Original Manuscript

Competition & Change

Competition & Change
2024, Vol. 0(0) 1–20

DOI: 10.1177/10245294241266048
journals.sagepub.com/home/cch


The regulator's trilemma: On the limits of technocratic governance in digital markets

Nick O'Donovan
Keele Business School, Keele University, Keele, UK

Abstract

Policymakers increasingly recognise the need for regulatory intervention in the digital economy to promote competition, privacy and innovation, among other policy objectives. Much policy-focused literature presents regulation as a technical puzzle to be 'solved' through identification of the appropriate intervention in a particular context, though there is persistent disagreement among experts about what remedies are preferable in different digital markets. At the same time, many external observers emphasise the sheer multiplicity of public policy objectives that regulatory interventions might fulfil, claiming that conflicts between these objectives are inevitable and thus require political rather than technocratic solutions. This article attempts to bridge the gap between these perspectives through a novel theoretical analysis of digital markets characterised by strong network effects, conceptualising different markets in terms of common underlying structural characteristics. The resulting framework helps policymakers to anticipate which remedies will safeguard competition, privacy and innovation/efficiency under what circumstances, both in well-established digital markets and with respect to emerging technologies such as artificial intelligence. In so doing, it also highlights limits to the technocratic governance of digital markets, identifying circumstances in which conflicts between competing public values cannot be neatly resolved through technocratic regulatory intervention alone.

Keywords

Digital markets, competition, privacy, innovation, network effects, artificial intelligence

Introduction

Over recent years, policymakers have become increasingly concerned about the ways in which tech companies collect and deploy user data, and the implications of large digital platforms for the economy and society (Crémer et al., 2019; Furman et al., 2019). Although commentators have long

Corresponding author:
Nick O'Donovan, Keele Business School, Keele University, Newcastle, ST5 5NS, UK.
Email: n.j.o'donovan@keele.ac.uk

been aware of the threats that digital businesses pose to competition and privacy (Froomkin, 1999; Stiglitz, 1999), during the 1990s and early 2000s policymakers tended to prefer *laissez-faire* approaches that relied on market discipline to more interventionist alternatives (O'Donovan, 2022). However, with the growing dominance of platform companies straddling multiple digital markets – operating systems, web browsers, online search, digital advertising, app stores, ecommerce, social media and so forth – *laissez-faire* has become increasingly untenable. These concerns have inspired the introduction of new rules such as the EU's General Data Protection Regulation; the creation of new regulatory bodies such as the UK's Digital Markets Unit; and a range of specific business-level interventions such as the EU's anti-trust actions against Google (Kornelakis and Hublart, 2022), or the fines imposed on Facebook following the Cambridge Analytica scandal by the UK Information Commissioner's Office.

The new legislative frameworks currently at various stages of development and implementation in the US, the UK and the EU are even more ambitious, aiming to address the systematic market power of major digital platforms such as Alphabet, Amazon, Apple, Facebook and Microsoft. There are important differences between the American Innovation and Choice Act, the UK's Digital Markets, Competition and Consumer Bill and the EU's Digital Markets Act (Fletcher, 2023). Nevertheless, they all tend to treat the challenges posed by digital markets as in principle *solvable*, requiring the application of the correct techniques to the correct cases. This paper defines these approaches as 'technocratic': relying primarily on technical expertise and professional judgement to identify solutions, as opposed to wider public consultations or broader democratic processes (Durose et al., 2015; Maman, 2022). By contrast, other approaches to the governance challenges posed by digital markets depict digital regulation as a 'wicked problem' (Montgomery, 2020), emphasising the compromises and trade-offs inevitably involved in any regulatory intervention and the irreducibly political nature of conflict over competing policy objectives (Cioffi et al., 2022; Nitzberg and Zysman, 2022; O'Hara and Hall, 2021).

This paper evaluates the prospects for (and limits of) technocratic governance through a novel theoretical analysis of digital markets, conceptualising diverse sectors, products and business models in terms of a common set of underlying variables. It focuses on the compatibility (or incompatibility) of competition, privacy and what might be termed 'innovation' or 'efficiency' (namely, the development of new, improved and/or less expensive products) in markets characterised by strong network effects. These objectives have been selected as they reflect some of the longest-standing policy concerns of the World Wide Web era, reaching back at least as far as the Microsoft anti-trust cases and online privacy movements of the 1990s. They are also (perhaps not coincidentally) core objectives of (neo)liberal forms of technocratic governance (Burnham, 2001; Majone, 1994). This selection is not intended to imply that these public purposes *should* be prioritised above other objectives such as child protection, mental health, cybersecurity, freedom of speech, media plurality or democratic integrity. The point is rather that these aims figure prominently in much of the technocratic policy literature and practice around digital regulation. If regulators cannot reconcile these objectives, even in a familiar regulatory setting that privileges liberal market relationships between sovereign individuals and profit-seeking enterprises, then the limits of technocratic governance may be narrow indeed. Conversely, to the extent that regulators can reconcile these competing objectives, problems in other policy domains may diminish too (to some degree, at least).

The paper begins by outlining why digital markets are conventionally understood as problematic from the perspective of competition and privacy, while also highlighting how attempts to address these problems raise concerns about negative impacts on innovation/efficiency. It describes how policymakers have sought to reconcile these objectives, focusing on the regulatory leadership of the

European Union. The following sections of the paper argue that these interventions presuppose a particular analysis of digital markets and of the network effects that render these markets prone to 'tipping' decisively in favour of a single provider. While requirements such as gatekeeper neutrality and interoperability address what we describe as 'first-order network effects' (the tendency for dominant platforms to offer a larger *quantity* of matches to users, thereby rendering them ever-more attractive to prospective users), they are less effective at dealing with 'second-order network effects' (whereby more users enable platforms to offer a better *quality* of matches). Second-order network effects are simultaneously more problematic from a privacy perspective but less problematic from a competition perspective than their first-order counterparts. In digital markets characterised by certain structural features – a large and/or rapidly expanding universe of potential matches, a heterogeneous population of users, where match quality is decisive to commercial success – second-order network effects confront regulators with a trilemma, in which regulators cannot maximise all three of privacy, competition and innovation/efficiency simultaneously. In choosing to prioritise any two of these objectives, they must inevitably compromise on the third: pursuing privacy and competition at the expense of innovation/efficiency, privacy and innovation/efficiency at the expense of competition, or competition and innovation/efficiency at the expense of privacy. The paper concludes by exploring how regulatory trajectories in the EU and UK express different approaches to navigating these trade-offs.

Competition, privacy and innovation: Conflicts and current solutions

The digital economy poses distinctive challenges for the achievement of competition, privacy and innovation/efficiency. In terms of competition, many digital markets are highly concentrated, dominated by a small number of firms (or even a single firm). Many high-tech sectors are characterised by substantial fixed costs but low marginal costs, reflecting upfront investment in research and development to create new products that can be cheaply replicated thereafter (in the case of software and online services, for the near-zero cost of transmitting data across the Internet). Other factors contributing to concentration include network effects (whereby additional users create benefits for existing users, which in turn render the product more attractive to subsequent users) and advantages associated with large datasets (which allow firms to improve user experience/services, target advertising, and develop new products and services by training algorithms on these data). Further barriers to entry include learning effects (users have sunk time into mastering incumbent platforms, leaving them reluctant to switch or multi-home), challenges in porting personal data/reputation/connections assembled on one platform to another, as well as anti-competitive contractual terms that render shifting platform or multi-homing unattractive (Arthur, 1994; Baker and Morton, 2018; Furman et al., 2019). Consequently, first-movers that amass large numbers of users early in the development of particular digital markets can enjoy substantial advantages over later challengers, even if these challengers offer a product/service that users would have preferred had it been available earlier, or would prefer *now* if only enough other users were to transfer over simultaneously.

Privacy, too, is threatened by the practices of many companies in the digital economy. As people navigate the online and offline world, they generate vast quantities of data: not just information that they explicitly provide (their name and address when making a purchase or signing up to a service; their likes and shares, posts and product ratings) but also granular data tracing how they navigate and respond to the online world (how many different links they click when presented with search results for a flight to Wichita), and increasingly the offline world too (GPS data on the frequency and duration of their visits to McDonald's, information from a smart watch revealing their endocrine

responses to different stimuli). Even small amounts of data can be used to predict personal characteristics such as religion, politics, ethnicity and sexual orientation (Kosinski et al., 2013), potentially enabling individuals to be identified on the basis of other public domain data (Frankowski et al., 2006). When the data created by our digital activity are triangulated against similar data from other people (both those who resemble and those who differ from us), when they are combined across a multitude of websites, apps, and physical devices, and when they are coupled with the opportunity to perform iterative experiments on an ongoing basis, these data enable tech companies to build highly nuanced profiles of individuals that can be used to both predict and shape individual responses in a wide range of contexts (Kohl, 2021). People might be highly reluctant for these data (and the profiles predicated upon them) to be made accessible to their friends, families, partners, governments, employers, employees, customers, fans, blackmailers and so forth. Even where companies keep these data secure, the results of such profiling might be embarrassing (receipt of an advert for erectile dysfunction treatment while scrolling through your feed in a cramped train carriage) or costly (personalised pricing that inflates the cost of attending a family member's funeral in Wichita). The ability to tailor messages to individuals can blur into the ability to mislead and misinform them, subverting their economic and political preferences (Bradshaw and Howard, 2018; Kohl, 2021; Plunkett, 2018).

Efforts to encourage competition and protect privacy must however be weighed against potential harms to businesses, consumers and the wider economy. Where positive network effects are large, a fragmented market structure imposes additional costs on users. Instead of being able to access all their customers, suppliers and/or contacts in a single place, users are instead forced to navigate multiple platforms to connect with the same population. Where initial investment costs are high but marginal costs are low, duplication of investment effort can waste societal resources that would be better deployed elsewhere. Consumers may prefer a suite of products from a single provider to a set of less well-integrated applications from diverse providers. In these cases, intervening to create a more competitive market structure could be inefficient, resulting in a lower quantity and quality of output than would otherwise be the case. Furthermore, unless intervention also alters the underlying dynamics of the market in question, it is possible that greater competition will prove shortlived, before network effects and economies of scale once again conspire to 'tip' the market in favour of a single dominant provider (Geroski, 2003).

Less concentrated market structures and greater levels of privacy can also inhibit certain forms of innovation. Economists have long noted that the stable profits generated by monopolies could potentially provide a basis for *more* long-term investment in research and development (Schumpeter, 1942), although there is limited empirical evidence of a robust connection between innovation and freedom from competition (Gilbert, 2006). More pertinently, many of the algorithms upon which today's digital services are predicated – from search engine results to content recommendations to targeted advertising to predictive text to image recognition – have been trained in part using massive datasets collected from large numbers of people over long periods of time. In the field of artificial intelligence (AI), businesses that are quick to build a network of active users (or that can leverage users they have accumulated in an adjacent part of their platform ecosystem) may be able to harvest training data from those users, giving them an advantage in the development of next-generation foundation models (CMA, 2023). Advances in digital services often exploit synergies between disparate products, datasets and networks (Haskel and Westlake, 2018). It follows that certain regulatory interventions – interventions that fragment markets, prevent incumbents from acquiring rivals in their own sector and promising start-ups in complementary sectors, or prevent the collection and sharing of user data within and between companies – risk stifling innovation,

producing outcomes inferior to those that consumers and businesses would otherwise prefer (Nuccio and Guerzoni, 2019).

Regulating conflict: From GDPR to anti-trust and the digital markets act

To date, regulatory efforts to resolve these tensions have been led by the European Union: a reflection both of the EU's longstanding political commitments to individual rights, and path-dependent developmental processes that have led to the dominance of EU digital markets by US tech giants (Bradford, 2023). EU regulatory efforts thus act as a useful starting point for exploring the conventional understanding of digital markets embodied in current policy trajectories, the limitations of which will then be examined in the remainder of this article.

EU-led initiatives that target digital markets have differed dramatically in character and scope – from regulations such as the Digital Services Act (2022), through directives such as the Directive on Copyright in the Digital Single Market (2019), to voluntary codes of conduct such as the Code of Practice on Disinformation (2022). For purposes of the current analysis, however, we will focus on a small subset of key initiatives: the General Data Protection Regulation (GDPR) of 2016, the 2022 Digital Markets Act (DMA), and various anti-trust cases against Big Tech undertaken by the Directorate-General for Competition. These examples illustrate how the EU has navigated trade-offs between competition, privacy and innovation/efficiency to date, and the evolving understanding of digital markets that underpins this approach.

Although formally agreed in 2016, the GDPR was the product of several years of development and debate: the Commission's first proposal was published in early 2012, reflecting understandings of (and concerns about) digital markets that date back even further. The GDPR introduced wide-ranging curbs on tech companies' ability to harvest data from individuals without their express consent, and in theory empowers individuals to withdraw their consent and data from one provider and transfer them to another (Houser and Voss, 2018). It requires organisations to obtain authorisation from individuals, covering both the personal data collected and the different purposes for which that data is used. Under the GDPR, individuals have the right to access data that an organisation has collected about them, to receive information about how that data is being used, and to have inaccurate records rectified.

Underpinning this regulatory approach was an assumption that (unbiased, informed) consumer choice will facilitate privacy, competition and innovation/efficiency (Graef et al., 2013). The emphasis on informed consent implies that individuals are the best judge of the value they place on personal privacy: where individuals do not approve of how their data is used, they can select an alternative provider. Portability of data would supposedly facilitate competition between providers offering rival services on different terms, which should in turn drive innovation in service provision (including the development of alternatives offering higher levels of privacy). The Commission itself claimed that 'the possibility to move data from one service provider to another would increase competition in some sectors, for example between social networks' (European Commission, 2012: Annex 5).

The limitations of this approach were already evident by the time the GDPR was enacted. In digital markets characterised by strong network effects, portability alone cannot generate competition (De Hert er al., 2018). Where the value of a service is closely related to network size, it is unattractive for isolated individuals to defect from a dominant platform to alternatives where they cannot access as many friends, contacts, potential customers and/or potential vendors. This dynamic is a major feature of social networks (e.g. Facebook, TikTok and Twitter/X) as well as two-sided marketplaces (whether marketplaces for takeaway food and second-hand books, or for services such

as accommodation and taxi rides). Individual rights to data portability will thus have minimal effect on the competitive dynamics within these markets.

The EU has responded to these concerns in two distinct ways: by imposing restrictions designed to limit the economic, social and political influence that incumbents wield as a result of their dominance of important parts of society's digital infrastructure, and by imposing obligations designed to subject incumbents to greater competitive pressure in their core markets. National-level competition authorities as well as the European Commission itself have launched a series of anti-trust actions against Big Tech. In many of these cases, the companies in question have been accused of using their dominance of particular 'chokepoints' within the digital landscape to influence the wider digital ecosystem (Giblin and Doctorow, 2022). Alphabet has been the subject of multiple complaints and fines for prioritising its own products and services on its platforms ('self-preferencing'): for example, privileging paid adverts in Google Search results, or its own applications in installations of its Android mobile operating system. Apple is under investigation by the European Commission for denying third-party developers access to Near-Field Communication technology on Apple products such as iPhones (preventing the development of products to rival Apple Pay), and by the Netherlands' competition authority for abusing its dominant position in the app store market to levy exorbitant fees on app creators. These anti-trust actions do not challenge Big Tech's dominance over critical pieces of digital infrastructure (search, mobile operating systems, hardware and app stores, respectively), so much as discourage Big Tech from using that dominance to influence the wider digital ecosystem. Similar logic is visible in US discussions about regulating dominant tech platforms as 'public utilities' (Rahman, 2018; Schiller, 2020). These draw inspiration from the period of US legal history in which private owners of infrastructure such as railroads and electricity networks were subject to universal service requirements or common carrier provisions, ensuring that critical infrastructure was open to all on an equitable basis (Novak, 2010).

In parallel to this approach, however, the European Commission has also sought to inject competition into the core markets dominated by Big Tech. The DMA imposes a range of requirements on large tech firms providing certain platform services, which it designates as 'gatekeepers'. In addition to prohibiting some of the self-preferencing behaviours that have prompted anti-trust actions, the DMA also places certain interoperability requirements on platforms. Interoperability involves making networks hosted by one platform accessible to users on another platform, thereby reducing the impact of network effects on competition: accommodation listings on Airbnb could be automatically cross-listed on Booking.com, taxi drivers registered with Uber could become bookable through Lyft, users currently accessible on Facebook could connect with users on LinkedIn. Although the DMA itself focuses on interoperability in a limited set of cases (notably communication and messaging services), delivering on its overarching commitments to fairness and contestability may require extending this logic to other sectors, perhaps even imposing an overarching interoperability duty on digital gatekeepers (Crémer et al., 2023; Scott Morton et al., 2023). In the wider economics and policy literature, interoperability is increasingly seen as an important means of tackling concentration in digital markets (Marty and Warin, 2023; Zingales, 2022).

Where does this leave competition, privacy and innovation/efficiency? Interoperability prevents network effects from tipping digital markets decisively in favour of a single incumbent, increasing scope for competition. At the same time, under conditions of interoperability, competition does not produce the inefficiencies associated with network fragmentation: if anything, network effects will be larger when they occur at the market-level rather than the firm-level. Stripped of the incumbency advantages that they presently enjoy, tech giants will be forced to innovate and/or cut prices to stay ahead of their competitors. Entrepreneurs will be encouraged to enter markets with innovations of

their own, once they no longer fear that dominant companies will simply ape their products and roll them out to existing users before innovators achieve the scale necessary to survive. Admittedly, data-sharing across platform boundaries has the potential to raise privacy concerns: Scott Morton et al. (2023) suggest licensing regimes as one way of mitigating the risk of third-parties mishandling data. Yet, commentators also point out that interoperability requirements that increase competition in digital markets might have privacy benefits too. One important way in which companies might choose to differentiate themselves in these newly competitive digital markets is by offering consumers different choices regarding how their data is collected and used, allowing the privacy-sensitive to opt for services that do not track their online (or real-world) behaviour, and/or to punish providers who misuse their personal data (Scott Morton et al., 2023).

Reconceptualising digital markets and network effects

Emerging regulatory practices reflect the view that network effects are responsible for many of the problems that beset digital markets. Consequently, interventions that reduce the influence of network effects (whether interoperability requirements, or rules regulating how private firms operate critical digital chokepoints) have the potential to resolve tensions between competition, privacy and innovation/efficiency. Appealing though this analysis is, this section of the paper will show that it is incomplete. While emerging regulatory practices such as interoperability can be viewed as a 'supertool' for digital platform governance under certain conditions (Scott Morton et al., 2023), some digital markets are characterised by different kinds of network effect that pose distinctive regulatory challenges.

Conventionally, network effects are viewed as increasing the *quantity* of connections available to users (including connections to the goods, services and content that users might offer one another). In these cases, interoperability promises to increase user choice between platforms without compromising the network effects that users enjoy when adopting a common platform. Privacy concerns are limited as (to some degree) users deliberately choose to make themselves public within these networks, because they want to transact or share or connect with other users. To the extent that users of a ride-hailing app want to connect with any potential drivers or riders in their vicinity, or users of an online marketplace want to reach as many potential customers/vendors as possible, requiring platforms to make their networks interoperable is unobjectionable, and will if anything increase the scale of the positive network effects available. Users of a social network might only want to share certain posts with certain people, but they might also want to select those potential audience members from as wide a network as possible. Admittedly, in some cases users will want greater levels of curation and quality control, and may actively value more exclusive networks where they are more likely to find the contacts, content, goods and services that they desire. Limits to interoperability might be particularly valuable to gay people trying to date in communities that discriminate against homosexuality; young people might be appalled by the prospect of joining social networks used by their parents. In such cases, interoperability is less appropriate, but equally competition concerns may be less acute, as there is scope for a range of providers catering to a range of different groups. While single providers may dominate individual niches of this ecosystem, competitive pressures may nevertheless exist due to the ready availability of alternative adjacent networks, the limited size of any single niche and the fact that users might habitually multi-home anyway (though much depends here on the size and scope of the niches involved: see Afuah, 2013).

Some digital markets, however, are characterised by a different kind of network effect. A larger network of users can also improve the *quality* of connections available through a platform. By triangulating user data against the profiles of other users, and the kinds of connection that have been

validated as 'good for' those other users in some way (whether by user engagement, in the case of clicking on a link or dawdling over a social media post, or by an external form of validation, such as a certified medical diagnosis), some platforms provide better connections the more users they have amassed. Such dynamics are visible in many recommender algorithms: for example, algorithms that automatically queue up posts on a social media feed or videos on a streaming platform.[1] But quality of connection matters in many digital markets, such as medical diagnostic services that seek to connect users to information about their likely pathologies, or generative AI services that seek to match a response to a user's prompt.

These network effects – hereafter 'second-order' network effects, though sometimes described as 'user feedback loops' elsewhere in the literature (e.g. Furman et al., 2019) – have subtly different properties to the 'first-order' network effects that commonly feature in analysis of digital markets, and that current EU regulatory practices address. Second-order network effects are simultaneously *more* problematic from a privacy perspective than their first-order counterparts and *less* problematic from a competition perspective.

With respect to privacy, matching algorithms work by sorting results according to their likely relevance to the user, providing a curated list of contacts, content, responses, goods or services with the most relevant items at the top, or even a single optimal response (often the case with text-based generative AI). They do this in part by learning from the responses of previous users to previous results (feedback on a particular response; which options were selected, ignored, prevaricated over). These results can be tailored to the current user by triangulating their profile against profiles of previous users, and it is this 'personalisation' dynamic that generates serious privacy concerns. Individual profiles may be based on previous queries and/or other personal data drawn from previous online interactions with the platform in question, possibly combined with data drawn from other services operated by the same provider, as well as from third parties (Jannach et al., 2010). Where results are personalised, the data used to profile users often result from detailed monitoring of individuals' online and offline behaviours (how long they linger over a post by an ex-boyfriend in their newsfeed, where their mobile phone really is when they tell their employer that they are off sick). Unlike posts on Twitter or Instagram, unlike a status change showing that a taxi driver is now available for hire, these data were not consciously intended to be shared with other people. Overcoming barriers to entry by rendering these data accessible to competitors thus raises acute privacy concerns: any consent I gave to the platform collecting these data likely was not intended to include sharing this information with competitors of the company I am interacting with, to optimise services that I might never use (assuming my consent was informed in the first instance, rather than resulting from an 'accept all' click made in haste – see McDonald and Cranor, 2008). Although in principle these data might be anonymised, in practice it is often possible to identify specific individuals from a small number of data points (Frankowski et al., 2006). Although datasets can be scrambled to increase anonymity, the more anonymised these data are the less valuable they become for personalisation purposes, limiting the scope for data-driven innovations that could benefit the consumer; whereas the less anonymised they are, the more vulnerable they become to de-anonymisation attacks (Ji et al., 2017).

Although second-order network effects give rise to greater privacy concerns than first-order network effects, they often have less serious implications for competition, because they display more limited potential for value growth as network size increases. With first-order network effects, every additional user offers an additional possible connection to every existing user, so the connectivity-value of new users *increases* with network size. By contrast, with second-order network effects, there could come a point when it becomes difficult to improve the quality of connection between any given individual and the things to which they might be connected (products

in online retail, webpages in a search engine, diagnoses in a diagnostics app, responses to a prompt in generative AI). Beyond a certain level, additional data may cease to affect results, instead serving primarily to confirm matches. This means that incumbency advantages associated with second-order network effects do not always grow indefinitely. The risk of markets tipping irrevocably on this basis alone is thus limited, and there may be less need for privacy-invading and/or innovation-curtailing interventions to preserve competition. Conceivably, multiple organisations could acquire the number of users necessary to provide an adequate quality of matches.

First-order and second-order network effects are not mutually exclusive. They can and do coexist in certain digital markets. For example, in the case of social networks such as Facebook, Twitter/X and TikTok, network growth creates both new potential connections for users, as well as potential improvements in the quality of connections between users (and the content they generate). The same is true for some two-sided marketplaces such as eBay or Amazon Marketplace, where diverse products need to be matched to diverse users. However, not all two-sided marketplaces display strong second-order network effects: in a ride-hailing app, additional users are valuable as they increase the pool of customers available to taxi drivers and vice versa, but matching buyers to sellers is a relatively straightforward mechanical exercise based on availability and proximity.[2] Similarly, it is possible for second-order network effects to exist without first-order network effects, where the content, responses, goods or services that users are connected to are not provided by other platform users, but where data generated by the network of users nonetheless enhance the quality of matches offered to any given user. Second-order network effects can be deployed to improve the way in which users are matched to public domain content (as in the case of web search engines), or content that is proprietary without being user-generated (as in the case of streaming platforms such as Netflix or Disney+).

Regulating second-order network effects

Analysing individual digital markets in terms of the relative significance of different species of network effect is an important first step in understanding which regulatory solutions are most appropriate to them (see Figure 1). In many digital markets characterised by strong first-order network effects alone, competition and innovation can be introduced via interoperability without giving rise to major privacy concerns. Where second-order network effects exist, however, regulators must further interrogate the structure of the market in question. In some cases, second-order network effects may not convey decisive advantages over competitors: they may be a nice-to-have, rather than an essential feature. In other cases, second-order network effects may display rapidly diminishing returns - for example, where the universe of potential matches is small, and/or where the users to be matched are relatively homogeneous. In some cases, however, the universe of matches might be expanding so fast and users might be so diverse that additional data will improve the quality of matches indefinitely, meaning that second-order network effects will continue to grow indefinitely. As we will see in the final parts of the paper, in these cases, regulators will be forced to make trade-offs between competition, privacy and innovation/efficiency.

The range of goods, services or content to which algorithms connect users can vary dramatically. At one extreme, an online store might offer only a handful of largely undifferentiated goods or services. At the other extreme, the universe of things might be massive (the ways in which words in a language can be combined in response to a generative AI query) and/or constantly expanding (the number of videos on YouTube, the number of tweets on Twitter, the number of webpages through which a search engine must trawl). Between these extremes lie diverse possibilities, from producer-retailers that stock a limited number of product lines to online marketplaces selling almost

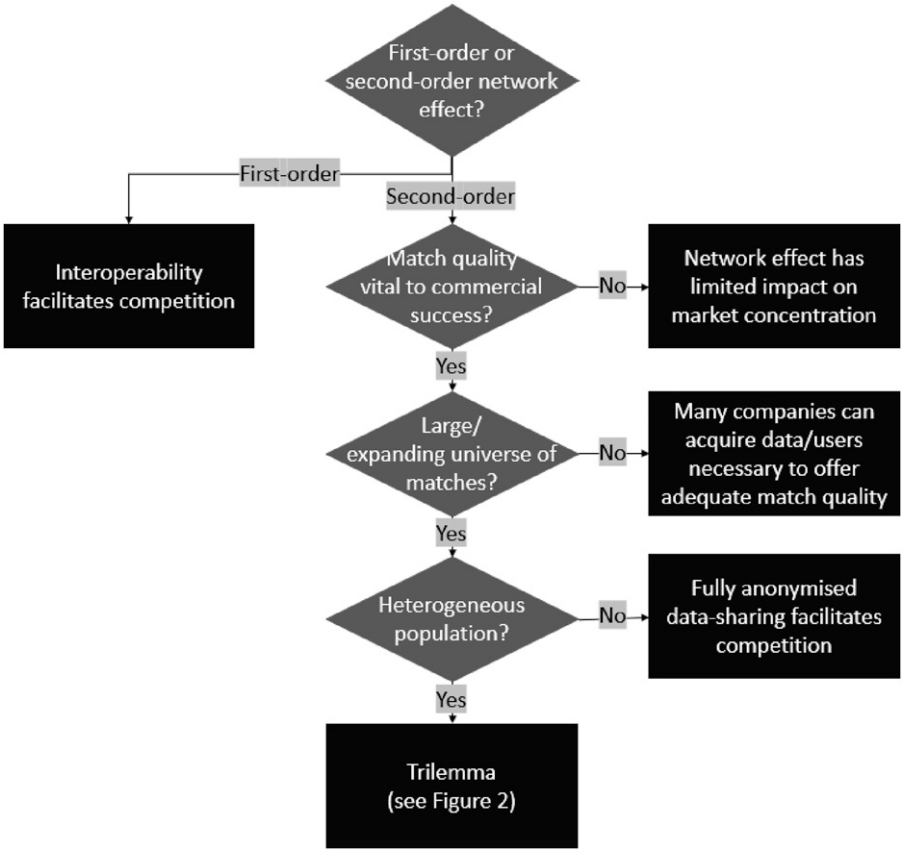

Figure 1. Regulatory interventions to address barriers to market entry caused by network effects.

everything, from video streaming services with hundreds of films and thousands of episodes to audio streaming services with millions of individual tracks and podcasts.

Where the range of possible matches is smaller, there is limited scope for user heterogeneity with respect to that range. But even where there is a large range of options to search through, users might still be largely homogeneous for matching purposes: for example, where users fundamentally want the same thing *despite* the diversity of products offered. A price comparison website might offer a dizzying range of products from different suppliers, but if all users want fundamentally the same thing (the cheapest product available), then no detailed knowledge of potential customers is necessary to provide a high-quality match: simply ranking the items with the cheapest option first would suffice. Moreover, even where users *are* interested in different things, easily communicable *im*personal information alone might be sufficient to provide the matches that they want. For example, users might filter results according to certain criteria or stipulate alternative ranking criteria (sustainability metrics or average customer reviews). The matches that result do not require knowledge about the user above and beyond the generic criteria that they have entered. True, platforms might enjoy a competitive advantage if they possess more customer reviews, but this information is a form of first-order network effect (content wilfully created by users for other users). Consequently, it does not (usually) give rise to the same privacy concerns as second-order network

effects, and it would be relatively straightforward for regulators to require these data to be made publicly accessible (or accessible for a regulated price, to preserve incentives to collect these data).

The same logic applies to many other instances where matches can be made with information that users supply for that matching instance alone – typing the word 'lawnmower' into a textbox on the website of a DIY store, for example. Indeed, such connections might be made without relying on feedback on the quality of responses from a network of users at all: an algorithm might rank items in an online store by reference to the search term and product data alone, or an AI foundation model might be trained on a corpus of public domain material with any further 'fine-tuning' of results performed by paid workers rather than users (CMA, 2023). Similarly, Google's early PageRank algorithm did not require second-order network effects to match results to user prompts, instead sorting matches based on how prominently the search terms featured and how 'popular' pages were (measured by how many other websites linked to them: see Langville and Meyer, 2004). As the web grew in size and complexity (and as web developers sought to 'game' algorithms to improve their ranking), search engines drew on additional data to improve their matches. These included both

(i) feedback from users on the relevance of search results from similar queries (which search results were clicked on most frequently, whether users returned to the search results to select another option: so-called 'click-and-query' data), and
(ii) profiling of users to provide personalised recommendations (understanding what matches someone will prefer based on what matches similar people have preferred in response to similar queries, potentially combining individual search histories with other data on both the individual and the population from other websites/sources).

The former data could in principle be anonymised relatively easily and shared between competitors (they involve only responses to isolated search queries, rather than any information about *who* is doing the searching, including what searches they have run in the past), whereas the latter is more problematic from a privacy perspective (CMA, 2020). Nevertheless, it is an open question as to how relevant user profiling is to match quality in online search – that is to say, how heterogeneous users are *given the search term they have entered* (He et al., 2017; Schaefer et al., 2018).

The importance of second-order network effects is less ambiguous in markets where individual users are 'fed' bespoke content based on minimal active input (algorithms that automatically cue up videos on TikTok, posts on Facebook or tweets on Twitter), or where users might be matched to different things despite very similar impersonal inputs. A search for 'restaurants near me' might offer very different options for people with different historical dining habits, as tracked by previous search data, previous restaurant rankings and GPS monitoring of how much time they spend in McDonald's in an average week. A medical diagnostic algorithm might connect a given pulse reading to very different diagnoses, depending on the user's individual medical history, their personal genome, live information from wearables, and/or GPS data that reveals their recent environmental exposure to different pathogens (and/or how much time they spend in McDonald's in an average week). In cases like these, the quality of connections is improved by locating individuals within a wider population of people who resemble and differ from them in diverse ways, and thus the quality of connections a given platform can offer will improve the larger the user network said platform has assembled (Chiou and Tucker, 2017; De Fortuny et al., 2013).

Even where the universe of possible matches is large and the population that must be matched to it is diverse, high-quality connections derived from second-order network effects may not play a particularly important role in overall commercial success. I do not prefer one online bookstore over

another because of the quality of unsolicited personalised recommendations on the homepage, helpful though these can on occasion be. Admittedly, better recommendations may enable the business to extract more cash from its customers, which may give it an advantage over a website that offers visitors a more generic shop window (perhaps using that additional income to undercut rivals on price or outspend them on marketing). Quite how decisive such considerations are depends on how much additional value is extracted from how many customers. Nevertheless, the point remains that it may be beneficial for a platform to offer such a matching service (given the data/users it has already accumulated) without that matching service in and of itself acting as a substantial barrier to challenger firms.

In summary, not all digital markets in which second-order network effects play a role give rise to similarly problematic conflicts between competition, privacy and innovation/efficiency. Where the universe of potential matches is limited, it is relatively easy and inexpensive for platforms to gather the data needed to make matches of an adequate quality: the diminishing returns associated with second-order network effects mean that they only need a comparatively small number of users to obtain these data. Even where the universe of potential matches is large, if the population is homogeneous, then much of the data needed to make adequate matches could be made publicly accessible, or platforms might be obliged to share it with rivals at a regulated price, without giving rise to privacy concerns. Finally, even if the user population is diverse and the universe of potential matches is large, match quality might not be essential to commercial success and thus might not exert a decisive influence over the competitive landscape. Figure 1 (above) outlines how these structural features of different digital markets imply different solutions. However, it also highlights the existence of residual category for which solutions are not straightforward: cases where the universe of possible matches is large, the population to be matched is diverse, and in which second-order network effects are nonetheless vital to commercial success. In cases such as these, competition is threatened by the fact that the quality of matches continues to improve the more users are attracted to a platform, so platforms that establish an early lead in these markets become increasingly difficult to challenge over time. Match quality generally relies on personal data that people are reluctant to broadcast publicly, problematising attempts to improve competition through data-sharing. And yet the ways in which incumbent platforms combine these personal data from a diverse population of users also promises new innovations and efficiency gains based on data-driven insights.

The regulator's trilemma

These kinds of digital markets confront policymakers with a trilemma, whereby pursuing any two out of competition, privacy and innovation/efficiency inevitably requires compromising on the third (see Figure 2).[3] In these cases, regulators are forced to choose between:

1. Prioritising competition and privacy at the expense of innovation/efficiency;
2. Prioritising innovation/efficiency and privacy at the expense of competition; or
3. Prioritising competition and innovation/efficiency at the expense of privacy.

This section of the paper develops these alternatives, drawing on recent examples from the EU and UK to illustrate the choices implicit within existing regulatory practices.

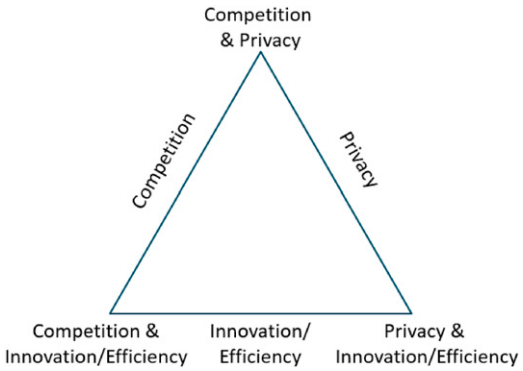

Figure 2. The regulators' trilemma.

Competition and privacy

The first option seeks to level the competitive playing field by *prohibiting* incumbents from reaping benefits from the users and data that they have already accumulated, perhaps even preventing them from collecting that data in the first instance. There is however a cost in terms of efficiency, as data can no longer be used to enhance services (whether for users or for other parties such as advertisers) or to deliver existing services at lower cost. The development of innovative new products and services based on these data is stymied and firms must sink resources into (re)creating user networks for new applications.

An example of such an intervention is the regulation of Google's 'Privacy Sandbox' initiative by the UK's Competition and Markets Authority (CMA). In August 2019, Google announced plans to phase out support for third-party cookies on its Chrome browser, providing users with greater control and transparency over how they are profiled and targeted by advertisers. On the face of it, this private sector initiative should be privacy-promoting: an example of companies responding to competitive pressures (notably, in this case, from Apple) to improve privacy settings. However, it also raised the prospect of Google denying third parties the ability to track users' online behaviour, while still collecting and using that data itself (e.g. directly through Chrome), further entrenching its dominance of the online advertising marketplace to the exclusion of its rivals.

In response to these developments, the CMA launched an investigation into the Privacy Sandbox proposals in January 2021, culminating in Google making a series of commitments that included an agreement not to collect data via Chrome to support its own advertising products or monitor the performance of its rivals (CMA, 2022). These commitments should facilitate competition within the digital advertising sector by removing one means by which a dominant platform (such as Google) can better connect advertisers to particular pieces of digital real estate (instances of a given website displayed to a given viewer). In so doing, however, the risk of an inefficient use of digital real estate increases (irrelevant advertising content displayed to users, and a corresponding reduction in prices that advertisers are willing to pay and revenues that websites will receive, in turn potentially reducing the availability of desirable website content to users). These harms may be deemed a price worth paying for competition and privacy, but they involve a trade-off nonetheless.

Notably, Google's commitments in the Privacy Sandbox case only secure competition and privacy in the narrow (albeit lucrative) domain of digital advertising. In theory, Google could still collect tracking data for other purposes (subject to user consent), enabling it to develop new

innovations/efficiencies in other markets, with its Privacy Sandbox initiative shielding it from rivals who might have used third-party cookies to collect data to compete in these markets. Had the CMA prohibited Google from collecting tracking data outright, it would have levelled the competitive playing field in these other domains too, albeit at the expense of potential innovations and efficiency gains.

Privacy and innovation/efficiency

The second solution to the regulators' trilemma effectively concedes the market to the dominant player or players, instead seeking to preserve privacy while also sustaining innovation and efficiency. Whereas the first solution preserves privacy by preventing the collection (or at the very least, the use) of user data, to the detriment of data-driven innovations, the second solution preserves privacy by ensuring that data is only collected and used subject to user consent, leaving incumbents free to use these data to generate second-order network effects. The recent CJEU ruling in the case brought against Meta by Germany's competition authority, the Bundeskartellamt, reflects this logic. Although Meta's data collection practices were deemed unlawful, the case itself hinged on whether Meta had obtained adequate consent to its harvesting of user data on third-party sites, not whether it could in principle obtain such consent (CJEU, 2023: paragraphs 147–152). Had Meta done so, it could have then used these data to drive efficiency gains and innovations.

The EU's GDPR, with its emphasis on consensual data collection and use, embodies this approach. Personal control over one's private data is preserved by predicating data collection on individuals' explicit informed consent, potentially bolstered by regulating the collection/storage of data and imposing punitive fines on firms for data breaches. This means that platforms that offer users sufficient benefits in exchange for their data (potentially including benefits derived from second-order network effects) can continue to harvest these data and use them to drive efficiency gains or develop innovative new products and functionality. These data remain the property of particular firms and their platform ecosystems, preventing market entry and thus restricting competition where incumbents enjoy strong network effects (Campbell et al., 2015; Gal and Aviv, 2020). Although these data are in theory portable (a right that has recently been augmented by the 2023 European Data Act, which *inter alia* entitles users to access and transfer data generated by any smart devices that they own), individuals must actively *choose* to transfer these data. Such rights are undoubtedly valuable (for instance, empowering users to authorise a third-party repair shop to analyse data from a broken smart device). However, they do not address the fundamental coordination problem that arises in markets characterised by strong network effects: namely, that individuals will only change provider if they stand to gain from doing so, but they will only stand to gain if other people change provider at the same time.

Critics of the EU's approach to privacy rights argue that overzealous regulation acts as a barrier to innovation (Cennamo and Sokol, 2021; McAfee, 2021). It is a valid question as to whether obtaining consent is disproportionately cumbersome under EU regulations, and a *de facto* ban on data collection would indicate a 'competition and privacy' solution to the trilemma. However, as the Meta versus Bundeskartellamt ruling illustrates, the GDPR does not prohibit the collection of data that could be used to drive innovations *per se*. More problematic, for regulators pursuing a 'privacy and innovation/efficiency' solution to the trilemma, is the question of how to preserve incumbents' incentives to innovate where competition is lacking. Imposing public obligations such as common carrier or universal service requirements (requiring the platform to be open to all on equal terms), stipulating minimum service standards (e.g., limiting the ratio of paid advertising content to other material in a newsfeed), regulating prices and taxing excess profits all limit opportunities for

incumbents to extract monopoly rents and abuse their dominant position, potentially forcing them to generate profits through efficiency-promoting investments and socially-valuable innovations instead. The (admittedly remote) threat of new technologies and platforms catastrophically destabilising an incumbent's core business activities might also stimulate innovation (Gilbert and Katz, 2001).

Competition and innovation/efficiency

The final option seeks to overcome barriers to entry in markets characterised by strong second-order network effects by requiring incumbents to share data from their user base with rivals. The data transferred would need to be sufficiently rich, current and personal for competitors to develop and train their own rival matching algorithms and models. Incumbents and challengers alike could then use these data to innovate and drive efficiency gains, delivering both competition and innovation. Although these data could be anonymised (e.g., through 'k-anonymity' techniques that render any given record indistinguishable from a specified minimum number of other records), in digital markets subject to the regulators' trilemma, the universe of potential matches is large and where users are highly heterogeneous with respect to those matches. This means that anonymisation will result in loss of functionality, equating either to less competition (if challengers are only granted access to anonymised data), or limits on data-driven innovation (if the incumbent too is denied access to the full dataset). There may also be a residual risk to privacy as even anonymised datasets remain vulnerable to user identification, especially where organisations acquiring that data have their own overlapping datasets that might enable them to decode missing values (Ji et al., 2017).

Interestingly, of the three trilemma options, it is difficult to find any real-world examples of this final possibility. Commentators and policymakers increasingly recognise that digital markets characterised by strong network effects are not inevitably fated to 'tip' in favour of a single incumbent, and that market concentration is instead a product of firm-level obstacles to interoperability (Zingales, 2022; Scott Morton et al., 2023). Yet, for all the interoperability and data-sharing requirements contained in the EU's DMA (Crémer et al., 2023), third-party access to the kind of personal data that generally underpins second-order network effects remains subject to explicit user consent (Article 6.10). The US regulatory model, often characterised as having a comparatively lax approach to the protection of personal data (Bradford, 2023), still stops short of requiring platforms to place personal data in the public domain, despite the potential gains to innovation and competition that would result. Although privacy often appears undervalued in the digital era (Kokolakis, 2017), it is noteworthy that abandoning privacy altogether in the face of the regulators' trilemma reads more like dystopian science fiction than a serious policy proposal.

Conclusion

This article has advanced a novel conceptual framework for analysing digital markets in terms of first- and second-order network effects, exploring the matching functions that underpin many digital services. As we have seen, this approach can identify *ex-ante* which regulatory interventions will reconcile competition, privacy and innovation/efficiency under what circumstances, suggesting that technocratic solutions to conflicts between these objectives *do* exist, at least under certain conditions. Because this framework is based on the underlying structural features of different digital markets, it can be applied dynamically to emerging technologies (such as new forms of AI) as well as to more established business models.

At the same time, however, this analysis also highlights the limits of technocratic governance: instances where prioritising some public purposes necessarily comes at the expense of others, and selecting the 'right' course of action inevitably involves a political choice between competing visions of collective life. Here, critics of a technocratic approach to digital regulation stand on firmer ground, and questions arise as to how to structure and institutionalise these political decision-making processes (Büthe et al., 2022; Cioffi et al., 2022; Nitzberg and Zysman 2022).

Faced with these choices, different societies might reasonably choose to adopt different approaches. It is even possible to pursue different objectives in different digital markets *within* a single jurisdiction, prioritising (e.g.) privacy and competition in digital advertising markets while opting for innovation and privacy in medical diagnostic services. To navigate these trade-offs in a deliberate and strategic matter, policymakers must acknowledge their existence: not just at an intellectual level, but also institutionally. Privacy rights cannot be established in isolation from competition policies, and vice versa. Enumerating an expansive range of rules and restrictions that apply to all major digital platforms (as per the EU's DMA) may make it difficult to pick and choose different solutions in different markets. A legal framework that grants digital regulators a greater degree of discretion (such as the UK's Digital Markets, Competition and Consumers Bill) may be preferable, although proportionality requirements may yet render the DMA more flexible in practice than it appears on paper (Fletcher, 2023). Similarly, public bodies charged with data protection cannot be segregated from institutions with anti-trust responsibilities. In this respect, recent efforts to foster cooperation between regulators with potentially conflicting mandates should be welcomed (such as the creation of the UK's Digital Regulation Cooperation Forum in 2020, or the 2023 joint declaration by France's Autorité de la concurrence and Commission nationale de l'information et des libertés). There is however a risk that these evolving arrangements might marginalise policy objectives that lack established institutional champions: innovation, for example, has often been treated as a function of competition and thus subsumed within the mandate of competition authorities, which may leave it underrepresented in these emerging regulatory configurations.

Questions also arise as to whether regulators and policy experts are competent to adjudicate on conflicts between competing values, or whether these are ultimately political decisions that require democratic input from the general public and/or elected representatives. At the same time, the rapidly changing and technically complex nature of digital markets poses significant logistical challenges to public consultation and deliberation (Büthe et al., 2022). Even if democratic input is warranted and practicable, regulators will still have an important role to play in identifying where trade-offs arise and clarifying what is at stake, perhaps even commissioning public consultations and contributing to these deliberations themselves (Maman, 2022). Identifying the boundaries of technocratic governance, as this paper has sought to do, does not eliminate the need for technocratic insight. Just as depoliticising a policy domain and handing it over to independent experts is often a deeply political act (Burnham, 2001), repoliticising a policy domain and returning it to the public sphere may require expert judgement on the limits of expertise.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD

Nick O'Donovan https://orcid.org/0000-0002-0588-7734

Notes

1. Recommender algorithms do not always aim at improving quality of connections *for users*: the same data might be used to maximise connection quality for advertisers, for example. In such cases, there would not be a network effect, in theory reducing the chances of users becoming locked-in to a dominant platform by match quality. In practice, however, dominant networks can alter the balance between monetisation and user benefit in response to the emerging competitive landscape, meaning the *threat* of a network effect can still dissuade would-be challengers from contesting these markets (O'Donovan, 2021).
2. Second-order network effects may arise *indirectly* where rider and driver data enable platforms to anticipate demand and deploy dynamic pricing to encourage supply at peak times. In these cases, however, regulatory solutions such as anonymised data-sharing requirements (discussed in the next section of the article) may suffice to alleviate threats to competition, as users remain relatively homogeneous with respect to what they want (namely, the nearest available taxi).
3. As with other notable 'trilemmas' in political economy (e.g. Fleming, 1962; Iversen and Wren, 1998; Mundell, 1963; Swenson, 1989), the term is used here to describe a situation in which three outcomes are presumed desirable yet cannot all be maximised simultaneously. They thus present a choice between three limit cases: other combinations may be possible within the space that these limit cases demarcate.

References

Afuah A (2013) Are network effects really all about size? The role of structure and conduct. *Strategic Management Journal* 34(3): 257–273.

Arthur WB (1994) *Increasing Returns and Path Dependence in the Economy*. Ann Arbor: University of Michigan Press.

Baker JB and Morton FS (2018) Antitrust enforcement against platform MFNs. *The Yale Law Journal* 127: 2176–2202.

Bradford A (2023) *Digital Empires: The Global Battle to Regulate Technology*. Oxford: Oxford University Press.

Bradshaw S and Howard PN (2018) *Challenging Truth and Trust: A Global Inventory of Organized Social Media Manipulation*. Oxford: Oxford Internet Institute.

Burnham P (2001) New Labour and the politics of depoliticisation. *British Journal of Politics and International Relations* 3(2): 127–149.

Büthe T, Djeffal C, Lütge C, et al. (2022) Governing AI–attempting to herd cats? Introduction to the special issue on the Governance of Artificial Intelligence. *Journal of European Public Policy* 29(11): 1721–1752.

Campbell J, Goldfarb A and Tucker C (2015) Privacy regulation and market structure. *Journal of Economics and Management Strategy* 24(1): 47–73.

Cennamo C and Sokol DD (2021) *Can the EU Regulate Platforms without Stifling Innovation?* Cambridge, Massachusetts: Harvard Business Review.

Chiou L and Tucker C (2017) *Search Engines and Data Retention: Implications for Privacy and Antitrust (No. W23815)*. Cambridge, Massachusetts: National Bureau of Economic Research, 23815.

Cioffi JW, Kenney MF and Zysman J (2022) Platform power and regulatory politics: polanyi for the twenty-first century. *New Political Economy* 27(5): 820–836.

CJEU (2023) *Meta Platforms Inc and Others V Bundeskartellamt*. Luxembourg: Court of Justice of the European Union. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62021CJ0252

CMA (2020) *Online Platforms and Digital Advertising*. London: Competition and Markets Authority. Available at: https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study#final-report

CMA (2022) *Decision to Accept Commitments Offered by Google in Relation to its Privacy Sandbox Proposals*. London: Competition and Markets Authority. Available at: https://assets.publishing.service.gov.uk/media/62052c52e90e077f7881c975/Google_Sandbox_.pdf

CMA (2023) *AI Foundation Models: Initial Report*. London: Competition and Markets Authority. Available at: https://assets.publishing.service.gov.uk/media/650449e86771b90014fdab4c/Full_Non-Confidential_Report_PDFA.pdf

Crémer J, De Montjoye YA and Schweitzer H (2019) *Competition Policy for the Digital Era*. Brussels: European Commission, Publications Office of the European Union.

Crémer J, Crawford GS, Dinielli D, et al. (2023) Fairness and contestability in the digital markets act. *Yale Journal on Regulation* 40: 973.

de Fortuny EJ, Martens D and Provost F (2013) Predictive modeling with big data: is bigger really better? *Big Data* 1(4): 215–226.

De Hert P, Papakonstantinou V, Malgieri G, et al. (2018) The right to data portability in the GDPR: towards user-centric interoperability of digital services. *Computer Law & Security Report* 34(2): 193–203.

Durose C, Justice J and Skelcher C (2015) Governing at arm's length: eroding or enhancing democracy? *Policy & Politics* 43(1): 137–153.

European Commission (2012) *GDPR: Commission Staff Working Paper*. Brussels: European Commission. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A52012SC0072

Fleming JM (1962) *Domestic Financial Policies under Fixed and under Floating Exchange Rates*. Washington, DC: Staff Papers - International Monetary Fund, 9(3), 369–380.

Fletcher A (2023) International pro-competition regulation of digital platforms: healthy experimentation or dangerous fragmentation? *Oxford Review of Economic Policy* 39(1): 12–33.

Frankowski D, Cosley D, Sen S, et al. (2006) You are what you say: privacy risks of public mentions. In: Proceedings of the 29th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval (SIGIR '06). New York, ACM, 565–572.

Froomkin AM (1999) The death of privacy. *Stanford Law Review* 52: 1461.

Furman J, Coyle D, Fletcher A, et al. (2019) *Unlocking Digital Competition: Report of the Digital Competition Expert Panel*. London: HM Treasury.

Gal MS and Aviv O (2020) The competitive effects of the GDPR. *Journal of Competition Law and Economics* 16(3): 349–391.

Geroski PA (2003) Competition in markets and competition for markets. *Journal of Industry, Competition and Trade* 3(3): 151–166.

Giblin R and Doctorow C (2022) *Chokepoint Capitalism: How Big Tech and Big Content Captured Creative Labor Markets and How We'll Win Them Back*. Boston: Beacon Press.

Gilbert R (2006) Looking for mr. Schumpeter: where are we in the competition--innovation debate? *Innovation Policy and the Economy* 6: 159–215.

Gilbert RJ and Katz ML (2001) An economist's guide to US v. Microsoft. *The Journal of Economic Perspectives* 15(2): 25–44.

Graef I, Verschakelen J and Valcke P (2013) Putting the right to data portability into a competition law perspective. *Law: The Journal of the Higher School of Economics, Annual Review* 15: 53–63.

Haskel J and Westlake S (2018) *Capitalism without Capital*. Princeton: Princeton University Press.

He D, Kannan A, Liu TY, et al. (2017) Scale effects in web search. In: *International Conference on Web and Internet Economics*. Cham: Springer, 294–310.

Houser KA and Voss WG (2018) GDPR: the end of Google and Facebook or a new paradigm in data privacy. *Rich. JL & Tech* 25: 1.

Iversen T and Wren A (1998) Equality, employment, and budgetary restraint: the trilemma of the service economy. *World Politics* 50(4): 507–546.

Jannach D, Zanker M, Felfernig A, et al. (2010) *Recommender Systems: An Introduction*. Cambridge: Cambridge University Press.

Ji S, Mittal P and Beyah R (2017) Graph data anonymization, de-anonymization attacks, and de-anonymizability quantification: a survey. *IEEE Communications Surveys & Tutorials* 19(2): 1305–1326.

Kohl U (2021) The pixelated person: humanity in the grip of algorithmic personalisation. In: Kohl U and Eisler J (eds). *Data-driven Personalisation in Markets, Politics and Law*. Cambridge: Cambridge University Press, 3–36.

Kokolakis S (2017) Privacy attitudes and privacy behaviour: a review of current research on the privacy paradox phenomenon. *Computers & Security* 64: 122–134.

Kornelakis A and Hublart P (2022) Digital markets, competition regimes and models of capitalism: a comparative institutional analysis of European and US responses to Google. *Competition & Change* 26(3-4): 334–356.

Kosinski M, Stillwell D and Graepel T (2013) Private traits and attributes are predictable from digital records of human behavior. *Proceedings of the National Academy of Sciences* 110(15): 5802–5805.

Langville AN and Meyer CD (2004) Deeper inside pagerank. *Internet Mathematics* 1(3): 335–380.

Majone G (1994) The rise of the regulatory state in Europe. *West European Politics* 17(3): 77–101.

Maman L (2022) The democratic qualities of regulatory agencies. *Policy & Politics* 50(4): 461–482.

Marty F and Warin T (2023) Multi-sided platforms and innovation: a competition law perspective. *Competition & Change* 27(1): 184–204.

McAfee A (2021) *EU Proposals to Regulate AI Are Only Going to Hinder Innovation*. London: Financial Times.

McDonald AM and Cranor LF (2008) The cost of reading privacy policies. *Isjlp* 4: 543.

Montgomery M (2020) *Disinformation as a wicked problem: why we need co-regulatory frameworks*. Washington, DC: The Brookings Institution.

Mundell RA (1963) Capital mobility and stabilization policy under fixed and flexible exchange rates. *Canadian Journal of Economics and Political Science* 29(4): 475–485.

Nitzberg M and Zysman J (2022) Algorithms, data, and platforms: the diverse challenges of governing AI. *Journal of European Public Policy* 29(11): 1753–1778.

Novak WJ (2010) Law and the social control of American capitalism. *Emory LJ* 60: 377.

Nuccio M and Guerzoni M (2019) Big data: hell or heaven? Digital platforms and market power in the data-driven economy. *Competition & Change* 23(3): 312–328.

O'Hara K and Hall W (2021) *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*. Oxford: Oxford University Press.

O'Donovan N (2021) Personal data and collective value: data-driven personalisation as network effect. In: Kohl U and Eisler J (eds). *Data-driven Personalisation in Markets, Politics and Law*. Cambridge: Cambridge University Press, 74–91.

O'Donovan N (2022) *Pursuing the Knowledge Economy: A Sympathetic History of High-Skill, High-Wage Hubris*. Newcastle upon Tyne: Agenda Publishing.

Plunkett J (2018) *Markets Don't Work like They Used to*. San Francisco: Medium. Available at: https://medium.com/citizens-advice/markets-dont-work-like-they-used-to-and-people-are-starting-to-notice-af00ed38014d

Rahman KS (2018) The new utilities: private power, social infrastructure, and the revival of the public utility concept. *Cardozo Law Review* 39: 1621.

Schaefer M, Sapi G and Lorincz S (2018) *The Effect of Big Data on Recommendation Quality: The Example of Internet Search*. Düsseldorf: Düsseldorf Institute for Competition Economics Working Papers, 284.

Schiller D (2020) Reconstructing public utility networks: a program for action. *International Journal of Communication* 14: 12.

Schumpeter J (1942) *Capitalism, Socialism and Democracy*. New York: Harper and Brothers.

Scott Morton FM, Crawford GS, Crémer J, et al. (2023) Equitable interoperability: the "supertool" of digital platform governance. *Yale Journal on Regulation* 40: 1013.

Stiglitz J (1999) *Public Policy for a Knowledge Economy*. London: Remarks at the Department for Trade and Industry and Centre for Economic Policy Research.

Swenson P (1989) *Fair Shares: Unions, Pay, and Politics in Sweden and West Germany*. Ithaca: Cornell University Press.

Zingales L (2022) *Regulating big tech*. Basel: Bank for International Settlements, 1063.