Tim Cowen Barrister, Preiskel & Co LLP, Claire Barraclough, Solicitor, Preiskel & Co LLP, and Joshua Koran Zeta Global.

[2] On January 7, 2021, the CMA launched an investigation under Chapter II of the Competition Act 1998 into suspected breaches of competition law by Google. The investigation concerns Google's proposals to remove third party cookies (TPCs) on Chrome and replace TPCs functionality with a range of 'Privacy Sandbox' tools, while transferring key functionality to Chrome. Press release: CMA to investigate Google's 'Privacy Sandbox' browser changes (8.1.21).

[3] *Pacific Bell Tel. Co. v. Linkline Communications, Inc.*, 555 U.S. 438, 450 (2009). See generally also U.S Dep't of Justice & Federal Trade Comm'n, Horizontal Merger Guidelines (2010) § 1 ("When the Agencies investigate whether a merger may lead to a substantial lessening of non-price competition, they employ an approach analogous to that used to evaluate price competition.").

[4] *Allied Tube & Conduit Corp. v. Indian Head, Inc*., 486 U.S. 492 (1988).

[5] Such as https://gdpr-info.eu/art-4-gdpr/.

[6] https://gdpr-info.eu/recitals/no-28/.

[7] https://gdpr-info.eu/recitals/no-78/.

[8] https://twitter.com/TXAG/status/1339283520099856384.

[9] As stated at para 13 of *USA v. Google* https://www.justice.gov/opa/pr/justice-department-sues-monopolist-google-violating-antitrust-laws its dominance means that users have no choice over the terms of trade and the privacy protections they are offered: "Google is now the unchallenged gateway to the internet for billions of users worldwide. As a consequence, countless advertisers must pay a toll to Google's search advertising and general search text advertising monopolies; American consumers are forced to accept Google's policies, privacy practices, and use of personal data; and new companies with innovative business models cannot emerge from Google's long shadow.

[10] Paragraph 140, *Texas et al v. Google*.

[11] Paragraph 140, *Texas et al v. Google*.

[12] Paragraph 141, *Texas et al v. Google*.

[13] Paragraph 143, *Texas et al v. Google*.

[14] Paragraph 143, *Texas et al v. Google*.

[15] https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes (accessed January 2021).

[16] https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study (accessed January 2021).

[17] https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf (accessed January 2021).

[18] CMA Online Markets Final Report at 5.326 and Appendix F.

[19] The application to the CMA for injunctive relief against such a devasting impact was brought by Marketers for an Open Web ("MOW"), a not-for-profit consortia. Given this foreseeable impact on the continued viability of certain websites, MOW seeks interim measures to prevent Google's proposed changes from being implemented until the pending legislation designed to provide a level playing field in digital markets has been put into effect.

[20] Department of Justice and Federal Trade Commission, HORIZONTAL MERGER GUIDELINES, §1 (2010).

[21] *United States v. Continental Can Co.*, 378 U.S. 441 (1964).

[22] The issue might arise with relation to consumers' willingness to shop at a particular store depending on how data collected from in store consumers purchases is used. Fierce battles between grocery retailers attest to the importance of loyalty and discount cards (such as Nectar cards and other rewards cards).

[23] WhatsApp did have a notional $1, £1, or Euro fee but virtually no revenue collected at the time.

[24] http://ec.europa.eu/competition/publications/cmb/2015/cmb2015_001_en.pdf; see also CMA Lear Report for criticism of the Commission Decision.

[25] See fn 8 EU commission discussion. It also recognised the potential for anticompetitive harm if a dominant company could increase the price at which it sells its data post-merger or refuse to supply such data altogether (e.g. to foreclose competing providers of data analytics services, who rely on data as an input for providing their services).

[26] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_17_1369/IP_17_1369_EN.pdf.

[27] https://www.wsj.com/articles/facebook-feared-whatsapp-threat-ahead-of-2014-purchase-documents-show-11573075742.

[28] https://www.whatsapp.com/legal/updates/privacy-policy?eea=0&_fb_noscript=1; see also

https://9to5mac.com/2021/01/06/whatsapp-share-your-data-with-facebook/.

[29] https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_17_1369/IP_17_1369_EN.pdf.

[30] *Microsoft/Linkedin* (Case COMP/M.8124), Commission decision of December 6, 2016

[31] Similarly, in *Google/DoubleClick*, the U.S. Federal Trade Commission ("FTC") acknowledged that mergers can "*adversely affect non-price attributes of competition, such as consumer privacy*."

[32] https://www.foley.com/-/media/files/insights/publications/2017/09/dryden-coauthors-antitrust-article-for-cpi/files/article/fileattachment/cpi--dryden--iyer.pdf.

[33] https://www.foley.com/-/media/files/insights/publications/2017/09/dryden-coauthors-antitrust-article-for-cpi/files/article/fileattachment/cpi--dryden--iyer.pdf.

[34] Paragraph 140, *Texas et al v. Google*.

[35] https://services.google.com/fh/files/misc/disabling_third-party_cookies_publisher_revenue.pdf (accessed January 2021).

[36] https://www.gov.uk/government/news/cma-to-investigate-google-s-privacy-sandbox-browser-changes (accessed January 2021).

[37] Autorité de la concurrence, Décision n° 14-MC-02 du 9 septembre 2014 relative à une demande de mesures conservatoires présentée par la société Direct Energie dans les secteurs du gaz et de l'électricité, p. 52-53.

[38] See CMA remedies and Fair Trading remedy outlined in section 7 especially page 342 as well as the creation of an independently overseen Transaction Identifier or ID. CMA FR 8.216-8.218 p 409. Regulation of transaction data that needs to be shared to enable cross site measurement being included in the remedy – see 8.227 and the Common User ID 8.231 & 8.240-243.

[39] https://www.nytimes.com/2019/05/28/opinion/privacy-antitrust-facebook.html.

[40] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3247362.

[41] https://www.nytimes.com/2019/05/28/opinion/privacy-antitrust-facebook.html.

[42] The CMA investigated the platforms approach to customer engagement and concluded at 4.232 that "platforms do not give consumers the right information in a consumer-friendly way and frequently rely on choice architecture that is likely to impede consumer engagement and which favour the collection and use of data for advertising."

[43] https://www.nytimes.com/2019/05/28/opinion/privacy-antitrust-facebook.html.

[44] https://www.nytimes.com/2019/05/28/opinion/privacy-antitrust-facebook.html.

[45] Eric Auchard, "Google wary of behavioral targeting in online ads," Reuters, (Jul. 31, 2007) https://www.reuters.com/article/us-google-advertising-idUSN3135052620070801 (accessed January 2021).

[46] Eric Auchard, "Google wary of behavioral targeting in online ads," Reuters, (Jul. 31, 2007) https://www.reuters.com/article/us-google-advertising-idUSN3135052620070801 (accessed January 2021).

[47] Susan Wojcicki, Google Official Blog, "Making ads more interesting," (March 11, 2009), https://googleblog.blogspot.com/2009/03/making-ads-more-interesting.html (accessed January 2021).

[48] See section 4.46 CMA notes research (eg Brown (2001), Acquisti (2004), Barnes (2006), Acquisti et al (2016), Kokolakis (2017), Barth and de Jong (2017)) that consumers are very concerned about their privacy but they then behave in a way that contradicts this clearly stated preference eg by not using available privacy controls. The debate as to whether this is in fact a genuine paradox (e.g. consumers could be acting in a rational way and properly evaluating the costs and benefits), or whether there are factors at work which prevent consumers from being able to make effective choices. This so-called "privacy paradox" is explored further in Section 4.48-4.84 where barriers to effective consent, and attitudes to use of personal data are reviewed, followed by review of engagement and at 4.109 CMA records its concern that consumers have limited control and "are often compelled or nudged to agree." At 4.232 The market study then finds that "platforms do not give consumers the right information in a consumer-friendly way and frequently rely on choice architecture that is likely to impede consumer engagement and which favour the collection and use of data for advertising."

[49] *Aspen Skiing Co. v. Aspen Highlands Skiing Corp.*, 472 U.S. 585 (1985).

[50] *Belgian Association of Pharmacists* OJ [1978] L 47/42.

[51] Case 48/69, *ICI v. Commission* [1972] ECR 619, at paras 100 to 103.see also *Ford Tractors*.

[52] Paragraph 141, *Texas et al v. Google*. One wonders whether this was the same data that Facebook argued was incapable of being shared in the Facebook WhatsApp merger case and was later fined for misleading the Commission.

[53] *Associated Press v. United States*, 326 U.S. 1 (1945).

[54] https://www.foley.com/-/media/files/insights/publications/2017/09/dryden-coauthors-antitrust-article-for-cpi/files/article/fileattachment/cpi--dryden--iyer.pdf.

[55] See section 7 of the EU Horizontal Guidelines & ad refs to U.S. guidelines.

[56] Justin Schuh, Chromium Blog, (Jan. 14, 2020), https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html, (accessed January 2021).

[57] *USA v. Google* also refers at para 45 to the fact that presets and exclusivity in search appears to have extended "more recently, *other search access points* on Apple's mobile devices." See also Section 6 p27 et seq.

[58] *USA v. Google* para 73.

[59] *USA v. Google* para 120.

[60] See for example the Vitamins cartel where the companies involved sought to operate "as a virtual company."

[61] Google references in a blog discussing the Privacy Sandbox that its actions to restrict information sharing are taken with full knowledge of the actions of Apple, see Justin Schuh, Chromium Blog, (Aug. 22, 2019), https://blog.chromium.org/2019/08/potential-uses-for-privacy-sandbox.html. (accessed January 2021).